THE SPOOK BOOK

A Strange and Dangerous Look at Forbidden Technology

Mick Tyner

READ THIS BEFORE YOU READ THE BOOK

This text treats a number of topics, many harmless, others extremely dangerous, at least to carry out, not to read about, and that meets the author's intent: to provide something lively to read. He states here, and repeats throughout, that he recommends absolutely no hazardous or illegal activity to anyone.

Human nature includes in its repertoire the capacity for vicarious experience. We may read a murder-mystery laced with killings, robbery, torture, kinky sex, and pigging out on chocolate—and relish every page. Yet no sane person would actually wallow in those perversions, especially not thick indulgence in dark candy.

The same point applies to surveillance, lock-picking, strange weapons, illegal fireworks, and a host of spooklore this book treats as casually as talk of cross-stitch. The author intends it as no more than vicarious adventure for the reader.

Reading about it and doing it tap different sides of human nature. Age does nothing to dull our fascination with risk, but brings with it an appreciation of our frailty and mortality. The text speaks easily of gray-zone projects now fading from memory, but would no more endorse them today than it would condone child-molesting.

The book relates the step-by-step of things because they happened that way, at least those of which the author was a part some years back. Journalistic credibility demands that frankness. People read tech studies to glean hard detail. Books that omit it prompt them to look elsewhere, often to sources unconcerned with safety, or to those that invoke a handy political code to justify reckless advice.

Nothing contained herein may be construed as evidence of illegal activity on the part of the author. Some names of individuals and organizations have been fabricated to suit a literary need for fictitious entities. All registered trademarks mentioned in this book are hereby recognized.

Neither the author nor the publisher assumes any responsibility whatever for use or misuse of the information contained in this book. This book is sold solely for informational purposes.

THE SPOOK BOOK

A Strange and Dangerous Look at Forbidden Technology

By Mick Tyner

Printed in the United States of America

ISBN 0-940401-72-X Softcover

Neither the author nor the publisher assumes any responsibility whatever for the use or misuse of information contained in this book. This book is sold solely for informational purposes.

CONTENTS

INTENTS, PURPOSES, & ACKNOWLEDGMENTS

Many books that deal with spooklore carry the look of a catalog. To a degree this is unavoidable: The hardware bears the message. A picture of a microtransmitter stuck to the end of a thumbnail speaks silently of its potential. In fact, perusing a catalog from the typical "police supplier" tells much of what is possible, from both attack and defense, with modern bugging technique. The U.S. Embassy fiasco in Moscow highlights a climate of technological subterfuge that demands a hard-nosed approach to surveillance, since we have come to feel its cold hand in ever-more aspects of daily life. Those who refuse to learn the etiquette of attack and defense disarm themselves. They deserve to suffer their ignorance.

And yet, we still find room for that whimsy that takes us back to better days, touchy though it may be to treat some points. Readers have shown a lasting fascination with bugging, illegal fireworks, and tools of violence, along with sex and smut—but television has co-opted those last topics. This book admits and caters to the spy, cop, detective, commando, and basement bomber in us all, but discourages irresponsible conduct, and even throws in a few safety tips from an ex-pyro, long since quit from that racy caper.

The author has sought to avoid repetition of what's already seen print. He treats material either to flesh out points touched in other works or to tackle obstacles that arise when one applies techniques detailed in those texts, but not anticipated by them. His participation in a few offbeat gigs lets him offer bits of original material here and there.

Generous contributions from many individuals made this book possible. The author hereby expresses heartfelt thanks to those sources. After much thought, he has elected to credit no one by name, since persons who gave freely of their expertise were not aware when they did so that the book embraced material with which they might not wish to be identified. Some sources were placed with firms that most surely would take a dim view of studies presented herein. Rather than have sources suffer guilt by association, the author has given them anonymity.

Have fun, but don't break the law and don't get hurt.

1
AUDIO

...the ineluctable modality of the audible.
—James Joyce, Ulysses

* * *

Sometime in the dark interlude between Taxi Driver and Blue Velvet America admitted to itself, if only at some sunken gut level, that bugging had become more pervasive than venereal disease. That uneasy sense seeped through the national regard like an evil anesthetic, slowly numbing us to ever-more fearsome means of privacy invasion, an almost welcome surrender to the lewd caress of 1984. By and large, a sheep-like populace embraced Isaac Asimov's roll-over-and-die stance that you can't regain what's already lost. Much of the fare to nurture this nervous change crawled out of spook literature and slunk toward big-time in the media.

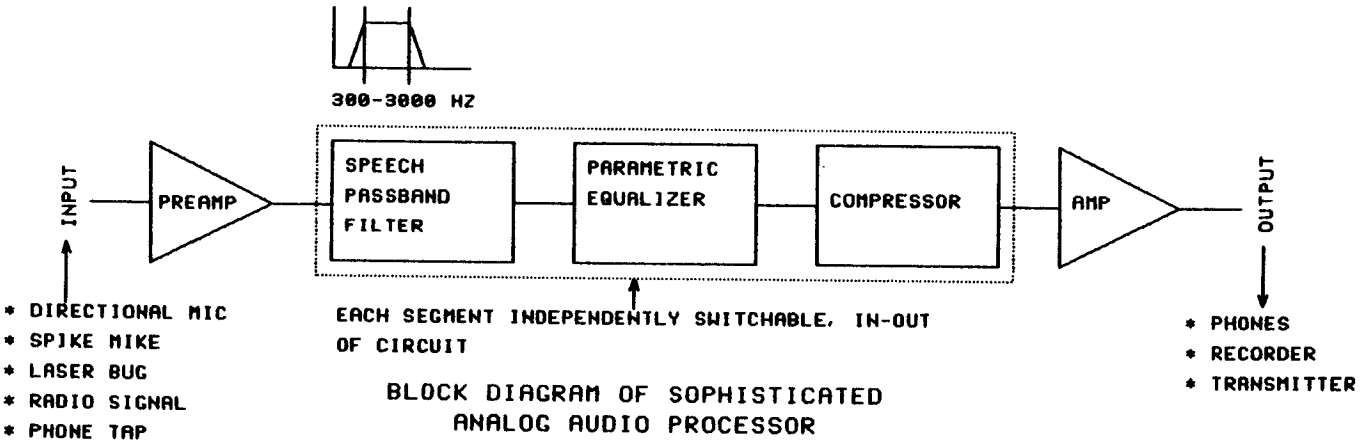
One school of journalistic thought insists that the reporter involve himself in the scene to impart it correctly. Others argue for detachment. But this business of bugging and its close cousins have eliminated detachment as an option. The wolf is at the door, in the basement, and coming down the chimney like some Soviet Santa Claus. Bugging and its emotional fallout have sewn themselves into the fabric of American life.

Audio maintains the pre-eminent spot in surveillance. It seeks to maximize pickup of intelligible human speech. The simplest surveillance unit is an eavesdropper. He performs all aspects of interception, processing, even interpretation. But most audio surveillance depends in varying degrees on some form of electronics. Analysis of the sound path in electronic surveillance generates a predictable circuit whose elements we must grasp:

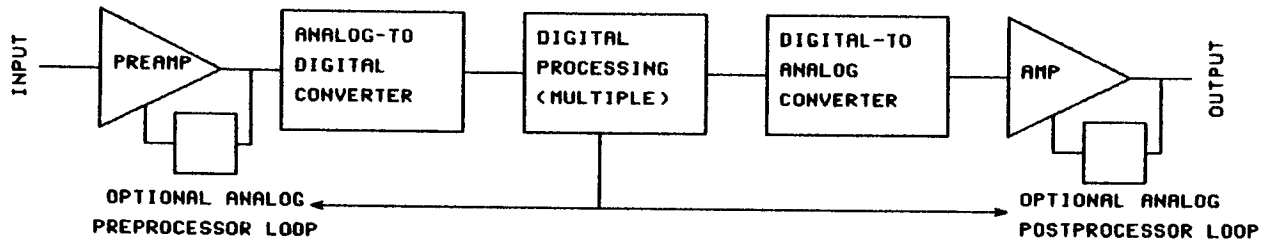
1) input—usually a microphone
2) preamplifier
3) processor(s)
4) output—headphones, recorder, transmitter, etc.
5) sometimes, post-processing

ONE: MICROPHONES—THE GOOD, THE BAD, AND THE TERRIBLY SMALL

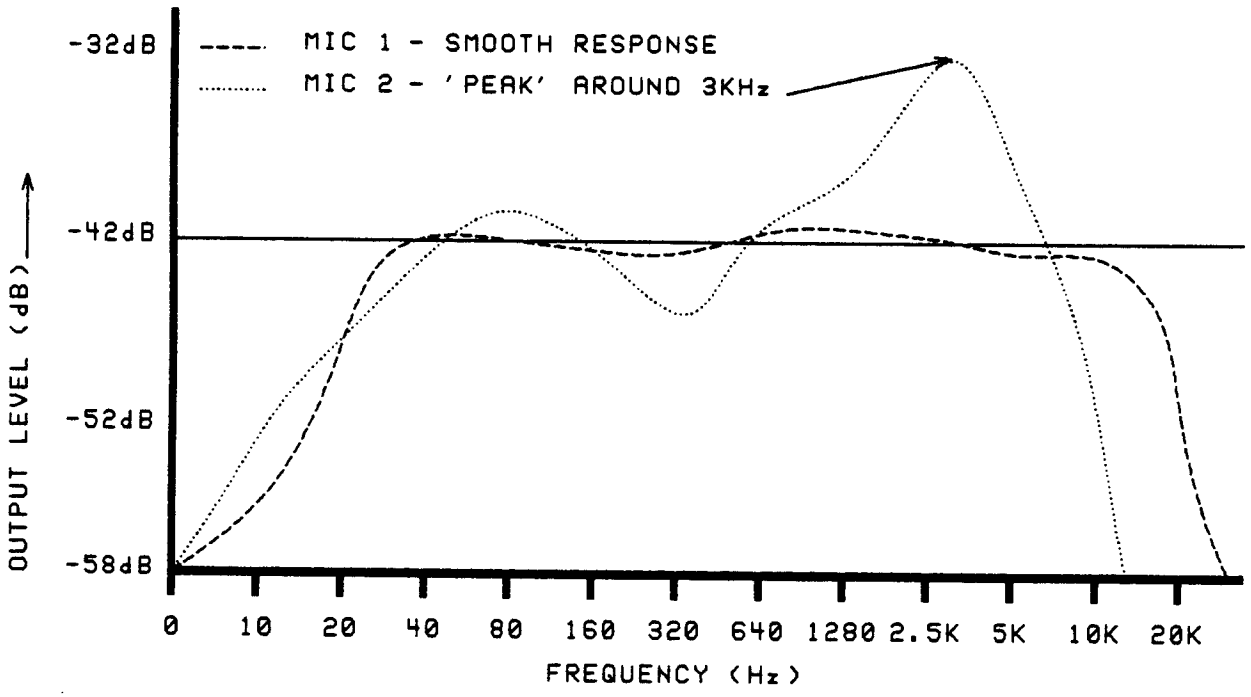
A microphone (mic) transforms one type of force into another. Energy enters as sound and emerges as electricity. Mics effect this sea-change through varied means that make for special properties that we must factor in to our selection and use of them. This details only the basics. Microphone design has proven



BLOCK DIAGRAM OF SOPHISTICATED ANALOG AUDIO PROCESSOR



BLOCK DIAGRAM OF DIGITAL AUDIO PROCESSOR



surprisingly complex, as perusal of texts on the subject will show. The tricky stuff slips wretchedly into fourth-semester calculus.

DYNAMIC MICROPHONES

Take the grill off one of your stereo speakers. Pump in some music with a heavy bass-beat, and watch, or feel, the largest speaker, known as the woofer. It vibrates in response to electrical output from your stereo amplifier.

Were you to connect the speaker terminals to a sensitive voltmeter, then tap the woofer cone, you would see that speakers work in reverse: If you move their cones, they generate electricity. This has to do with movement of a conductor in a magnetic field, Michael Faraday, and a depraved series of equations the author never mastered.

Dynamic mics are miniature loudspeakers optimized for their ability to produce electricity in response to sound, while speakers are optimized to perform the reverse.

These units tend to be rugged, weather-resistant, low impedance—and large. They find use in directional mics, but only the rare dynamic element can rival the electret for tiny size. The photo illustrates a modern dynamic mic element; the single-tube listener project described below uses a 3" speaker as its dynamic mic. They are prone to pick up 60 Hz AC hum unless shielded.

Most dynamic elements the author has seen are optimized to the human voice spoken less than a foot from the mic. To no one's surprise, this type performs poorly in surveillance applications.

CRYSTAL MICROPHONES

The species takes its name from the crystal of Rochelle salt that forms its piezoelectric heart. Subject this salt to physical force and it generates electricity, up to thousands of volts from a truly sharp rap. But place a small bit of the stuff on the end of a tiny piston connected to a diaphragm, then wire the crystal to an output, and we have a crystal microphone. Its close cousin, which differs in no major regard, is the ceramic mic, a crystal mic by another name, since it uses barium titanate in lieu of Rochelle salt. It has proven a bit more weather-resistant than the usual crystal mic, offers slightly lower impedance, but belongs with the same breed.

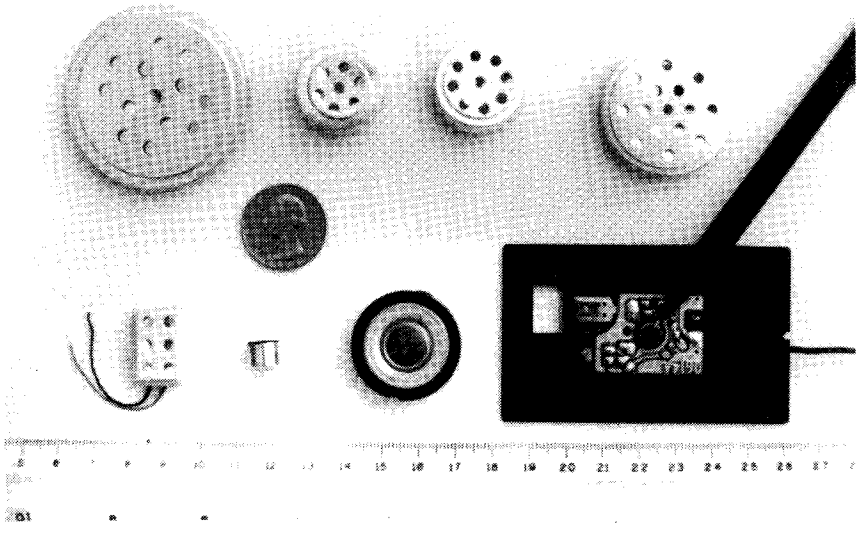
For more than 30 years the darling of the hobbyist, the crystal mic has ceded its place to the modern condenser mic. Yet, it still finds application where its high output, high impedance, and low cost give us an edge. Some hearing aids, for example, use crystal mics.

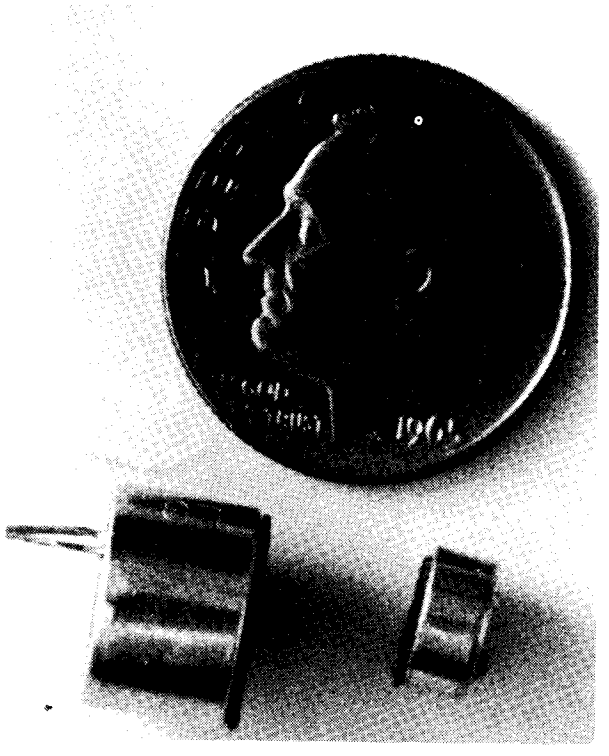
While testing our nascent Ultra Amp, described in the next chapter, we wrung it out with a gaggle of mics, including 5 different crystal and ceramic mics. We discovered a world of similarity in performance among them. All sounded tinny and/or gave nasty treble peaks. Lowest impedance was 7K, highest 25K ohms. Output ranged from -70 dB to -55 dB. Taking the electret at -64 dB as average, we found that the -55 dB mics gave the equivalent of 10 dB of boost before the signal reached the preamp. Unfortunately, their abysmal fidelity took them out of contention for serious work unless we were saddled with electronics which only their high output could overcome. They cost about the same as the average electret element.

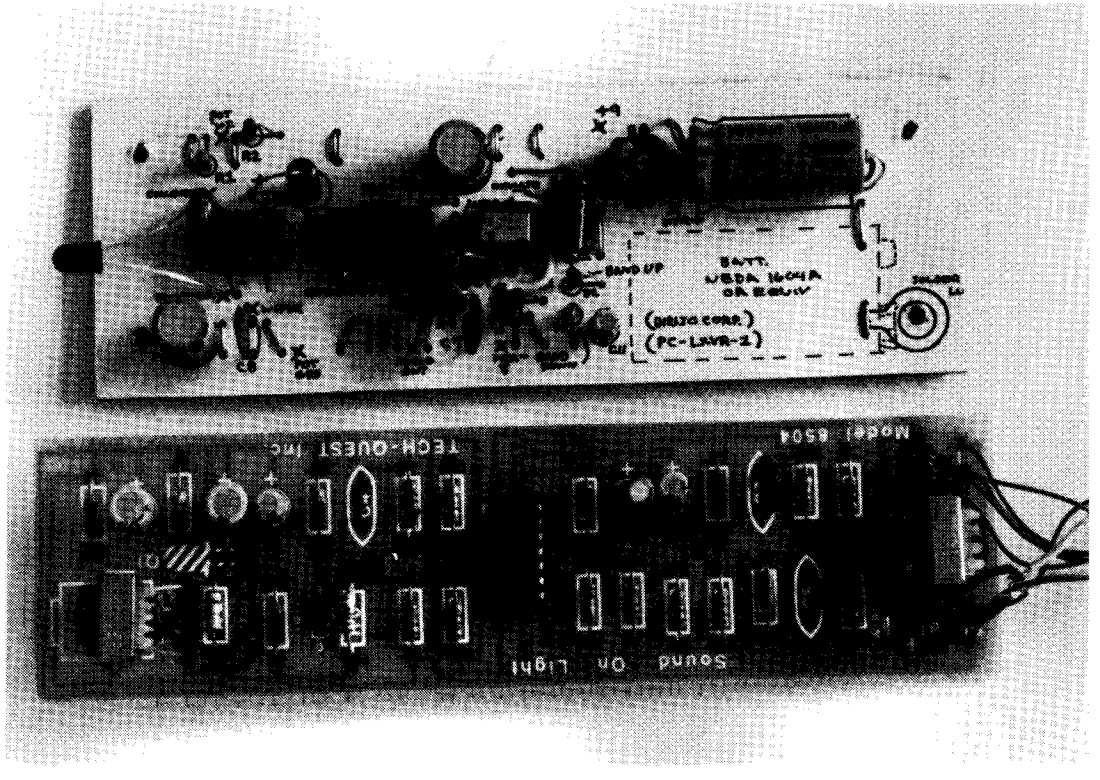
Perhaps the major application for crystal mics in surveillance are contact mics—spike mics, limpet mics—wherein a probe of some sort links directly to the piezo crystal.

CONDENSER AND ELECTRET MICROPHONES

The breed predominates nowadays. Modest cost coupled with wide, smooth frequency response and surprisingly small size make it attractive, particularly for clandestine work. The photo shows a dime, which dwarfs Radio Shack's Model 270-090, which in turn dwarfs Panasonic's Model WM-62A (found in the innards of Radio Shack's credit card-size omnidirectional mic, catalog #33-1089, mounted with its preamp/impedance matcher). Digi-Key carries the WM-62A sans frills for $3.75.







TOP LEFT: Parade of mics. Top row various crystal/ceramic mics. Bottom row, from L to R: crystal mic, electret, dynamic element, and another electret mounted w/preamp. ABOVE: dime, Radio Shack's PC-mount electret mic, and the tiny Panasonic WM-62A. LEFT: Top is Richard Pearson's "laser listener" board, bottom is similar device from "Sound On Light." See text.

The operating principle depends upon a change in distance, and therefore capacitance, between 2 electrically charged membranes. At least 1 of the 2 membranes is flimsy, such that sound alters the distance between them. Few amplifiers can deal with variable capacitance as an input, so the condenser must mate to its own built-in field effect transistor (FET) amplifier, which does two things. First, it changes the capacitance variation into a change of voltage or current. Second, it drops what would be an impedance of millions of ohms to mid-impedance territory, 500-2000 ohms being typical. Thus, these mics require a power supply. Some use a tiny battery held in the mic casing itself. Others draw energy through their output leads, something known as "phantom power."

The true condenser mic uses its power supply to create a voltage across its membranes, while the electret mic is nothing more than a condenser mic that maintains its charge permanently through some wizardry we needn't explore. But the electret still needs that FET preamp/impedance match and so requires external power.

Frequency response here rates good—too good in fact, for it reaches well below the range of the human voice. Than means pickup of unwanted and typically overwhelming low frequency noise that we must filter, adding another set of parts to the amp. We performed our tests using a pair of AKG-240 headphones for monitoring. These phones are renowned for their bass response. Without exception, all electret mics we tested with preamps set for "flat" response overpowered us with their bass fidelity. After achieving high gain, our first processing step turned toward trimming the bottom end. (Of course, if we intend to put the signal through a voice-stress analyzer or similar tool of evil, and can record in genuinely quiet surroundings, we may wish to retain that awesome low end....) The high end, too, extends far above all but soprano harmonics. We can roll it off around 6 KHz and miss little.

OTHERS

Some mics just weren't meant for surveillance. The size, cost, and fragility of large ribbon mics used in recording studios disqualifies them from surveillance work.

The carbon mic seems now to be gasping its last. Formerly the exclusive mic of telephone mouthpieces, it packed carbon granules between conductive plates charged relative to one another. Sound pressure hitting the plates compressed the carbon granules, altering their net resistance in response to audio modulation, thereby changing the current flowing between plates.

The carbon mic is big, offers mediocre response adequate for phone lines, and is now found in only a few phones made and sold by companies who made them before deregulation, and who've found no reason to change.

A popular item in bugging circles used to be the drop-in transmitter, a device close in size and shape to a carbon phone mic that could be dropped into the screw-off mouthpiece of any "standard" phone. It would transmit the conversation via radio over short distances. Needless to say, with practically no two phones alike today, and most using condenser mics, the carbon mic has become a relic in the lore of surveillance.

The pressure-zone microphone (PZM[tm]) is not so much a type as a design, since the element could in theory be dynamic, condenser, or what-have-you. Pressure zone refers to the placement of a boundary about 1/32" in front of the mic surface. This results in a special phenomenon, the arrival of direct and reflected sound at the element such as to cancel echoes. Since much of the boomy quality of sound recorded in closed spaces traces to echoes, the PZ mic enhances intelligibility. Its drawback is bulk, though models are available that will fit in a front shirt pocket. Crown holds the patent on this design but has licensed manufacture to other firms.

MICROPHONE SPECIFICATIONS

All mics possess unique operating characteristics known as specifications or specs. We must know these and understand them in order to select and use mics to best advantage.

The first spec defines frequency response: What range of sound will drive usable output from the mic? Human

hearing is said to span 20 Hz to 20,000 Hz. High fidelity recordings demand the widest response we can get. But for surveillance work, which consists almost entirely of intercepting the human voice, we seek to limit the response to the range of speech fundamentals and overtones, and to exclude bands that would interfere, such as wind-noise or 60-cycle hum.

Whatever the range of frequency response, we seek smoothness. Refer to the diagram. It shows two microphone response curves. The first is smooth, with little deviation from flat at most frequencies. The second shows a nasty "peak" at about 3 KHz. This causes a harsh, tinny sound that makes listening tiresome.

Second, how sensitive is the mic? In other word, for a given sound level, how much electrical output can we expect? In scenes where prized sounds may be mere whispers, or have traveled from afar, we seek the most sensitive mic that does not sacrifice other performance variables.

Third, what is its signal-to-noise ratio (abbreviated S/N)? Even the quietest of microphones introduce their own electrical noise, typically hiss-like. This emerges as a problem when the amplitude of the mic's own noise looms large relative to its input signal. This specification is usually expressed in "dB" or decibels. The S/N ratio tells the number of decibels louder than the mic's noise the input signal measures.

Some compact disc players quote a phenomenal S/N ratio of 90 dB. The appliance itself makes no noise audible to humans. Vinyl records, on the other hand, clock in at 50-60 dB. In quiet passages their hisses, clicks, and pops sound like "Rice Crispies" cereal, but a S/N figure of 50 dB is not bad when talking surveillance gear. Typical condenser mic cartridges claim S/N ratios of 38-42 dB, not that great. When added to the noise of high-gain preamplifiers, we cannot escape annoying hiss.

Note also that noise accumulates with each stage: mic noise, preamp noise, processor noise, amplifier noise, and tape recorder noise, particularly if we must use shoddy gear or dub the tape. This points up the advantages of digitizing an audio signal as early as possible, since we can process or dub infinite generations of digital data with no decline in S/N ratio when we return it to analog form. See section below on the ominous specter of digital sound processing.

Fourth, what is the mic's impedance? Impedance refers to net resistance to flow of alternating current, usually at a specified frequency, such as 1000 Hz.

Mics fall into one of two impedance categories, high and low. High impedance mics suffer a potential shortfall in that their high frequency response falls off rapidly in long runs of cable, a problem low impedance mics do not share.

Low impedance generally means anything from 50 to 600 ohms, high covers 5000 to more than 20,000 ohms. Most dynamic and condenser/electret mics are low-impedance devices, while crystal and ceramic mics are high-impedance. Some mics come with tiny transformers built into them such that impedance may be toggled high or low at the flip of a switch.

For spook work it is not so much the mic's absolute impedance as it is the need that we closely match it with interfacing machinery, or suffer a loss of signal or a decline in S/N ratio. Lousy function blamed on the electronics often traces to mismatch between amp and mic or other source.

If a mic and its interface do not match, use a transformer to match them. Take the example of the single-tube directional mic described below. Its mic is in fact a 3" speaker whose impedance measures about 8 ohms; but the input impedance of the amplifier rates about 1000 ohms. That explains the interposition of a transformer that matches the impedance of the mic to that of the amp. Without it, tests showed a sharp drop in performance. (If we chose a mic whose nominal impedance rated 1000 ohms we could dispense with the transformer.)

Fifth, how durable is the mic? How does it hold up under environmental changes of humidity, temperature, and shock? Dynamic and electret mics have proven sturdy and stable in most respects.

Sixth, how large or small is the mic? Refer to the mic photos, and note that hearing aids use mics smaller than the smallest we have shown here, a Panasonic WM-62A.

Large size proved to be an asset in one case, since it almost fooled the sweep-team on the trail of a concealed mic. A crafty snooper had used a built-in ceiling speaker, ordinarily a source of background music, as a low-impedance mic. What put the sweepers onto it was its silence while the rest of the speakers in the office played some variant of Muzak[tm].

TWO: PREAMPLIFICATION

Generally, the caliber of the preamp determines worth of the system. Good preamps can compensate for marginal elements elsewhere in the sound path. Bad ones can nullify the best mics and equalizers. Prime preamps are scarce.

Signals generated by most mics or other sensors, such as phototransistors in the dread laser bug, lack power to do anything useful. We must enlarge them to allow further exploitation, known as processing. This initial boost is known as preamplification because it usually precedes a second stage of boost that drives speaker or headphones.

Two key factors in preamplification are gain and noise. Gain refers to increase in signal afforded by the preamp. Noise refers to unwanted sound introduced by preamplification.

No theoretical barrier limits the amount of gain we may apply. The practical barrier looms as noise and electrical breakdown. Noise parallels gain, limiting gain to the point at which noise remains tolerable. Electrical breakdown occurs when we push gain so high that either oscillation occurs, sending a hefty squeal through the phones, or inaudible ultrasonic feedback caused by mere proximity of components shuts down the amp.

Practical preamplifiers enjoy high gain and low noise. Preamp designers tend to favor Del Shannon's records, 'cause they're always Searchin'—for higher gain and lower noise.

The engineering trend toward operational amplifiers and away from discrete components lies with the fact that op amps are easier to handle, the math less complex, manufacturing simpler, and they tend overall to cost less. Yet, after testing a gaggle of amps/preamps, we found that properly executed designs that used discrete components in the front end did not suffer in comparison even to "low noise" integrated circuits.

THREE: SIGNAL PROCESSING

Gathering sound and boosting the signal pose little challenge for even the dilettante spook. Culling intelligible speech from marginal signals presents a conundrum that we may conquer using methods that fit under the rubric of "processing." Ideally, we process the audio as it leaves the preamp, but sometimes this proves impractical; so we tape the signal and process later, but call it "post-processing." (Ideally, taping introduces no noise. The better open-reel decks and video-based recorders pass muster. Hand-held units throw in noise from their own electronics and basically rotten tape, dumping added freight on the post-processor.)

3-A: SPEECH PASSBAND

A first step in processing might well remove sounds outside the speech band. This takes a load off later segments of the chain in that they need deal only with this pre-screened sound, rather than a barrage of useless interference along with the conversation. Those who have used a spectrum analyzer appreciate the point. The spectrum analyzer displays relative sound levels centered at octave frequencies in home stereo gear, one-half or one-third octaves in studio gear. We are hardly aware of the 40 dB nearly subsonic boom of footsteps until we see it on the analyzer, or of the constant, 30 dB rumble of distant traffic. Our internal auditory processors filter it automatically. Your mic and amp will not. At the least these sounds annoy. At worst they defeat surveillance. Thus, we eliminate many headaches—literally—by limiting the frequency response of the amplifier to the speech passband.

To grasp this step, think of a hi-fi speaker with three drivers, typically a woofer for low frequencies, a

midrange for the mids, and a tweeter for the highs. Such speakers incorporate a passive device known as a crossover. Crossovers shunt low frequencies to the woofer, mids to the midrange, and highs to the tweeter. Let's assume our imaginary speaker's midrange driver covers 300-3000 Hz, the speech passband. By discarding the woofer and tweeter, as well as those elements of the crossover that fed them, we could both accomplish our goal and simplify the setup.

Speaker crossovers employ big inductors and capacitors that would dwarf the average spy-type amp. They ill-suit the task. On the other hand, operational amplifiers have shown themselves perfectly suited to electrically powered ("active") filters. We seek a filter to cut out sounds below 300 Hz and above 3000 Hz. This is known as a speech passband filter.

Actual circuit design can get dangerously complex, as perusal of Don Lancaster's classic (11 printings from '75 to '86) Active Filter Cookbook will show; yet, the task lies within the grasp of the average electronics hobbyist, at least if he or his computer are willing to wade through the math. (Or use the "ripoff" section in Lancaster's book. It prints tables that let the first-timer design filters with 6 to 36 dB/octave slopes.)

3-B: COMPRESSION

A second dreary hindrance of spook amps lies with subjects' ruthless tendency to speak at vastly different levels, from a whisper to a shout, and to move about the surveillance area, altering their distance from the microphone, thus changing the sound level. This creates an input of extremely wide dynamic range.

The advent of digital recording thrust this twisted concept into the limelight. Formerly, with the recording media of tape and vinyl records, we could not bring full dynamic range to the listener due to the fact that the recording medium would not support it. Fifty to 60 dB was considered excellent for vinyl. Digital recordings on compact discs or digital audio tape, and "Hi-Fi" videocassette recorders offer dynamic range in the 80-90 dB spread, an enormous increase given that power doubles with each few dB. Now we can record the majesty of an orchestra with full dynamic fidelity from its pianissimos to its fortissimos and beyond, and play it back as forcefully as our amplifiers, speakers, and ears will stand.

We desire the exact opposite of expanded dynamic range when recording speech in surveillance work. We wish to hear whispers as if they had been spoken aloud. We want shouts reduced to the level of conversation. This calls for a type of processing known as compression. It automatically boosts the level of small signals, and cuts the level of big ones, handing us an even signal level easy on the ears for real-time monitoring, as well as more intelligible.

A door slamming or sounds of gunfire could distort your recording; or, if you happened to be monitoring in real time, with gear capable of accurately capturing the ruckus, you could suffer hearing damage, or at least a headache. (Those who have done hard time hooked up to high-gain amps running wide open to catch that ghastly incriminating moan will confirm that the noise gets to them, and quickly. Oh, our Divine Lady of Alka-Seltzer, don't quit me now....)

The diagram shows in graphic form what the NEC uPC1571 compander chip does in compressor mode (it may be configured also as an expander; call NEC at 1-415-960-6000 and ask for the data sheet on this versatile chip, available from Mouser Electronics for less than $3; this chip is known generically as a "571," and is available from other manufacturers). An input at 0 dB level results in neither gain nor cut. An input at -80 dB, extremely low level, results in automatic signal boost of 40 dB, a tremendous gain. Input at +20 dB causes the signal to be cut to +10 dB. The broken line shows the theoretical effect of feeding the output of one channel of this dual-channel unit into the second channel: double compression.

How much does compression improve listenability? Once you have used a genuinely effective compressor, you can't go home again.

The limiter makes a brutal but undeniably sure substitute to the compressor. This simple electronic arrangement clamps peak-to-peak voltage at a set level. The resultant harsh/fuzzy sound takes some getting

used to. Listen to radio communications in the opening carrier-deck sequence of Top Gun to catch the effect. A reversed diode-pair coupled capacitively to the output of the preamp shunts the signal to ground once it passes the turn-on voltage of the diodes. We can use 4 diodes—2 in series, reversed—to raise the cutoff level. Limiters leave signals below their threshold alone, meaning that only loud sounds will provoke their ruthless effect. A limiter is easily engineered into a preamp, protects us from sudden, unexpected bursts of sound that might overwhelm a compressor; but, after extensive testing, we found it a feature that should be selectable.

3-C: EQUALIZATION

Inevitably, we will meet unwanted sound within the speech passband, as noisome as that outside it. We wish both to have the capability to boost the level of speech, and tone down the level of speech-band noise, feats easily met by an equalizer, but one with special properties. The equalizers familiar to most home-stereo owners are called "graphic" equalizers. The frequencies they boost or cut are set by the design of the unit, usually at octave points (30 Hz, 60 Hz, 120 Hz, and so on up to 16 KHz). What if the unwanted noise lies between two of the equalizer's center frequencies? We must compromise by adjusting the controls nearest it.

But there exists another type of equalizer that lets us select the exact center frequency to boost or cut, and the width of adjacent frequencies affected, something related to an audio concept called "Q," an obscure notion it would cloud matters to discuss. Best that we refer to it as bandwidth to keep things simple. This other brand of equalizer is known as the parametric. Due to its infinite audio frequency span, we have need of far fewer bands than a graphic equalizer. A parametric equalizer with two or three bands can out-perform a one-third-octave graphic equalizer having 30 bands in this specialized arena. In most cases, we need zero in on only one or two noises to tone down, and on speech to boost. The parametric suits this to a tee.

Since sound energy below 300 Hz and above 3 KHz will have been filtered by the time the signal reaches this stage, the dedicated parametric should concentrate its effects from, say, 200-4000 Hz. Two or three independent controls covering this range should suffice.

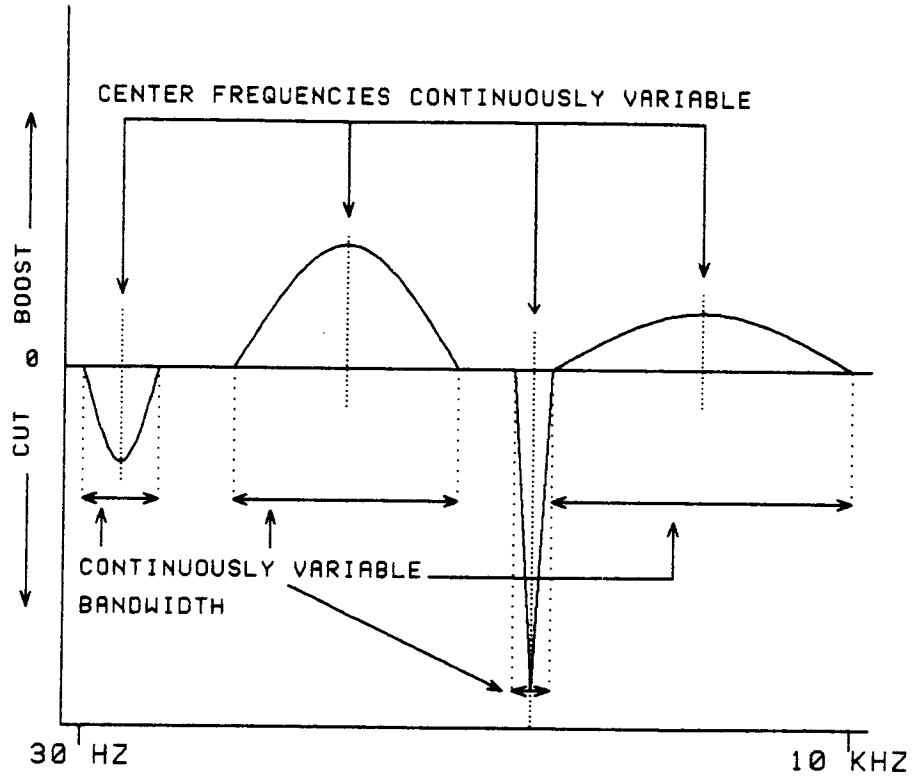
As for the parametric in action, let's say you have locked on to the target with your limpet bug stuck to the window. Speech passband filtering has attenuated 80 percent of noise, your compressor has kept dynamic range from lapsing into helpless depravity. Yet, the marks have set some manner of appliance, probably the refrigerator, right next to the window. Its monotonous whir lies well within the speech band, but is separate from voice-tones of your marks. First, narrow the bandwidth, adjust cut to max, tune in on the noise, then widen bandwidth to remove most noise possible without detracting from speech. Next, narrow the width of another band, crank up the gain, then fine tune the bandwidth to heighten speech signals.

These define the essentials of a dedicated spook amp. Other features qualify as desirable. We would like to be able to switch each processor in and out of the circuit at will. We would like not to have to drag out an impedance-matching transformer when switching from one type of mic to another. We would like for the unit to be able to process mic-level as well as line-level inputs without external attenuators. We would like to be able to drive a speaker, or headphones of either low or high impedance, and to have appropriate output jacks for line-level gear, such as a recorder.

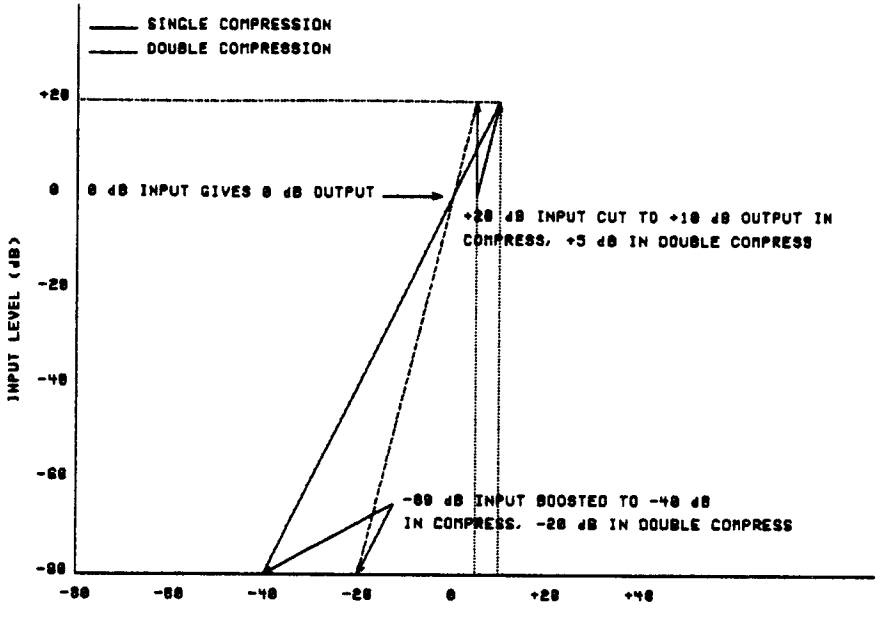
....all of which are easily built into the unit if factored into the design phase. Trouble is, few amps, at least among those we have seen marketed from an array of vendors, build all features into the works. It may be more profitable to sell this gear a la carte, which would explain it. Think about it long enough and money explains everything.

HEARING AIDS AND....

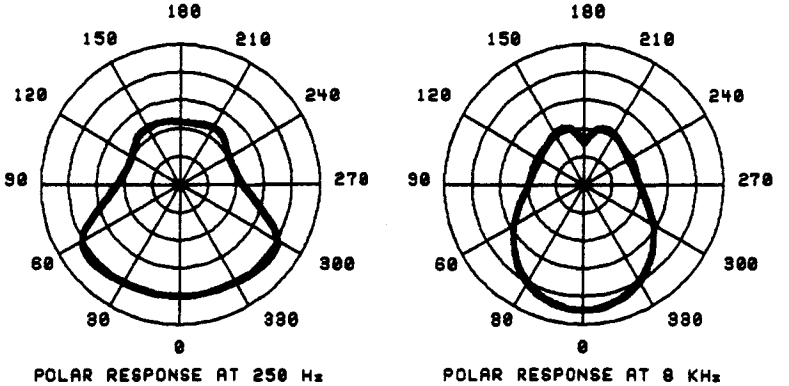
It came with little surprise that some of the meatiest material for the would-be snooper crops up in the literature of hearing loss and hearing aids. Audiologists, too, seek low noise, high gain, selective frequency amplification, compression (sometimes dual-mode and quite sophisticated), miniaturization, and application of digital technology to screen noise and enhance intelligibility.



TRUE PARAMETRIC EQUALIZER;
CONTINUOUSLY VARIABLE BOOST/CUT,
BANDWIDTH, AND CENTER FREQUENCY.
GRAPHIC EQUALIZER ALLOWS VARIATION
ONLY OF BOOST/CUT; OTHER VARIABLES FIXED.



GRAPH ILLUSTRATING EFFECT OF NEC μPC1571 DUAL-CHANNEL COMPRESSOR CHIP.
SINGLE COMPRESSION CUTS OUTPUT SWINGS TO HALF THEIR INPUT dB LEVEL,
FEEDING OUTPUT OF ONE CHANNEL INTO SECOND COMPRESSION CHANNEL
CUTS OUTPUT SWINGS TO ONE QUARTER OF INPUT IN dB (A LOGARITHMIC SCALE).
THE "IDEAL" COMPRESSOR WOULD PRODUCE A VERTICAL LINE,
WITH 0-dB-LEVEL OUTPUT IRRESPECTIVE OF INPUT. (GRAPH AFTER NEC DATA)



POLAR RESPONSE AT 250 Hz

POLAR RESPONSE AT 8 KHz

POLAR RESPONSE OF SHOTGUN MIC. NOTE DECLINING
DIRECTIONAL RESPONSE AT LOWER FREQUENCIES.
0 DEGREES IS "STRAIGHT AHEAD."

Truly, nothing new has sprung under the sun. Amplification For The Hearing Impaired quotes a galaxy of references. Digital sound processing exists in real-time, but not yet in portable, mass-market hearing aids (but soon).

Getting this industry to talk to you about applying its gains to surveillance...well...if they wouldn't talk to Popular Science, they wouldn't talk to us. It may be possible to pump an audiologist or hearing-aid vendor if he believes you are interested in hearing aids, rather than spook stuff.

Audiology keys in on what makes human speech intelligible. Vowels, most of whose energy concentrates in low frequencies, convey emotion. Consonants contribute most to intelligibility and content. Spectral analysis shows their energy peak in the treble range. Now, the most common form of hearing loss as folks age happens to be high-tone loss, where, coincidentally, the consonant sounds clump their energy. Distance, closed doors, and walls attenuate high more than low frequencies, too....

Next time you hear communications between aircraft or spacecraft and ground control, notice A) the peculiar qualities that immediately identify them as air traffic transmissions, and B) the extremely high intelligibility of the speech, even when the speaker mumbles.

—none of which happened by accident. Aircraft depend upon reliable voice communications. It comes as no surprise that much engineering has gone into the study of making speech intelligible under adverse conditions. First, it is frequency-limited. Second, it's highly compressed and sometimes clip-limited. A whisper comes through as loud as a shout, nothing overloads the transmitter by exceeding its input limits. Third, there is threshold activation of the transmitter such that all systems are muted when nobody's talking (this led to deletion of a snippet of Neal Armstrong's mini-speech when he stepped onto the lonely surface of the moon). Fourth, microphones and filter circuits reject ambient noise, such as the thunderous roar of rocket boosters.

Vendors of ham radio and CB peripherals have surrendered to temptation. They have marketed processors that fit between the microphone and the transmitter input. Now, these perform useful functions, such as compression and bandwidth-limiting; but some models lapse helplessly into a foul and loathsome indulgence by adding sound-effect generators, echo devices, and the like. Your good buddy on the CB can hear you as if you were standing on the edge of Echo Canyon; or you could zap him with your laser cannon sound generator as punishment for some degenerate pun. Hardly unexpected from a society that puts talking toilet paper on TV.

FOUR: OUTPUT (BETTER HOMES & RECORDINGS)

We can and often do monitor in real time, but most intelligence of any worth deserves to be archived for later review. That means recording it.

For fixed setups, open-reel tape is fading in favor of formats with both longer uninterrupted recording times and superior frequency response. VHS Hi-Fi, using T-160 tape and Extended Play speed, gives just over 8 hours of continuous recording per tape, near-digital quality. In many outlets these recorders sell for less than $400 and offer the freebie that, if the subject is under video surveillance, we can record video simultaneously.

Those with ultra-high fidelity taping needs might step up to Pulse Code Modulation, a true digital format with better dropout compensation than VHS Hi-Fi. Outboard PCM units can input to most any video recorder, and, at least until recently, some dedicated units had integral PCM capability.

Digital Audio Tape exists, but has snagged on coils of barbed wire strung by the folks who produce records and tapes. They claim DAT will allow duplication of copyrighted material in a form indistinguishable from the original. If DAT units are supplied with true digital inputs and outputs, they're right.

Digital inputs and outputs bear implications for security of our taped treasures. Wouldn't it be as easy as walking out before the end of Friday the 13th, Part XX to market an outboard encoder/decoder based on DES or a proprietary algorithm that would render confiscated tapes useless to those who grabbed 'em? Look

for it. Or, for an extra ten grand to cover a parts cost of $150, install an inboard unit, such that all digital recordings were automatically encoded, making them useless to any but the original recordist. (Studio analog masters of rock albums ready for the vinyl have been stolen. Rather than re-record the session, which took months the first time, the groups paid ransom. If the master had been digital, encoded, and a backup stashed in a secure cache—hey, no problem.)

Solid-state digital recorders that store and replay a few seconds of voice have been built into certain Japanese watches as a cute bell-and-whistle. The recently unveiled "Memo-me" records 16 seconds at high resolution or 32 seconds at low resolution, with an onboard memory of 512K. No moving parts, never any degradation of the sound, direct analog-to-digital conversion. The unit measures 5.6 x 3.2 x 2.3 inches, and from the looks of the conventional circuit board and components, could lose about 80 percent of its volume by substituting surface-mount devices and eliminating the built-in speaker. After all, bugs should be designed as record-only devices. "Memo-me" was available at press time for $69 in U.S. currency from: Computer Age Ltd., PO Box 730, Ontario, Canada, L0G 1N0.

The limit to such applications up to now has been memory; but with the 1 megabit chip a reality and 4 megabit chips on the way, it can't be long before we can record true digital sound for meaningful periods with this no-moving-parts technique.

Note the relationship between memory requirements and frequency response. To record to 20 KHz, we must sample at 40 KHz, preferably a bit above that. Given that the speech passband extends only to about 3 KHz, we need sample at only 6 KHz to give us that top end. The lower the sampling rate, the longer a recording we can store in a given bank of memory.

DIGITAL SOUND PROCESSING

Compact discs and the imminent DAT machines record by transforming analog signals into digital pulses. They reproduce the signal by the reverse process. Both formats employ error-correction circuitry that can interpolate between sounds otherwise lost from the datastream, whether due to damage to the tape or a sharp rap on the CD player. The best units conceal their work so well that we do not know when they activate.

And from that innocent revelation it is impossible not to extrapolate from music to speech, or to believe that this same error-correction technology could not fill in the gaps, as it were, in otherwise unintelligible analog speech recordings. Simply convert them to digital format and feed them through the processor.

But existing if expensive and/or classified digital processors can do much more. They can "remove" noise and echoes, filter, and compensate for changes in dynamic range in the digital domain, far better than analog technique. Note the alternative block diagram that factors in the power of digital signal processing. Even the analog portions of the chain change in response to computer command. True digital processing should, in theory, allow sound cancellation, interpolation and extrapolation of voices, automatic verification of truth, transcription, and translation from one language to another. Gear claiming some of these capabilities is listed in the CCS catalog, but the true state of the art in digital audio processing has not been made public. The NSA wants it that way. Like Lola, it usually gets what it wants....

On intuitive grounds, we can see that difficult bugging jobs, those that do not give us satisfactory audio from analog methods, demand a different approach, one that bypasses all processing in favor of digitizing the signal as early as possible. Once digitized, the signal can be recorded, dubbed to infinite generations without loss. Processing can proceed at a later date, under guidance of a supercomputer, to whatever level needed to pluck conversation out of the spirit-world.

MICROPHONES: DIRECTIONAL RESPONSE

We omitted one vital trait from mic specs: response pattern; that is to say, the output of the mic plotted in polar coordinates against direction of incoming signal.

When spook books speak of mics per se, they usually mean the mic element, rather than the completed device. Most elements are omnidirectional. Only placement in a properly configured holder endows them with directional properties.

A mic that responds fully to sound originating from any direction is said to have an omnidirectional response pattern. This proves desirable in some circumstances, but not those that call for us to zoom in on a target. Such mics have proven prone to feedback when used in public address work. Most find uses as lavalier mics (this gets awfully complex when we start talking about placing a mic next to a boundary, such as the wearer's body, since frequency response and polar pattern change).

A more desirable pattern has come to be known as cardioid, out of its heart-shape in the polar plot. It shows a null in response directly behind the mic, with a broad, even sensitivity sweep that semi-peaks to the front. Hand-held and stand-mounted mics use the cardioid pattern to best advantage out of their rejection of unwanted sound from the rear.

But some situations call for even greater rejection of sound to the rear and sides. The pattern has been dubbed hypercardioid. While more directional that the simple cardioid, the hypercardioid still leaves something to be desired in spook-level directional work.

The next step up in directionality is the supercardioid. Note carefully that it possesses no inherent amplification of incoming sound, merely rejects sounds coming from the back and sides, compared with those barreling in on the long axis. Think of it as the sound equal of a telephoto lens. The lens does not amplify light, merely captures a smaller segment of a scene.

If the supercardioid mic gives us only directionality, we must depend upon raw gain in the amp to let us hear what comes in, at least if we expect to hear better through the system than with the unaided ear. As gain rises, so do noise levels, even in the best amplifiers. Trouble comes when this parallel rise in noise cancels benefits of higher gain.

Finally, the most highly directional, non-amplifying mic is the shotgun, not the same as Popular Electronics' shotgun. This design is usually a single tube configured to eliminate resonances that would otherwise plague a unit tube. The diagram shows the polar response pattern of a shotgun mic. It rejects sound from the rear to the tune of 20 dB....

....but only at high frequencies. Look again at the diagram. Note that response at 250 Hz shows much less directionality than that at 8 KHz—and recall that the band we wish to hear spans only 300-3000 Hz, meaning that even the shotgun mic isn't as directional as its name or shape would imply. The same principle holds for parabolic mics. True, they amplify sound, but suffer the same drop in directional power as frequency falls below 8 KHz.

DIRECTIONAL MICS IN PERSPECTIVE

What percentage of audio intelligence is gathered by directional microphones compared with that gathered by bugging or wire-tapping?

Not much, by the look of things. Yet this fiendish tool, the mic that hears at a distance, fascinates enough people that directional gear has proven a perennial favorite. Space ads in magazines cost a great deal of money. From the persistence and pervasiveness of ads for hand-held microphones/amplifiers, with and without directional capability, there has to be a hefty market for them just to defray the cost of hype. Recent prices for outwardly similar products range $50-$130. Some incorporate a small (5" or so, by the look of it) reflector. While clearly less conspicuous than a full-size 18" dish, whose effectiveness in a properly executed design no one denies, we have to ask: Who buys these things, and for what do they use them?

The ads themselves are nebulous as to purpose; some perhaps unintentionally comic. As everyone knows, it is illegal to use a directional listening device to tune in on conversations of persons at a distance without their knowledge and consent.

BUGS

Relax. We aren't about to re-catalog all modes of bugs and bugging, merely hit a few spots that have caught our eye of late and which mirror an evolving technology. You'll find deep profiles of tape recorders, contact mics, assembled transmitters, and the like in references cited elsewhere in the book.

LIGHT TRANSMISSION OF SOUND: THE IR LED BUG

Those who build an effective RF sniffer learn quickly why it has remained the staple of the debugging trade since bugging via transmitter began. The sniffer picks up conventional RF bugs too easily. Once the target suspects he has been bugged and runs an RF sweep, the odds approach 100 percent a sniffer will lead him to the transmitter, which has your prints all over it, not to mention microtraces of your DNA if you built it yourself....

Although the dread laser bug has drawn greatest press, other light-reliant methods require less sophisticated and costly equipment and do not depend on the vagaries of windows. Nor do they betray themselves with ugly RF pollution. For example, take the infrared diode bug. A standard mic inside the target premises feeds a small preamplifier which, in turn, modulates the output of an invisible infrared light-emitting diode mounted discreetly outside the premises. A snooper need only know the location of the diode to lock in on it with a simple optical device equipped with an infrared detector, usually a phototransistor, that yields crystalline audio.

This type of bug comes in portable units about the size of a box of matches, designed to be placed at a window; yet these seem too obvious if discovered. Relying on battery power, they die after a day or so. A potential improvement would mount a solar cell on each side of the unit, to charge a nicad battery that would keep the mic going overnight. Who knows how long such a thing might remain active?

The simplicity of IR technology happens also to be responsible for the now-universal infrared wireless remote control devices, as well as recently introduced cordless headphones and speakers. The circuitry has been reduced to a pair of chips. The 1989 Radio Shack catalog lists an IR detector with built-in amplifier, limiter, bandpass filter, comparator, and integrator (part# 276-137; $3.49). It's the type of component whose power fairly begs for lewd abuse in surveillance work.

Straight audio modulation of IR intensity and use of a receiver that keys on these gross changes subjects the device to noise. For example, either fluorescent or incandescent lighting drowns light-sensitive viewers with 60 Hz hum. The solution to that problem lies with use of a carrier signal of tens of thousands of Hz on which the audio is frequency-modulated. The analogy to AM and FM radio is crude, but gives an idea of the reduction in interference and noise to be had with this technique (commercial cordless headphones and speakers use it). Natch, it bogs down the circuit in extra parts, and the operative must sometimes choose between size/power requirements and performance.

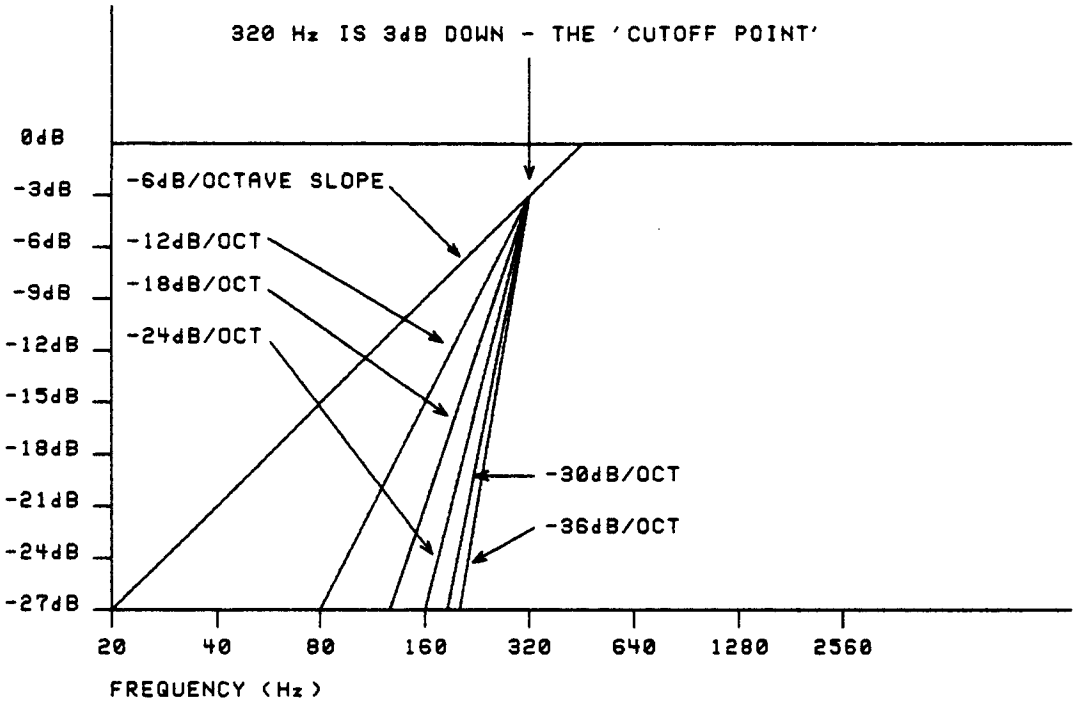
Infrared light shows up on infrared viewers, making a nocturnal IR-scan of the exterior of the premises part of a truly professional debugging sweep.

Incidentally, this type of setup lends itself extremely well to mounting behind an AC wall socket, where it can gulp all the power it needs, enough to power an IR laser diode if need be, perhaps visible to trained watchers from miles, and remaining active indefinitely or until the power company cuts you off....

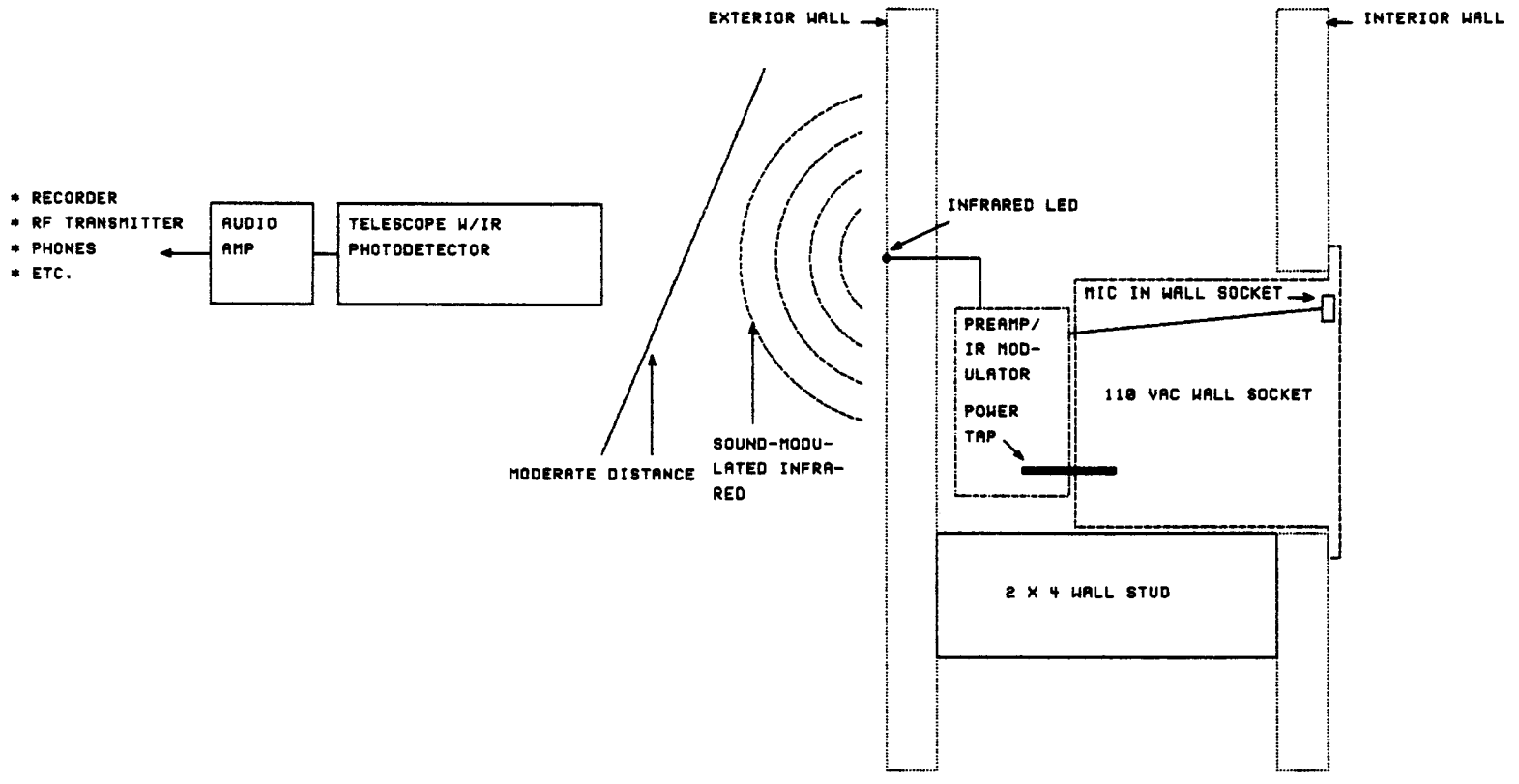
THE LASER LISTENER (SO WHAT ELSE IS NEW?)

Considered exotic a few years back, the laser bug graced the cover of the October, 1987 issue of Radio-Electronics in build-it-yourself trim. With a laser and about $25 worth of electronic parts the hobbyist can build an unsophisticated but working laser bug. R-E kindly granted permission for us to reprint the schematic. The discussion below of Dirijo Corporation bears on certain thematic aspects of laser bugging.

The principle must by now be known to all, but to summarize for those naive to it, laser light possesses the



EXPANDED SCALE SHOWS SLOPES OF DIFFERENT HIGH-PASS FILTERS CUTTING OFF AT 320 Hz



INFRARED TRANSMITTER BUG

property of coherence. Stated another way, it's light of a single wavelength, marching in step, as it were. Sunlight and other sources of white light contain the entire visible spectrum, as passage through a prism will show.

The laser's special properties that suit it to bugging lie in its near-inconsequential divergence over vast distances; power, which enables use at those distances; and invisibility in the case of infrared and ultraviolet lasers.

We have seen that one bugging method calls for an audio signal to modulate the output of an infrared diode. These changes in intensity can be picked up at moderate distances, demodulated, and processed as desired.

But the IR bug is active in the sense that it demands a mic inside the target premises, or at least a limpet mic hugging the wall or window. The laser bug is deemed passive because all working components lie outside the target.

Laser light bounces off surfaces. A thin, highly reflective mirror modulated by the voices of targets would make the ideal reflector, but we find few such surfaces accessible to the deadly beam. Windows have been primary targets out of their reflectivity, thinness, and outside visibility.

We beam the laser at a window. Since the window vibrates as the pigeons inside speak, reflected laser light carries these modulations. We detect the reflected light with apparatus similar to that used for the IR bug, and demodulate the signal to extract the audio.

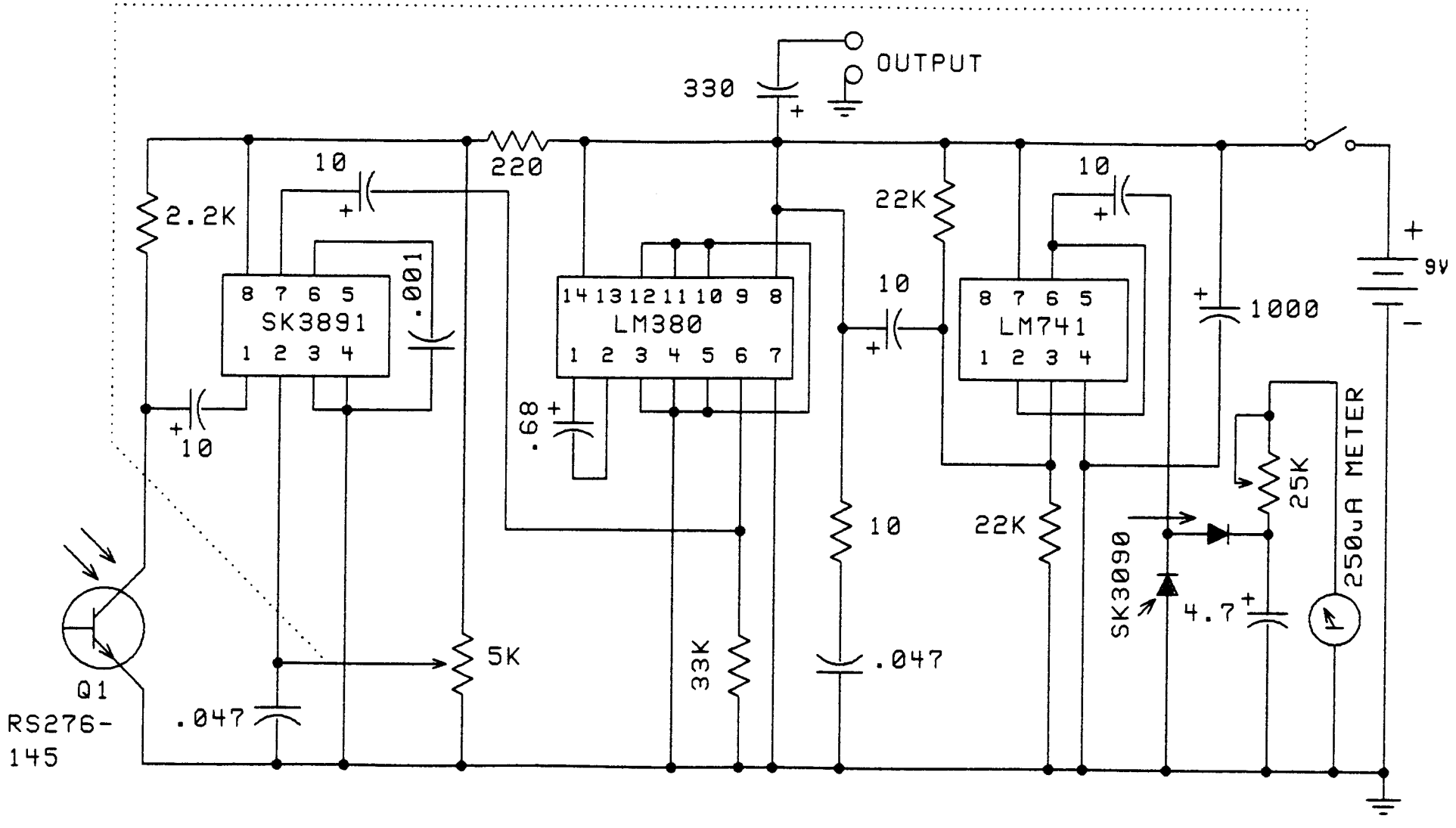
Angle of incidence can vary widely without degrading performance. The laser source could be mounted one location, the receiver at another, though finding the beam poses problems. Ideally, laser and receiver mount coaxially on a single unit, but this limits the angles from which we may shoot the target window to near-perpendicular in two planes.

Use of a visible laser at night carries risk if the target is familiar not with laser listeners, but with laser sights used on guns. He may spot that telltale red glow on the curtain and take you for a sniper. And who knows what breed of executive action that might prompt?

Experimenters would be advised to begin with visible, low-power lasers, always bearing in mind that even these can cause permanent eye damage. (Experimenting with lasers is a craft unto itself, with safety precautions for experimenter and bystanders, special goggles to buy, and the like. Master laser safety before trying the bug.)

The laser bug has been around long enough to have seen several sinister refinements. First, it's been found that window-glass is by no means the only surface that will suit the needs of the principle. Shiny objects inside the house can offer better reflectivity, and are less likely to be screened with white noise generators attached to them. Second, surfaces not ordinarily considered reflective have proven adequate for laser listening—walls, doors, and so forth. Third, we need not limit the technique to fixed structures such as houses or offices. Moving cars, reflective objects near marks engaged in conversation, and so forth have been targeted, though techniques involved lie beyond the financial reach of hobbyists. (Hint: For years, the military complained that the major roadblock to genuinely effective laser weapons lay with lack of an aiming system that would fix the beam in situations where both target and laser were moving. Airborne lasers have downed incoming Sidewinder missiles aimed at them. Breakthroughs in aiming high-power lasers could just as readily serve eavesdropping.) Fourth, in theory, the laser bug will work at frightening distances. One of the first experiments conducted with lasers bounced the beam off the moon. A range of several miles with Class IV (i.e., powerful) infrared lasers should surprise no one. We have to wonder whether this equipment nestles aboard our latest generation of spy satellites, to track conversations inside cars with a beam bounced off the roof. Digital audio processing has expanded the laser bug's potential by eliminating former noise obstacles.

To counter the laser bug, several firms market white-noise generators designed to stick on windows at risk. They modulate the window just as any sound would, only more strongly, making it difficult but not impossible to extract conversation.



SCHEMATIC OF LASER LISTENER, DESIGNED BY RICHARD PEARSON, WHICH APPEARED IN THE ARTICLE "LASER LISTENER" IN THE OCTOBER, 1987 ISSUE OF "RADIO-ELECTRONICS" MAGAZINE.

The letters column of Radio-Electronics, November, 1987, printed commentary from Forrest Mims III, a well known contributor to the electronics field (and, we learned through research for the rocket section, an innovative model rocketeer). He felt that R-E should not have published Richard Pearson's laser listener project in an article that allegedly encouraged illegal use of such a unit. Mims related that a newspaper had approached him in 1976 to use an infrared laser to bug Howard Hughes' suite atop a hotel. He stated that the paper had convinced him that Hughes' conversations might give evidence of illegal activity, but complained that the paper failed to tell him (Mims) that bugging in that manner was illegal. Few who've read this man's work doubt that he could have pulled off the feat, even back in '76. Due to missed connections the deal never went down. Other readers advised the editor that, while they agreed that certain knowledge could serve nefarious ends, they wished to stay informed, and applauded publication of the article. It is perhaps fair to say that some statements in or pointing to Mr. Pearson's article were suggestive, but that reasonable men could not conclude beyond doubt that they encouraged illegal conduct.

The author admits readily to a helpless naivete when it comes to electronic engineering, but even he cannot help but note that no laser listener circuit he has seen to date takes advantage of genuinely low-noise technology. The LM380 audio amplifier IC used in Mr. Pearson's circuit offers a S/N ratio adequate to portable radios and such, but preamps and op amps available in the past ten years eclipse its noise figure by orders of magnitude. Those amps coupled to progressively quieter infrared phototransistors should in theory enhance the LL's range and fidelity. Perhaps circuits printed to date represent sops tossed out to satisfy our curiosity and blunt the urge to improve.

TRANSMITTERS...AND WHAT THE ADS DON'T TELL

TRIMMING THE ANTENNA

Love, hate, and the fact that RF transmitters require power and antennas have found a place among universal human truths. The particulars do not see much space in ads for spook gear, though. Messy details detract from sales.

Spook transmitters are short-range devices, necessarily so in light of their unlicensed status and the fact that too much power would let innocents within a several-mile radius tune in on the conversation, if they happened accidentally to lock on to the signal.

This shortage of power leaves no room for error in configuring the device. Once the experimenter has selected a frequency, either by crystal tuning or adjustment of a variable capacitor, he must (or should) tune the antenna, a process known as "pruning."

Most spook gear uses a simple "pole" antenna. This can be a collapsible type, or, most likely, a strand of thin, insulated wire. Note that the length of the antenna should bear a special relationship to the wavelength of the frequency being transmitted. Ideally, they should be equal, but this is seldom practical with gear working below UHF band. More often, particularly for gear transmitting in the 108 MHz region, lengths half or a quarter of the wavelength perform best.

Now, it is possible to calculate antenna length working from frequency, but these calculations do not automatically result in a perfectly tuned antenna. Experience has proven that pruning offers significant gains. To prune an antenna, you must have access to either a field-strength meter or an RF sniffer easily built for less than $20 and quite sensitive. (In fact, the first piece of gear the beginner builds should be a reliable RF sniffer. In addition to avoiding legal hassles, it acquaints you with circuit boards, soldering, and facilitates later setup of RF senders that might or might not be legal....)

Power up the transmitter and the sniffer. Adjust the sniffer such that it reads about half scale when placed within easy view of the transmitter.

The antenna wire should be a few inches longer than its calculated length, whether quarter- or half-wave. It should hang as near to vertical as possible. Orient the sniffer's antenna vertically also.

Begin snipping off quarter-inch bites from the end of the antenna wire. Watch the meter as you go. When the

meter begins to show a stronger signal, cut the bites to an eighth of an inch. It may be necessary to lower the gain if the meter goes full-scale. When a snip gives a barely perceptible drop in signal strength, the antenna is tuned....

....at least for that set of circumstances. Environmental changes can detune the setup. For example, if you tuned a transmitter designed to be worn on the body this way, it would probably lose some of its gain when worn because proximity to the human body alters capacitance critical to tuning. The solution calls for antenna-pruning while a subject wears the transmitter.

Proximity of metal objects to transmitter or antenna can make a huge difference in signal strength. If surrounded by too much ferrous material, transmission may be blocked altogether. (Take a look at the metal backing that holds the punch-down block, discussed below. Although it's the perfect spot to secrete a transmitter, the antenna wire has to go somewhere not blocked by metal to send its now-detuned signal.)

Beware that once you have tuned the antenna for a set frequency, it would not do to let the frequency drift. Crystal-controlled transmitters suffer least drift, but happen to be the most expensive and least often built by hobbyists. The variable capacitor tuning method is especially prone to drift. Many pros who use this brand of gear lock the capacitor in place with a drop of epoxy, wax, or hot-melt glue after selecting a frequency but before pruning the antenna.

It goes without saying that the antenna should hang as near vertical as possible, and sit as high as practical, since these factors—proper orientation and height—give maximum range. Thin, multi-stranded wire handles more easily than single-stranded wire of the same gauge.

RECHARGE IT

Efficiency of solar cells continues its climb. It has reached the point that several firms market units designed to keep nicads charged in portable electronic gear. The concept fairly begs to be applied to surveillance devices that would otherwise die after a day or so. Check out the flyer from Sovonics[tm] Solar Systems, Box 1101, Southgate, MI, 48195. Send them a SASE.

REPEATERS

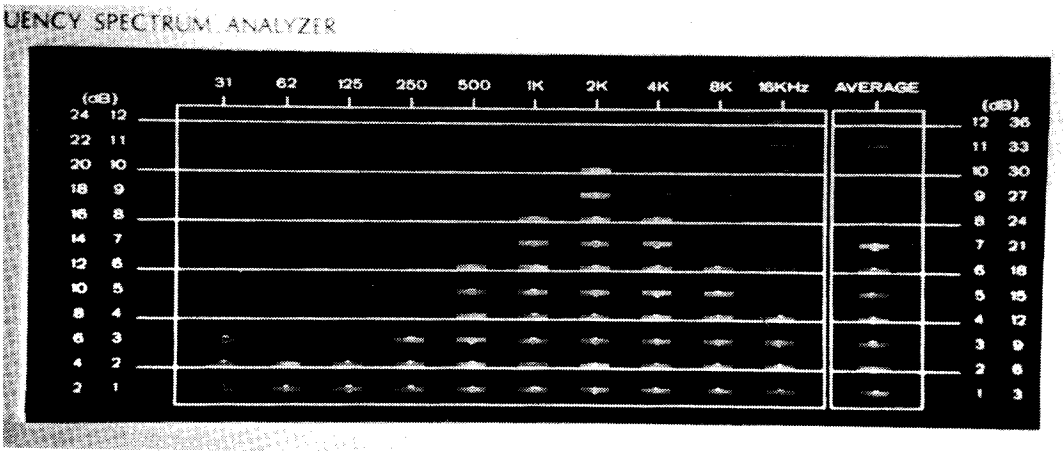
Gear that hobbyists build transmits most often in the 108-109 MHz region, accessible to FM radios. For reasons noted above, power has to be low or the world knows your game, since most of the world owns an FM radio. Far fewer geeks own CB radios, though enough to make transmitting on standard CB frequencies chancy as well (and more likely to bring in the FCC, whose computerized direction-finding gear is the envy of the trade).

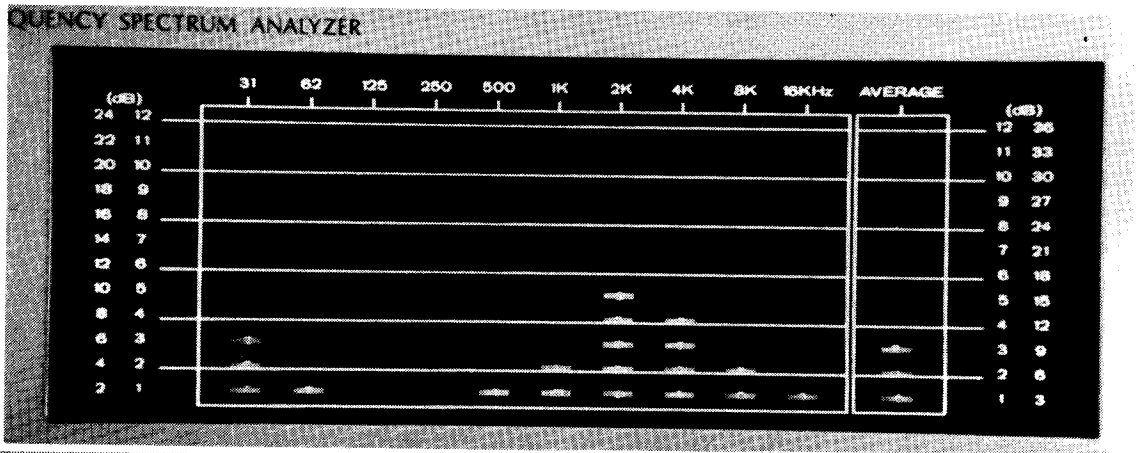
Hobbyists, under determined tutelage of veteran spooks, have been sold plans to build repeaters. A repeater receives a radio signal on one frequency and re-broadcasts it on another. The principle has found use all over the United States for years. Police departments, ham radio operators, and cellular telephone equipment use it.

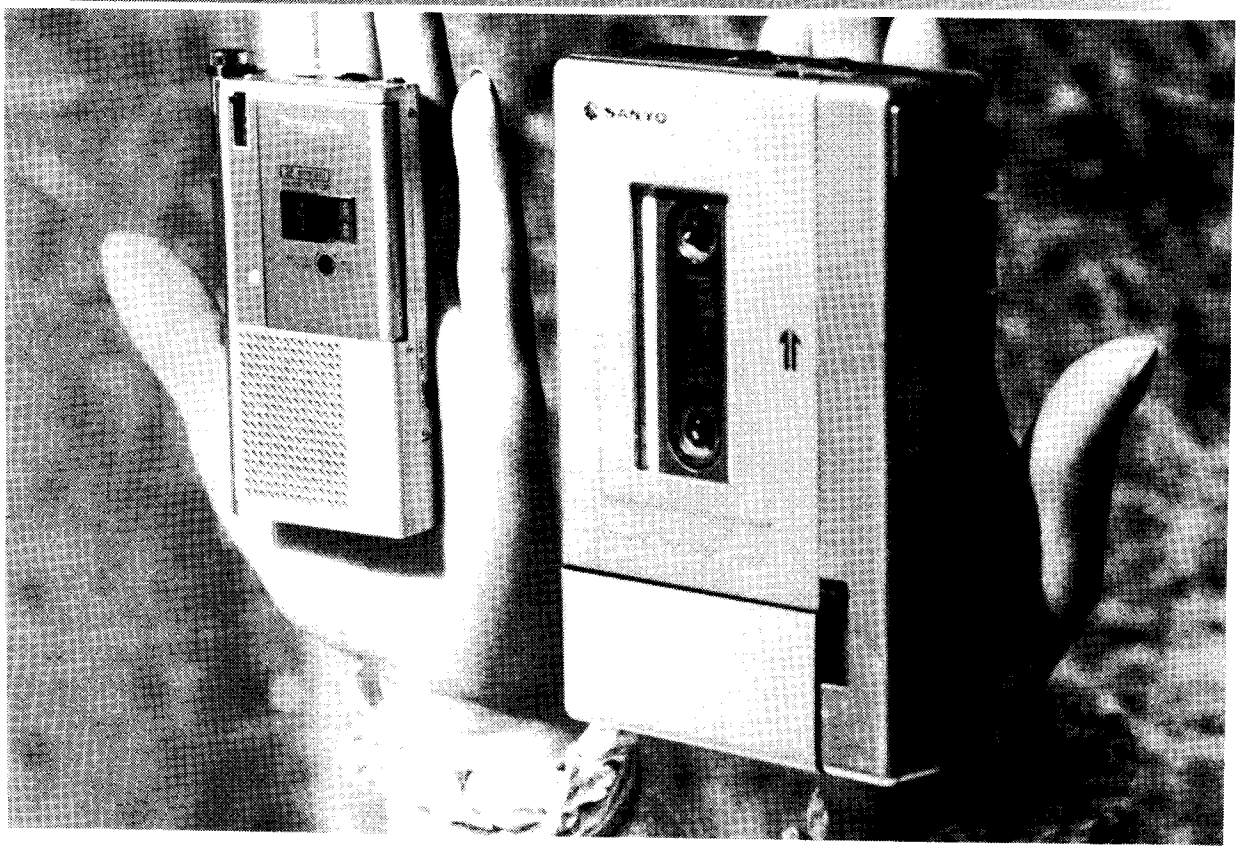
Spook repeaters, at least at the hobbyist level, typically receive 108 MHz signals and rebroadcast them at higher power on crystal-controlled gear or equally stable frequency-synthesis units that have been detuned slightly, such that a standard CB receiver will not lock onto the signal unless it, too, has been detuned. This technique adds blocks to miles to the effective range of an RF bug and is quite illegal.

THE ETIQUETTE OF WEARING A WIRE

The author has always felt a fondness for the Panasonic RN12. Selling for about $175 in 1985, measuring only 9/16" x 2-1/8" x 4", weighing mere ounces, and running quietly enough for field use. It goes at least 2 hours continuously on a set of fresh alkaline batteries, or, in the model the author tested with two different brands of nicads, 1.5 hours on them with a fresh charge.







TOP: Noise spectrum of Panasonic RN12 tape unit recording in dead-quiet room w/mic attached. MIDDLE: Same setup w/mic detached from unit. Note dramatic drop in noise level. Scale is 3 dB/division. BOTTOM: Delicate left hand swallows the tiny RN12; recorder using standard cassette in right hand.

Wearing a wire always involves a gamble, since the mark may be wearing gear that detects either the bias oscillations thrown off by the tape recorder, or an RF sniffer, or a combination unit. Such units let the wearer know without letting you know that he knows. They signal by means of a small, silent vibrator; or, in desktop models, with discreet flashing of an LED. (Crude models use an audio tone sent through an earphone. Beware of persons under the age of sixty wearing "hearing aids." If they're wearing aviator shades with the earphone and look like the athletic type, they're feds....)

TAPE RECORDERS

Scan the pages of any finished-gear discount electronics catalog. Odds are, it will feature a flock of microcassette tape recorders tiny enough to slip in your inside jacket pocket, in a ladies' purse, even in your front shirt pocket. From this vantage it can record face-to-face conversations handily from a built-in mic. Simple, no?

Actually, it isn't quite that simple. Details separate success from failure in all walks of life, and so it goes with wearing a wire.

Dry runs are essential. They tip you off to so many potential problems easily corrected once you know about them. Take externally audible noise, for instance. It would not do to have the mark hear that telltale whir of the motor. It could lead to embarrassing questions that undermine your, ah, credibility....

If tape transport noise proves externally audible, you'd better believe that an integral mic is not only picking it up, but it may overwhelm the conversation. A crude audio spectrum analyzer illustrates this graphically. The photo-pair shows the output of recordings taken in a dead-quiet room, using the unit's integral mic attached (a Panasonic RN-12), and that same mic detached from the unit. Note the dramatic drop in noise levels. (A third reading from bulk-erased blank tape showed near-complete absence of noise, at least relative to that produced by the recording process alone in this small unit.)

The RN-12 comes with a sensitive, detachable mic, complete with tie clip, though not the smallest we have seen. Make a test run with the mic detached but placed in the front coat pocket. Note the overwhelming rustle of fabric every time you move, even breathe. In this position the mic gives good recordings only if you remain rigid and breathe shallowly. We obtained somewhat better results in a serious run using Radio Shack's "credit-card-size" mic. Another advantage of using a separate mic is that it allows you to place the recorder somewhere less likely to betray itself. Your side jacket pocket, even a rear pants pocket. The author taped a sensitive conversation that way once. He had to punch holes in the armpit of his shirt and jacket to get the mic wire back around to the recorder, placed in his left rear pants pocket. Operation of the unit was inaudible, but it would have been embarrassing to have been asked to remove his jacket....

How long will the conversation last, and what will your unit do when it reaches the end of tape? Will it surprise you with a beep? Best to find out these things in advance. First, as to length, with unmodified units, we can record forty-five minutes at standard speed (2.4 cm/sec) or an hour and a half at half speed (1.2 cm/sec), without turning the tape over. Double these times for units equipped with auto-reverse, but test the auto-reverse to be certain it works inaudibly.

Tests will show that slow-speed fidelity is dreadful but usually intelligible. When you cannot gauge the length of the conversation in advance, best to use slow speed. High speed offers better fidelity, nothing near that of recorders that use standard-size cassettes. Those units bear the onus of size, though the gap has narrowed.

It goes without saying that the unit will run on batteries. Best that they not fail during the interview. Use only fresh alkaline cells. Burnish their contacts as well as the contacts in the battery compartment. If you are not sure they will drive the recorder for its maximum operation time, test a set before going into action.

You will note from early test-recordings an annoying, boomy quality to speech. Mostly reflected sound reaches the mic, which explains the boom. It is also a push for using a pressure-zone mic if possible, since this will reduce the boom.

VOICE-ACTIVATION CIRCUITRY (VOX)

VOX units start the recorder only when they "hear" conversation loudly enough to trigger them. They save tape, and in many cases it is impractical to use a recorder without a VOX, out of limited tape capacity. But the inertia inherent in tape-transport mechanisms means that VOX units lose starts of most phrases. If tests show the lag to be inconsequential, fine; but do not rely on the VOX without first testing its delay.

AUTOMATIC LEVEL CONTROL

In experimenting with the NEC uPC1571 compander chip, the author configured it both as a compressor and as an automatic level control per circuits supplied by NEC. The distinction sometimes blurs, since a fast-acting automatic level control will in essence compress the signal. That observation aside, note that many high-end compact tape recorders feature automatic level control as a bell-and-whistle, just like VOX. It's a good feature to have, and both ALC and VOX are available without resorting to dedicated spook gear.

WEARING A TRANSMITTER

Much the same advice about tape recorders applies to wearing a transmitter: dry run, check the batteries and range, etc. Transmitters aren't suitable for locales where you might walk out of range, unless a cohort shadows you with the receiver and recorder. Generally, they are iffier than portable recorders, cost considerably more in reliable trim, and demand more attention to detail than do portable tape units.

TELEPHONE SECURITY IN THE AGE OF CORDLESS PHONES

Until lately, there was no security when using these devices. The author has picked up one side of a cordless phone's duplex transmission on a plain FM radio. The voice was buried in a high-pitch howl, abrasive to hear but fully intelligible, apparently an unsuppressed harmonic of the 40-50 MHz range common to these units. On the other hand, maybe he intercepted the transmission of a sloppily designed bug....

These phones use separate channels on different frequencies, a setup known as duplex. Usual frequencies span 46 to 49 MHz. Ordinary scanners can receive the channels. A bugger need only know the make of the phone, check with the manufacturer to see what frequencies are being used. Or use an RF frequency counter. When it detects radio waves, it displays the frequency.

The latest phones automatically select among ten channels for clearest communication, something akin to so-called diversity systems used in high-end car stereos and professional wireless mics. This adds a degree of security, since selection cannot be predicted and changes constantly, though not in the same manner as dedicated frequency-hopping units. Southwestern Bell has introduced its model FF-4500 with built-in scrambling capability, though not DES-level. Still, it would require dedicated effort to intercept and descramble transmissions that both hopped about a spread of ten frequencies and sounded like Donald Duck stoned on Seconal. These features are long overdue on consumer products blithely assumed to offer privacy.

Cellular telephones present an even nastier problem, since everybody with a scanner can tap into them, either at their unit frequencies or at repeater frequencies. Cellular phones have become scary status symbols in this terrible era. One mailorder firm marketed a stick-on dummy antenna that looked like it matched a cellular phone, for about $20....

Scramblers based on DES are available on business-band and public service transceivers costing several thousand dollars. The transmissions sound like hiss and are secure to attack by non-governmental foes, at least for the time being. Either get a compatible receiver and today's code, or bug the car.

PHONE BUGGING

TAPPING THE OFFICE LINE: THE PUNCH-DOWN BLOCK

Assume for the moment that we will not be using inductive pickups or other iffy connections; that we will make direct contact with "the pair" as it's known in phone company jive. Short of tapping in on the pole, or the nearest junction box, where and how do we proceed?

Any number of attack points. First, in modular systems, if you can get to a wall jack, simply remove it and hook your clips onto the proper terminals (green and red color-coded). For the single-line phone, there will be only one pair. On multiple line phones you must decide which is likely to bear juiciest fruit.

For businesses, though, you will need to know about the punch-down block. This seems to be the universal interface between the phone company's lines and the user's. The photos show a typical example.

Note several points. First, wires are color-coded, with a sample being "line-1," which in all commercial and telco setups we have seen consists of the white wire with blue stripes and the blue wire with white stripes. The left side is the company side, the right side of the block is the user's. The two lugs on the left are connected internally to one another, the two on the right are connected to one another, but the left and right pair are not connected. To make contact, to make the actual connection between company and customer, the installer applies a bridge or clip across the inner pair of lugs, shown in the photos.

Now, if your design required interposition of the unit (a series bug), you would remove the clips, then attach your break-out using alligator clips or whatever (though we will see momentarily the better, chameleon's way to do things). Parallel bugs need no break in the line.

A "pair" consists of tip and ringer, but polarity makes no difference with most types of bugs.

In every installation the author has seen, the pairs always run from the top down: the first two wires, vertically, form the line-1 pair, the next two line-2, and so forth. Color codes for the first 3 lines of a "standard" system are blue/white, orange/white, and green/white; that is to say, the first pair consists of a white wire with blue stripes and a blue wire with white stripes; and so on down.

It takes little diligence to spot a pair of alligator clips clamped to the works, as in the parallel bug in the photo. Isn't there an easier way, a way that will escape casual inspection by even the phone company?

Of course. Attach your device using wires that match the color codes for the pair you want, and instead of using clips, simply use the punch down block. A telco employee could spot the extras quickly, if he is looking for them, but they will escape the casual glance, and non-telco personnel haven't the foggiest as to what wires belong and what don't. Where do you get color-coded wire? Purchase a length of cable with at least one Amphenol[tm] connector on the end. Strip off the insulation, and inside you will find these same universally color-coded pairs.

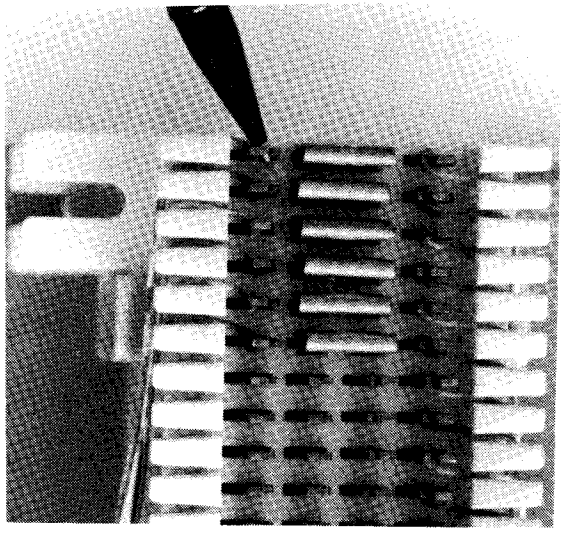
To do it in a genuinely professional way, you will need a special tool. It punches the wire down to the bottom of the clamp, strips a bit of insulation, then clips it off as neat as you please, all with one crisp stroke.

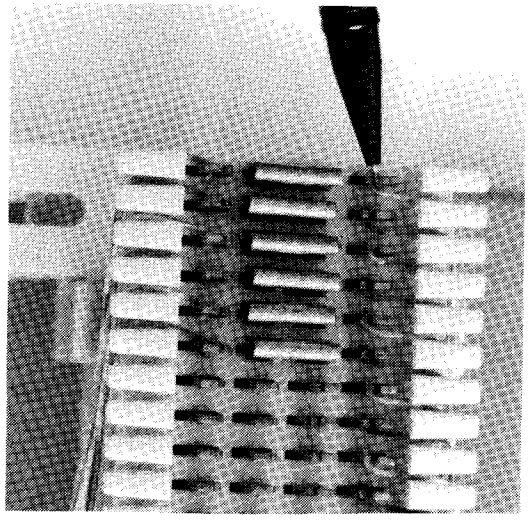
And it costs only $23 from Jensen Tools (7815 S. 46th St, Phoenix, AZ, 85044; 1-602-968-6231). But what's $23 compared to detection of your gimmick? The author once used a screwdriver in lieu of the special tool to install his own 3-line business phone system, including intercom and many extras. He found that the screwdriver left more than 10 percent of punched-down wires unconnected. These then had to be traced and manually stripped. Take it from one who has been there, that stiff price of a punch-down tool is worth it if you will be doing your own, ah, installations....

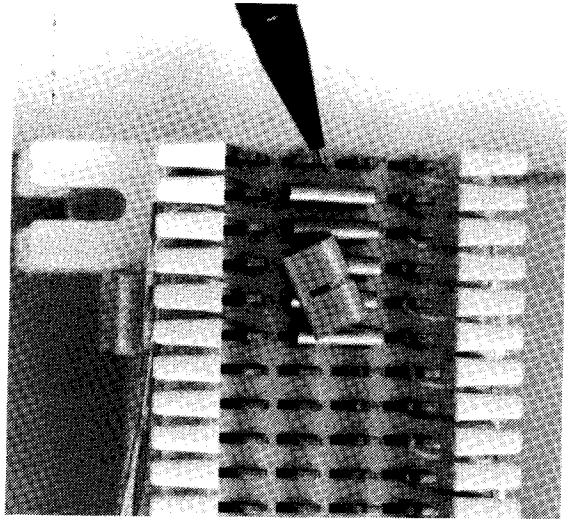
An alternative involves removal of the two large screws that hold the block to the mount. This offers extended access to that tangle of wire behind the block. Here the color coding helps enormously. You can tap in, parallel or series, in a region ordinarily hidden from view. An inductive bug might run into problems if several lines were in use simultaneously, though, but might offer the freebie of tapping into pot luck from a single bug.

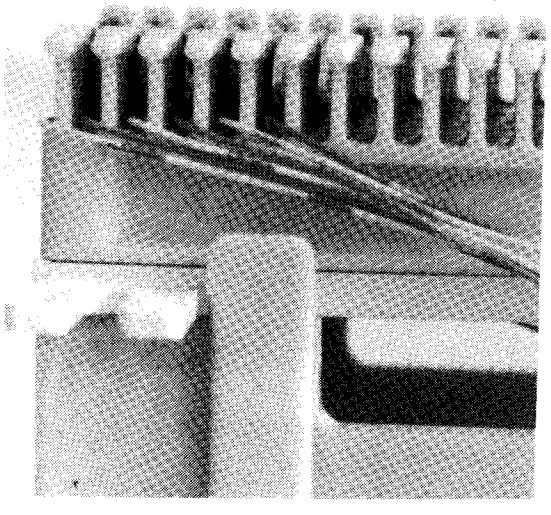
If you want lines 1 through 4, they are easily spotted by location and color coding. In more complex systems, as found in offices with 20 lines or so, you will have to identify the correct pair. This can be done in a number of ways. The oldest is to buy a phone company handset and systematically attach clips to pairs until you get the right one (it helps to have an assistant talking on the line; otherwise, the method is impractical).

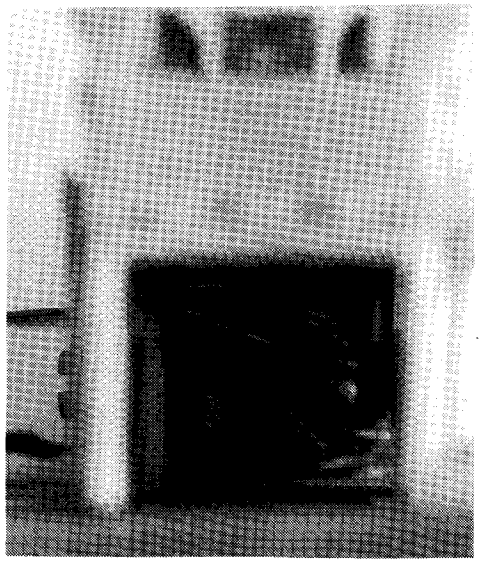
Several companies make equipment that sends a pulsing tone through the pair, sometimes audio, sometimes

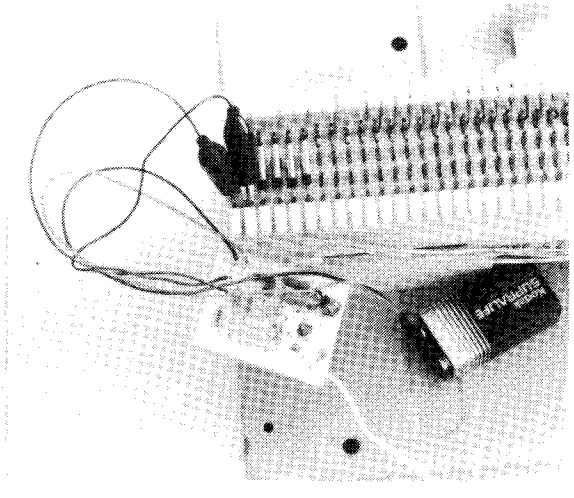












DETAILS OF THE PUNCH-DOWN BLOCK. TOP LEFT: Pointer on telco side. TOP CENTER: Pointer on user side. TOP RIGHT: Clip removed. Left pair and right pair are internally connected, but the two pair are electrically isolated, hence need for clip to make contact. BOTTOM LEFT: Telco side shows color-coded wiring as described in text. BOTTOM CENTER: Looking down into the maze of wiring behind the block. Color-coding makes it easy to get your chosen "pair." BOTTOM RIGHT: Experimental parallel transmitter connected to punch-down block. Transmitter no longer exists, and certainly wasn't used for bugging....

RF, that can be picked up by the operative in seconds, thus saving considerable time. John Wilson markets plans for a device that will not send its signal until you "tell" it to do so from your site at the block, a feature that enhances security. (Think hard. You are on the premises installing a bug, for chrissakes. That's a felony. You need all the protection you can get.)

It wouldn't hurt to inspect the block in your own office once in a while, would it....?

* * *

BUILD OR BUY?

Spookdom has evolved dichotomously, split like the rest of the world along lines of wealth. We have amateur gear that serves handily for most operations, and costs only the plans and parts. And this is only what's advertised. One professional engineer told the author that he "keeps the good stuff in the closet" in any case. Since his hobbyist plans are among the best to be had, it gets scary thinking what this man has cooked up for clients he asked us not to name....

DO-IT-YOURSELF: THE FINAL FRONTIER

Assembled gear of medium-to-outta-sight price has seen wide exposure in spook literature. A dedicated look at the plans market has been lacking.

At the deep-pockets end of the spectrum, we have the government—it dips as deeply as it wishes into our pockets—along with foreign governments and gaggles of extremely well heeled private rogues for whom money means little, but the notion of security holds worth. Touring devices accessible to them is like turning a kid loose in a toy store where everything is free.

Selection depends on your objectives, expertise, and budget. For those with no prior experience in electronic circuit design, and that includes most of the populace, and assuming an average budget, best return on time, money, and effort comes from building circuits designed by pros.

For modest cost—roughly $5 to $25—one can purchase plans for (potential) bugging gear, as well as debugging and audio processing circuits. Most vendors sell plans only, while others sell plans, parts, complete kits, and in some cases, assembled units.

The cost of making this gear varies, but, with a serious connection to one of the larger electronics suppliers, or dedicated hobbyist suppliers, one can build devices that out-perform slickly packaged merch selling for hundreds, even thousands, of dollars. (In one case some years back, a vendor sold plans for an RF-detector that flat shamed units a debugging supplier was foisting on Uncle Sugar for more than ten grand a hit. The vendor naturally sought to capitalize on his splendid plans and put the readily proven facts in his ads. The result was to call forth a shirtload of rancor, with ugly overtones of menace and heavy elements of ill will. Those who know Who's Who in countersurveillance engineering, and the system that turns $20 worth of parts into $500 worth of product, do not doubt this tale, which we happened to get straight from the horse's mouth....)

The point being, don't discount the performance of gear you assemble yourself. It lacks the panache of custom labels and enclosures. But it works.

"Companies" selling plans are in most cases one person, which is no sin. Free enterprise spawned this book. The person has usually not set out to become a designer of hobby electronics gear, but gathered the know-how through other avenues, such as professional engineering; saw an opportunity in the pages of electronics publications, whipped up plans, and marketed them.

Note that it is illegal to sell completed surveillance units of most types. Selling plans only, or at most a kit, stays on the lawful side of the fence.

When choosing a device, let's say and amplifier or transmitter, it is wise to check the length of time the

company has been around, their reported experience, whether they offer follow-up or other help after the sale.

Kits with all parts, and most important, an etched and drilled printed circuit board, will save many headaches. Matching components on perfboard to a schematic diagram has brought on many a migraine.

KNOWLEDGE FOR SALE

These five profiles sample what's current in the knowledge market. We chose a combination of vendors whose emphases tend to complement one another:

PANAXIS

Offering plans and kits since 1975, Panaxis Productions, under the tutelage of Ernest Wilson (no relation to John) has grown into what is probably the most comprehensive offering reviewed here.

Like many in the information business, Mr. Wilson calls upon an extensive technical background dating back to the fifties, which includes work with ion accelerators, analog computers, digital telemetry, and broadcast engineering. He has held posts teaching electronics, but has devoted his efforts primarily to Panaxis for the past 10 years, as well as serving as a broadcasting consultant.

Panaxis sells plans and some kits related to amateur radio, CB radio, various aspects of television, including scrambling; computer software, and low-power to full-power FM broadcasting. Some of the more interesting plans/kits include active antennas, anti-bugging devices, infinity transmitters, various transmitters named in the catalog as "bugs" (plans only); a transmitter for tailing autos; ultrasonic jammer, non-digital voice scrambler/descrambler; various RF sniffers, parabolic mic, electronic voice disguiser, SCA decoder, notch filters to remove hash video signals, 75,000-volt electrical defense weapon, theremin (see the discussion of proximity sensors in the Alarm section); various audio compressors—gear close to the author's heart; and a host of other plans and treatises that span an incredibly broad spectrum. Prices rank among the most reasonable we have seen, from plans up to complete kits.

Panaxis' catalog spans 34 professionally typeset pages. Any reader with an interest in electronics in general or surveillance/countersurveillance in particular should order a free copy from: Panaxis, Box 130, Paradise, CA, 95697.

CONSUMERTRONICS

What's related here reflects Consumertronics' catalog in profile, as well as hands-on experience with two items we had the publisher buy for testing. We asked all vendors for a more detailed bio than appears in ads or literature, but former Lockheed engineer John J. Williams' reply suggested that he wasn't interested unless we had national media connections. Judging from Mr. Williams' material, he's at least as deep-fringe-oriented as this awful rag....

Ah, well. To business. Consumertronics sells hard, meaty, usable data at upmarket prices, though not unreasonable beside prices of close-to-the-edge material sold elsewhere. We've detailed its marketing of the Pakistani "Brain" computer virus in the chapter on Security and threats thereto.

Consumertronics' current catalog includes treatises on computer phreaking, phone phreaking, cryptanalysis, encryption (Mr. Williams is among those who've posted a monetary reward for anyone who can break his cipher), magnetic fields, electrical weapons, various aspects of computer programming, and automatic teller machines. Appropriate material can be bought with or without diskettes of software discussed. In addition, he offers to research topics, no matter how outre', for a fee; and solicits consultants to pay $25 to sign up as part of his consultant database. That's right: You pay to be on his list. An offering that paid Consumertronics a commission based on fees consultants actually received as a result of referrals from the firm might attract more potential members, but that's hardly our affair.

We purchased two products: "Beyond van Eck Phreaking" ($20) and "Cryptanalysis Techniques" w/diskette ($25).

BVEP contains 12.5 pages of meat, including a letter to Wim van Eck and his reply, and a half page of advertising. Print density averages two to three times that of the average full, single-spaced typewritten page; Mr. Williams wastes few words attacking the point of the treatise: intercepting EMF radiated from computers and their peripherals and reconstructing the screen display. He offers several schematics, but, like the text, they assume the reader to have a genuinely slick grasp of electronics in general and video/television in particular. Readers without that savvy will drown quickly in this stuff. TV cognoscenti will find instantly applicable material—but do not expect the type of write-up that holds your hand from beginning to end, along with a parts list and PC board layout as one might expect from one of the project-oriented electronics mags.

Cryptanalysis Techniques (15 pages plus diskette) again serves up a platter of rich fare that demands several close readings to extract all its content. Running the computer programs offers insight into decryption as no text alone can, though do not hold unrealistic expectations of them. They teach about n-gram analysis and Kasiski analysis, among other things, but don't expect to load ciphertext, sit back and wait for the decrypted message to appear. The diskette throws in additional software in compressed form that those with access to an electronic bulletin board can decompress using a downloadable utility.

Assuming Mr. Williams writes his own ads we infer that he has a firm grip on the psychology of hype—and that's a compliment. Ads live or die by the force of their hype. Consumertronics' ads lack nothing in that sphere. Current catalog $2, free w/order. Box 537, Alamogordo, NM, 88310. Recommended...even if he won't rub elbows with us sleazos....

DIRIJO CORPORATION

Richard Pearson has been a notable contributor to Radio-Electronics magazine. He is also the principal of Dirijo Corporation. He wrote the now-infamous laser-bug article that made the cover of R-E and triggered a reproof from Forrest Mims III. He designed the schematic that R-E kindly let us reprint. Dirijo sells (or sold) a semi-printed circuit board for this project, with parts layout diagrammed for ease of assembly. It was well worth the price of $7, including P&H. Included with that board were refinements in the original design and changes in certain components that alone were worth money.

The current catalog lists plans for an FM transmitter with built-in automatic level control. It offers treatises on special aspects of satellite and cable TV descrambling and police radar. The radar material was particularly informative.

We wrote Mr. Pearson about visiting him, and mentioned casually that we would like to photograph his laser-listener prototype. His reply seemed defensive—and we are reading liberally between the lines here—in the sense that he stated that the device no longer existed; that he had been informed that possession of it was a crime.

Well. Let's digress a bit to tackle this business of when a bug is a bug is a bug. In 1985 the author received as a gift a kit called "Sound on Light." Its input was a phototransistor that fed an operational amplifier, the works mounting in a tube fitted with crude lenses for aiming. The device came with a shiny metal reflector, plus instructions for the following experiment: One subject would stand in direct sunlight, hold the reflector near his face, and bounce sunlight off the shiny surface in the direction of the second subject, who aimed the tube device—now activated, and feeding a pair of headphones—at the light. When the first subject spoke, the second subject could hear the words. His voice caused the metallic reflector to vibrate, modulating sunlight with audio. The receiver demodulated the audio.

No one with a basic grasp of physics can doubt that this project could demodulate laser light as easily as it did sunlight. It differs in design from Mr. Pearson's receiver only in its choice of phototransistor and amplifier, and the lack of a meter. Perhaps more important, nowhere in the literature that came with the device did it mention its potential use for bugging; whereas the laser listener article waved a red flag in the face of federal bulls charged with enforcing the anti-bugging laws.

True, it's hard to call a coaxially mounted laser and matching receiver anything but a laser listener, for its design speaks to that purpose. It is equally difficult, some might say impossible, to call a parabolic microphone anything but a listener; or to call the "babysitting transmitter monitor" sold at Radio Shack anything but a listener.

Listeners serve lawful ends. We can indeed see the mother of a young child wanting to listen to her infant's room while she rakes the yard. We have seen parabolic mics out in force at pro football games, and heard their pickup played back matched to films of the game. The individuals recorded had given permission, thus no crime was involved.

The point that seems to determine how the enforcers treat an item with potential bugging use lies with stated or overt intent as to its use, or with actual use. Who's to say that hundreds of laser listeners built by hobbyists represent anything more than experiments of the genuinely curious, aimed only at windows of knowing and cooperative subjects?

Enough badinage; the point has been made.

Mr. Pearson looks to have the know-how to expand his line of plans. We hope that he does. A hungry market for descrambling and laser-bug-like material is out here, waiting. Box 212, Lowell, NC, 28098.

INFORMATION UNLIMITED

Although Robert Iannini's book, Build Your Own Laser, Phaser, Ion Ray Gun & Other Working Space-Age Projects (ISBN 0-8306-0604-1), suggested that I.U. has several employees, Mr. Iannini is the man behind the firm. He holds a number of patents, including those related to use of ultrasonics in pest-control. We wrote and asked for his patent numbers to get the copies of the patents, in hope of extracting information of interest to readers. Mr. Iannini gracefully declined, but kindly sent us a free I.U. catalog.

I.U. has been profiled more extensively in other works. Our comments here try to clue readers in on the least expensive means to assess I.U.'s products: get a copy of the book, either through interlibrary loan or by purchase from TAB books for $16.95. Though copyright 1983, its plans show no remarkable changes from those in the current catalog (plans that cost us $40 before discovering the book).

His plans may intimidate the novice, what with their talk of custom-wound transformers and such. They speak of oscilloscope waveforms almost on the assumption that the builder has access to a 'scope and the chops to use it. The one kit we bought and assembled, described in the Weapons chapter, might challenge the soldering skills of all but experienced kit-builders.

I.U.'s emphasis lies with high-voltage devices, lasers, infrared imaging units, ultrasonic generators in varied configurations, and a few surveillance-related devices, such as FM transmitters and a two-foot parabolic microphone with high-gain amp. Catalog $1. Box 716, Amherst, NH, 03031.

JOHN WILSON, JR

Wilson has been around a number of years, made a solid reputation selling mainly plans and some completed gear, notably his RF-sniffer, which, to this day, has to be the bargain in countersurveillance. The plans cost $22; careful shopping can keep the parts cost below $20, including a Radio Shack "blue box" and knobs for the controls. (We ferreted out a 0-50 microamp meter for $2 from Fertik's. The typical panel meter goes for $10-$20.) For less than $40 total you get an incredibly sensitive device. How sensitive? We'd like to be able to put it in mathematical terms, but only engineers would grasp it. We built an FM phone-line transmitter whose antenna had not been pruned; yet that short-range unit sent the sniffer's meter to full scale from a distance of 10 feet. We tried it on a low-power UHF transmitter that an accomplice had hidden in a 2-bedroom apartment. This took a systematic sweep of all rooms, but the sniffer found that tiny bug as well. Here we had to get within a foot of it to read full scale.

The unit built by the author, with extreme and unnatural disregard for all cosmetic appeal, appears in the photos. Bulky, ugly, but goddamn is it sensitive. A bit of planning and a proper box could make it look presentable. Its useful bandwidth spans 10 MHz to "well into UHF." In fact, it reads microwaves leaking out your oven.

Wilson gives advice after the sale, will look over built-from-scratch units to help duffers find out where they goofed, answers letters promptly, and freely shares his vast knowledge of electronics and related lore. His catalog costs $5, but he says he pegged the price high to screen his clientele to those with some serious

interest in hobby electronics. In any case, the price is refundable with the first order. For the true beginner, his material offers the most in terms of guidance, with the assurance of "service after the sale" on boards etched and drilled from scratch, quite a commitment that has earned him something of an international fan club....

His current catalog offers plans and/or information on directional mics, audio amps and preamps; an array of transmitters, both crystal controlled and RC-tuned; bumper beeper, repeater, improved antennas, phone transmitter; his famous bug sniffer and a sniffer with more bells and whistles, known as a bug finder; a phone line locator, converting CB gear to non-standard frequencies, and making circuit boards and enclosures. He just brought out plans that use Radio Shack's "receiver on a chip" to make an FM radio that will fit in your palm, for those special frequencies.

Mr. Wilson does custom design work to just about any specification, but restricts special gear for those who have proper credentials, meaning a badge or connections with agencies usually tagged as three-letter groups. He also has the means to spot phonies very quickly, in case you were thinking of printing up a police letterhead to access his "back burner" stuff. He kindly lent us the tiny transmitter built into an aspirin box shown in the photo, and gave us an interesting BG on its history, probably best not chronicled here....

There is a great deal we would like to relate about Mr. Wilson and his activities, since it would lend this book more intrigue; inside dope always has that effect. Of all sources listed here his background puts him closest to true spooks, but he keeps a low profile out of legitimate intents that we respect.

Check out Wilson's catalog (John Wilson, Jr, Box 5264, Augusta, GA, 30906; $5). We do not aim to endorse or pan any product or vendor here, but, having built a trainload of projects researching this book, we have to offer as sound advice that the first piece of surveillance-related gear the beginner builds should be Wilson's RF sniffer. It will facilitate tuning transmitters and acquaint you with an extremely easy method to make printed circuit boards. The author swept his residence after completing that project, and found a little surprise in the master bedroom. The unit is so sensitive, it was probably a false reading. Probably....

MAGAZINES

The electronics literature has latched onto this fascination with spook stuff because it sells magazines. The cover of the October, 1987 issue of Radio-Electronics depicts use of the laser listener, something Buck Rogersesque back in the sixties, that the average hobbyist could build for less that $40, minus cost of the laser, which will run another $200 to several thousand, depending on power, aiming capability, wavelength, etc. R-E and Hands-On Electronics have featured articles and construction projects on cable TV descrambling (the multipart series in R-E is worth buying back-issues to get), copyguard defeating, directional microphones, defeating copy-protected software, data encryption, voice scrambling, phone phreaking (from the historical perspective only), and laser listening.

BUYING PARTS

Take a thousand parts off the shelf of any electronics supplier and test them. Odds are, a percentage will fail to meet their specs. The very best parts are individually tested before leaving the factory. This does not guarantee they will not fail later, but is the best that can be done short of a prolonged burn-in.

To no one's surprise, these parts sell for more than untested units. As an example, one vendor sells individual MRF901 transistors for $1.25. He has tested each one for all variables except gain (which should be tested before using this RF transistor in a critical application). The same vendor sells 901s ten for a buck, untested. He told the author in a phone conversation that he buys them $85 per thousand, and that about half test bad....

The MRF901 transistor qualifies as a considerably more delicate component than most resistors and capacitors, yet the same principle applies to all: The only means of assuring a component's integrity is to test it. Often, pre-testing components before soldering them to the board will save many hours of troubleshooting when the thing fails to work.

Resistors and capacitors test easily using the latest generation of digital multimeters, with accuracy heretofore unobtainable. Many units selling for $50 and up also sport the ability to test some aspects of diode and transistor function, though thorough testing will require a dedicated checker. Still, the multimeter gives a go/no-go signal for semiconductors.

Buying and using first-line parts will cost, but may save in peace of mind and fewer failed projects. Bulk buyers (a hundred or more of each part) are just the type to own equipment to test their cheap and iffy parts, and to catch bad merch before using it.

Some parts, such as logic devices, are impractical to test without a dedicated unit. Hobby magazines have published articles detailing construction of just such test devices, and they are available assembled at semi-reasonable cost.

The morals that concern parts: A) The second device you purchase should be a digital multimeter with as many functions as you can afford. You can get a carload for less than $75; B) Where possible, test key parts before using them; C) If your project uses integrated circuits, solder sockets in place of the chips the first go-round. That way, you do not have to desolder a 16-pin chip, with risk of heat destruction, to replace it. Merely plug in another chip.

MAKING YOUR OWN PRINTED CIRCUIT BOARDS

For projects that give you a schematic only, the novice starting from scratch will meet trouble. To get something worth building, and functional, almost always demands use of perfboard at the least, preferably a printed circuit. Making printed circuit boards is easy in theory, a bit tricky in practice.

Count on failure with your first try, because it will probably happen, and for that reason start with a small, simple pattern it won't wreck you to lose. The nature of the defects in your first board will guide you on the second. Make your first board an extremely simple one. The example in the photo set may tax the first-timer, but by no means lies beyond his reach if he is careful.

Printed circuit boards are nothing more than hard, flat insulators, such as phenolic resin or Fiberglas, laid with conductive traces of copper on one or both sides, and drilled to accept components to complete a circuit.

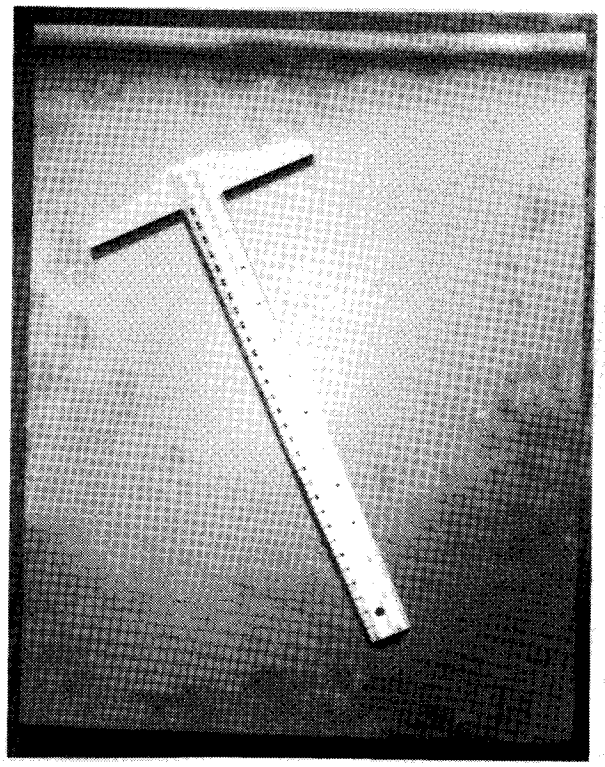
But most boards start out fully coated with copper on one side. Making a useful board demands removal of some copper to leave conductive pads and traces. This process is called etching.

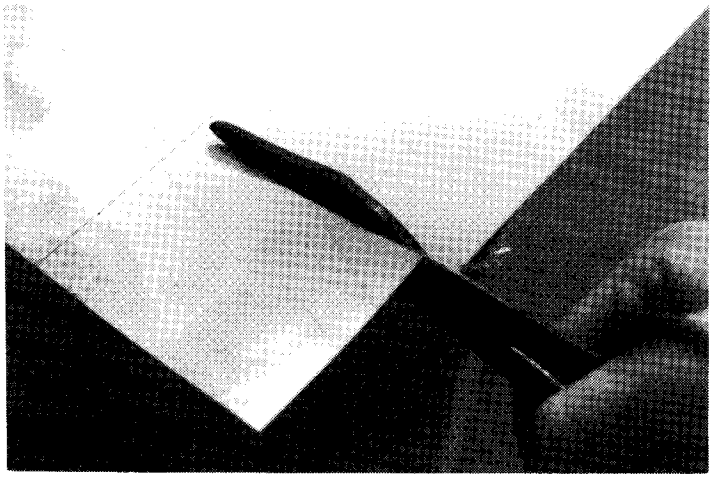
Etching involves immersion of the entire marked board in a solution that dissolves raw copper. This can be touchy. The chemical most commonly used is ferric chloride. You'll find this ugly brown corrosive (hydrochloric acid) on the shelf at the local Radio Shack, and stocked also by most purveyors of circuit-building goods. Before using it, be aware that it eats/stains almost anything, including a "stainless" steel sink. Spill it on the carpet and you are in either for a dye-job or replacement of a swatch. Take it from one who's been there that steam-cleaning won't cut it.

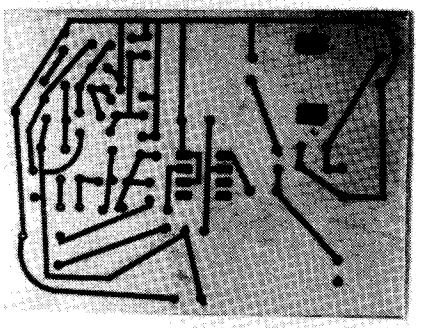
And as a corrosive, well, adequate eye-protection is a must. The author once spilled a cupful of ferric chloride etchant on his leg. It felt like fifty hungry mosquitoes biting at once. Natch, he hit the showers pronto.

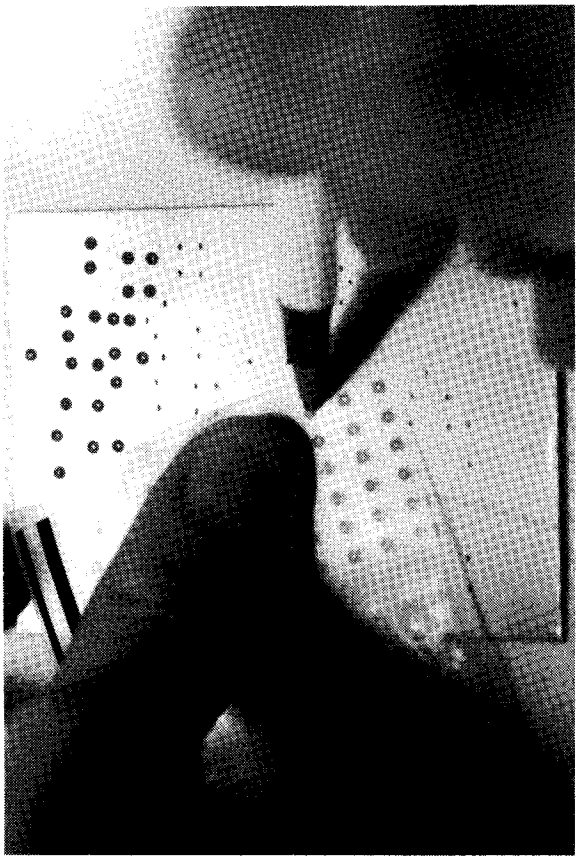
Begin with simple designs. Lay out pads and traces using either commercially sold rub-on pads and strips, or the resist-ink pen. Rub-on traces resist etchant much better than does ink. If you use ink, retrace the circuit after it dries the first time. These marked areas will remain while unprotected copper dissolves in the etching process. Photo methods discussed below offer many advantages for those projects that provide you a dandy black-and-white pattern, but best to use simpler methods for familiarization.

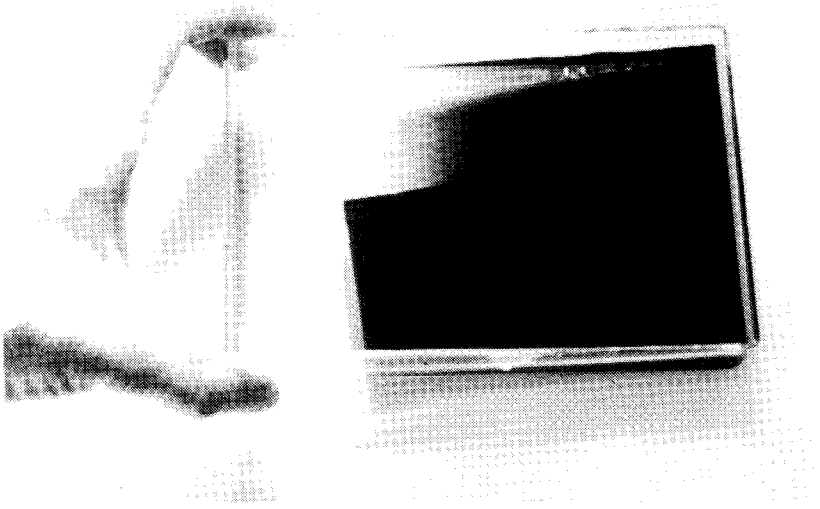
Cold solution etches more slowly than warm solution. Chemical reactions accelerate at higher temperatures. Ideally, ferric chloride should be heated to 90-120 degrees F. Pour about a quarter-inch of solution into your small, flat, clear plastic tray (the one that came with your beginner's kit works fine; NEVER use a metal tray). Pop it in the microwave on medium power for three seconds at a time. Stop when the solution as felt



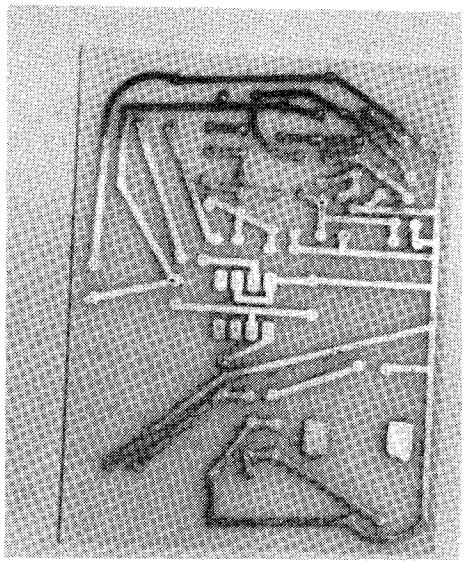


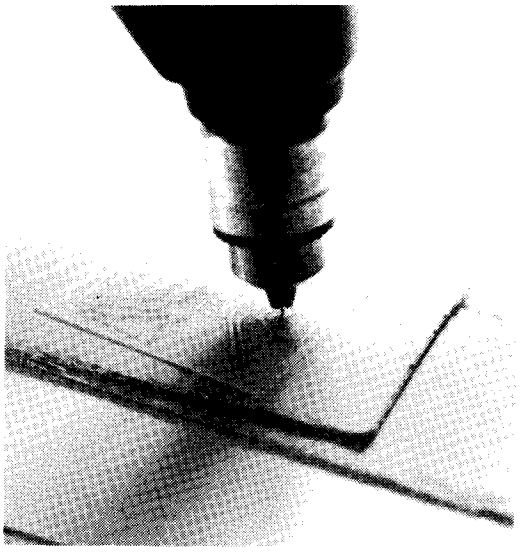


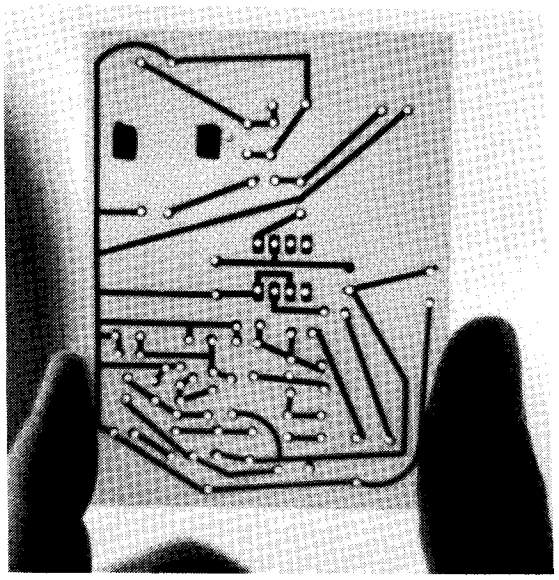


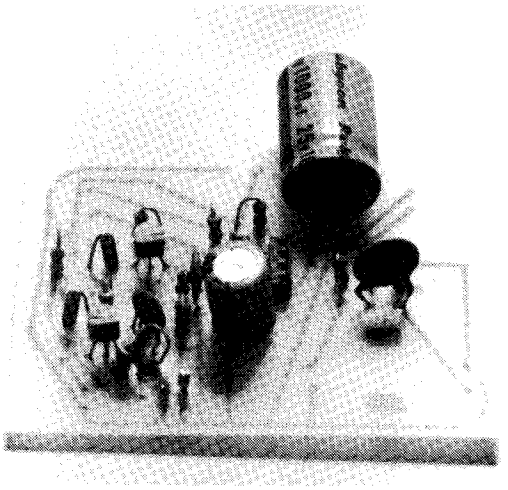


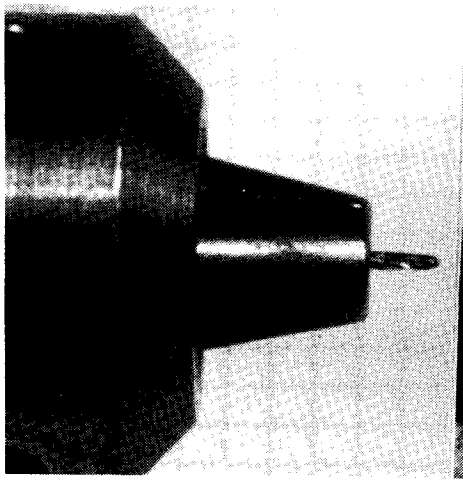
MAKING PRINTED CIRCUIT BOARDS. TOP LEFT: Thin copper-clad board, extremely inexpensive ($2 for the sheet shown) from Fair Radio Sales. TOP RIGHT: Easily cut with tin snips or heavy scissors. BOTTOM LEFT: Rubbing on traces and pads. MID RIGHT: Completed layout, ready for the tank. BOTTOM RIGHT: Etching. Be careful.... (continued next page)

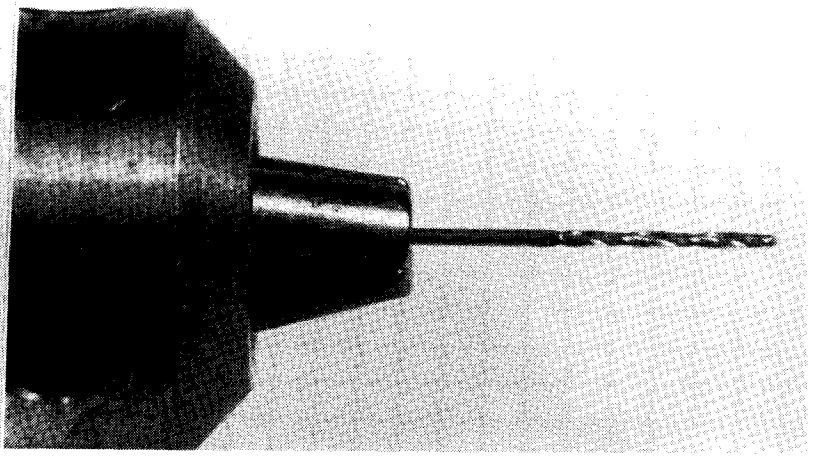












(continued from last page) TOP LEFT: Etched board burnished with steel wool. TOP RIGHT: Drilling. MID LEFT: Note that bit used was #60, too large for these pads; alternatively, we could have used larger pads. A #66 bit would have suited this project better. MID RIGHT: Project nears completion. BOTTOM LEFT: Correct mounting of thin bits for drilling boards. BOTTOM RIGHT: Incorrect mounting. The bit will break easier than a toothpick.

through the container (don't dip your fingers in it) feels just warm. Immerse the laid board copper-side up, then begin gently rocking the tray back and forth, side to side, washing etchant evenly over the surface.

Etching will seem to take forever. Count on 20 to 60 minutes' agitation per board. A hotter solution etches quicker, but adds the danger of eating through thin traces by getting up under the edges. The virtue of patience turns out the best boards, both cosmetically and functionally.

Do not assume, as many beginners do, that you can let the board soak overnight in cold solution and have perfect traces greet you next morning. The board will look moth-eaten with broken traces in many places. The etchant gets up under the edges of the resist. It usually means a wasted board.

Stop to inspect the board every few minutes while rocking it. Cease etching once all superfluous copper has dissolved. Since ferric chloride blackens as it works, you must remove the board and rinse it to inspect it closely. A pair of rubber gloves come in handy to keep your hands free of nicotine-like stains. Check the board more often as you near the end of the process.

When only traces remain, remove the board and place it under cold running water for at least two minutes. This stops the etch reaction still occurring under the edges of the traces. Pour the used ferric chloride in the commode and flush. Again, it will mar stainless steel, so don't splash it in the sink.

Another chemical, ammonium persulphate, will etch copper clad boards. It costs less than $2 per pound, and a pound dissolved in distilled water makes a gallon of etchant, far more economical than ferric chloride. Try both, see which you prefer. Ammonium persulphate is available from Mouser Electronics, as of this writing.

Next, clean off the lacquer or other trace material as recommended by the maker. Some traces require a lighter-fluid-like solution, while others come off with gentle scrubbing with a polyester pad. Then burnish the copper to a uniform sheen with fine steel wool under running water (wear gloves and goggles).

Fancier boards coat the copper with tin using a solution available from Datak. It prevents oxidation of the copper and wets more easily with solder.

Drilling holes: The 1/16" bit included with some PC kits makes holes that swallow the tiny wires of electrical components. It will obliterate small pads. It bores holes simply too big for quality work. A #60 bit is about the largest you will want for component leads, but even this size is a too big for some small-circuit work. As you become more sophisticated, you will want a variety of bit sizes, #66 and #74 for example, smaller ones for components with thin leads, larger ones for direct board-mounting of jacks and transformers. Hobby shops that cater to the radio-control airplane trade usually stock bits in this range, as do printed circuit vendors and Edmund Scientific.

A lightweight, cordless drill is used to good effect for circuits that demand only a few holes. Mount the bit in the chuck such that only enough protrudes to penetrate the board. Those slender bits break as easily as toothpicks. Center the tip of the bit on a pad or other spot needing a hole, then start the chuck turning slowly. Once it has begun to bite, go to "high" speed, i.e., enough not to waste time, but not as fast as the drill will go. You are holding a device that may weigh several pounds over a delicate structure. Should you punch through with too much verve, the chuck could tear the pad or fracture the board. Go easy until you get a feel for it.

For large boards, or for those demanding extremely precise placement of small holes, a jeweler's drill press may be needed.

There is no agreement as to whether you should drill before or after you etch. The author has had best results drilling after, but the reader should experiment.

DESIGNING BOARDS

Unless you intend to get into this heavily, best leave the work of designing the board to the person who created the circuit. Professionally made designs, such as computer motherboards, are masterpieces of elegant engineering that optimize component placement and minimize use of jumpers (connections between traces on

the upper surface of the board). Many of these designs could not have been produced without the aid of computers.

For extremely simple circuits, try laying out components in diagrammatic form and connect the dots. This will give a functional if inelegant piece of work.

If you can, examine some examples of professionally produced boards used in, say, stereo components. You will note that, unless it is a computer circuit, its traces are extremely thick compared to the ones on your first few boards. The reason has to do with speed, sometimes with shielding: the thicker the traces, the less copper must be removed, the less time etching takes, and the less chemical is required to process a given batch of boards. As the wisdom of this sinks in, you will find yourself filling blanks on your boards with etch-resist so at least that splotch need not be etched, saving you time and etchant.

With a bit of care, it is possible to lay out a board with paper and pencil, then transfer the design by hand, estimating visually, directly to a board using rub-on traces or a resist-ink pen. For a more professional appearance, or to modify a complex design at a later date, help is available in the form of several computer assisted design programs, some of them dedicated to making PC artwork, though generic CAD programs will serve well. Many will crank out an image on your dot matrix printer that you can use for one of the photo methods.

PHOTO METHODS

The magazine article for the voice scrambler described in the chapter on Security includes a life-size black-and-white image of the circuit board. But you must somehow transfer that detailed image intact to the copper clad side of a blank, and do it such that the black traces resist etching. This calls for the photoresist method.

Two basic principles are in use, the positive method and the negative method. The negative method, the copper traces appear in black. The positive method, they are white or clear. Both methods demand "exposure" (as to a strong light source) of a "sensitized" board, one whose copper has been coated with photoreactive material. Some boards come this way, other must be painted with photoresist.

The next step is "development." This removes the photosensitive compound from the appropriate areas, depending on whether it was a negative or positive, thus leaving the board coated with resist as if you had applied it manually.

From here, the etching process proceeds the same, though an added step involves removal of the photoresist from the finished board, followed by burnishing with steel wool, etc.

Whatever method you use, always inspect the completed board for shorted or broken traces. Repair those with minor flaws using either a wire jumper or conductive ink sold for the purpose.

SOLDERING

Soldering has changed. Irons the author bought in 1963 and 1975 to assemble electronic kits sported a 1/8" tip. Today, working tips start as 1/16" chisels and shrink to points that demand a magnifier to see. Solder has become available, of necessity, in strands that rival human hair for thinness. An illuminated magnifier is helpful during construction and for inspecting the work afterwards. Screw-ups happen so often that desoldering equipment to rectify them has seen a boom. Components have become so sensitive to static electricity that safely soldering some of them requires an iron with a grounded tip. The $4.95 special imported from Hong Kong has given way to the $200 variable console iron with an array of tips and integral grounding.

If you have no soldering experience whatever, you may run into trouble assembling that transmitter whose whole works will hide behind a quarter. Best to begin with visible (i.e., large) boards and work your way down.

The ancient teachings told us to place the iron simultaneously in contact with copper pad and lead of the

component to be soldered, wait a second for it to heat both metals up to the solder's melting point, then touch the solder wire to the junction. It would melt, form a globule, and make an electrical connection. Easy.

Or it would be if electrical components were immune to heat. Some, such as resistors and ceramic capacitors, show excellent heat tolerance. But others—transistors, especially infrared phototransistors; integrated circuits, and diodes—"die" when too much heat crawls up the lead into the device. And the smaller the part, the less heat it can take.

This has two implications. First, spend as little time as possible with the tip of the iron touching the board. Second, use heat sinks in heat-sensitive components, such as that $20 microwave transistor at the heart of your latest miracle. (A heat sink is a reservoir of sorts that soaks up heat headed for a component. An alligator clip snapped onto the lead you are about to solder will do in most cases.) For integrated circuits, instead of soldering the chip directly to the board on the first try, use an IC socket (sockets are available for most low-power transistors, too; give them a thought for early projects, or those whose components you wish to use in other projects, or to have to replace; it's ten times easier than desoldering).

While talking about the means by which components may suffer damage we should mention static electricity. Devices made with MOS (metallic oxide surface) technology, as so many low-power devices are these days, can be destroyed by an otherwise unnoticed static charge, the kind you pick up walking across carpet on a dry day, or sliding out of a vinyl chair.

Notice that these static-sensitive devices come packed in what looks like sponge. It's actually conductive material to keep all leads at the same potential. When handling such devices, the safest course places everything—you, the board, the work surface, the soldering iron, and the component—at ground potential. That means electrically connecting them all simultaneously.

Which ain't so hard in practice. First, place the board on a conductive surface. Specially made pads can be had, but a big swatch of aluminum foil works fine. Second, connect yourself to this ground. Laying your bare elbows on the foil will do. Third, before you remove the component from its protective sponge, touch the sponge. This way, you, the board, and the component are all connected electrically. Finally, touch the tip of the soldering iron briefly to the aluminum foil. In theory, there should then be no current to flow through the device before it gets plugged in.

Natch, you do not work with powered-up circuits in this fashion....

DANGERS IN FIRST-RUN ARTICLES AND PROJECTS

If you plan to build devices detailed in electronics hobby magazines, be aware that errors in parts lists, schematics, and PC board layouts are the rule. Authors or readers catch them, and usually the magazine will print corrections in its next one to three issues, so a subscription is indicated for those who plan to get heavily into this. (And in every case in which the author has ordered the etched and drilled PC board offered with many projects, the seller of the board pointed out changes or errors not mentioned by the magazine; none of these independent board vendors want the FTC hassle of returned boards: no mailorder sale is "final" for thirty days, whether the vendor says so or not, so they make a point of testing their work....)

BUT HOW DO YOU KNOW IT WILL WORK?

We are not dealing with Heathkits here. There is little recourse after the sale, certainly no "We won't let you fail!" philosophy. No, the only way to test a gizmo is either to go whole hog and build it, board and all, or build it first on a test-board, known in common parlance as a breadboard.

A breadboard provides a grid of holes with 0.1" spacing common to many electrical components, and usually includes an AC-derived power supply, though that is a convenience, not a necessity. Most projects will be battery powered in any case, and it is just as easy to hook up a battery pack as it is to run the AC supply (which usually introduces undesirable 60 Hz AC hum in preamplifiers; if your circuit uses transformers, it <u>will</u> pick up hum radiated by the transformer in the breadboard's power supply).

Slapping the circuit together correctly on a breadboard, like laying out PC boards, proves tougher than it looks. And if you make the wrong kind of wiring error, such as reversing the polarity of the power supply, you can kiss several expensive chips goodbye.

General rules: First, keep leads as short as possible, since this will closely mimic PC board layout. Second, use insulated jumpers (a wire-stripping tool is worth its weight in platinum). Third, always double check your work before applying power to the circuit. Fourth, if the circuit fails to work when power is applied, shut it down immediately. The same holds if a working circuit inexplicably quits on you. Feel the chip(s). Some types of wrong wiring kill the chip by overheating it. Realize that 99 percent of failures trace to your own wiring errors. Fifth, curb the tendency to move leads while the circuit is powered up. As one example of how this can kill a chip, many circuits use capacitors, units which store energy. Plucked out of one socket fully charged, then plunged into another, it may dump its load into a sensitive junction that lives no more. Work carefully, power down before altering a circuit. Note that, when experimenting with one half of a dual or "stereo" chip, killing one channel might not harm the other, leaving it in shape to carry on. Sixth, long leads make for unintended shorts. Watch this carefully. Finally, do not start with some complex function generator. Make something simple, a project to give you positive feedback in the form of success.

Those who breadboard circuits soon find themselves hankering for test gear. In many cases it is all but impossible to trouble-shoot a circuit without a VOM at the least, often a digital multimeter and an oscilloscope.

Exercise great care when transferring circuits from breadboard to printed circuit board. For reasons the author hasn't been able to delineate fully, projects that blew your socks off on the breadboard either lose it on the PC board or don't work at all. We encountered vexing problems with the LM382, which, after days of reconfiguring the circuit, turned out to be a partially blown channel 1. The second channel of this dual device worked fine, meaning that we had accidentally damaged the bad channel through exactly the amateurish practices the reader should avoid. If the entire channel would die completely, it would betray itself quickly; but mere parts of an IC die, leaving the rest to carry on, after a fashion, so as to mislead the trouble-shooter.

SURFACE MOUNTED DEVICES

Surveillance devices described, sold, and made using conventional electrical components are in any practical sense small enough to accomplish their task without detection due to size. Yet we must take note of increasing availability to the hobbyist of electrically identical components a fraction the size of the common variety. They are known as surface mounted devices, and have been around since the 1960s. Consumer electronics which called them to our attention were the ever-shrinking line of Sony Walkmen, and the Cincinnati Microwave Passport[tm] radar detector. SMDs are now available to the hobbyist.

Their two vital properties are A) small size, B) soldering to the copper side of the circuit board, rather than having their leads pushed through holes for soldering on the other side (they have no leads). It is possible also to increase the density of components by printing circuits on both sides of the board and loading them with components.

At this writing, you can purchase resistors, capacitors, variable resistors and caps, inductors, LEDs, and from some sources, ICs and transistors in surface-mount configuration. The electrical specs don't change.

Board design, handling, and mounting change, though. You will absolutely need that magnifier, along with tweezers, micro-tipped soldering irons, some special desoldering gear...and a great deal of patience. This can be like making a watch, the old mechanical kind, from scratch. The entire circuit board may fit behind a postage stamp.

Aside from a certain novelty about them, their place in home-brew surveillance equipment has yet to define itself. Servicing is harder out of small size, as is substitution of components in experimental work.

Best to know that they are available, though, for that transmitter that has to lose about 75 percent of its bulk to escape detection.

* * *

THE PARADE OF PROJECTS

To illustrate a sliver of the incredible variety of audio amplifiers, either sold or easily built, we include schematics of units, along with comments as to their idiosyncrasies. Some mate to directional mics, for readers interested in listening to bird calls.

1. CLONE AN AMP

The first schematic shows Radio Shack's model 277-1008B audio amplifier. It requires a 9 volt battery and sports an input impedance of 5000 ohms. It contains a small built-in speaker as well as low-impedance headphone output. For the money, it isn't a bad buy, but you can build superior amps for the same cost, starting from scratch. A good way to get your feet wet making PC boards would be to duplicate this unit's layout.

2. A GRIM AND FATEFUL HISTORY

In the summer of 1964, the author, then a tyke of 11 years, read an article in the now-defunct Popular Electronics that detailed construction of a device billed as a tubular microphone, known of late as a shotgun mic, a frightful and extremely sinister device for eavesdropping at a distance. In December of that fated year he built this tubular microphone as a science fair project. (Do schools still hold science fairs? "A New Method for Synthesis of Cocaine," by Robbie McPherson, 11th grade, Future Chemists of America....)

Reminiscing now, it's easy to grasp those terrible looks of dread and awe this engine of corruption evoked. Teachers and classmates seemed stunned that a mere child had hatched the deadly unit. It won no prize, but the eighth-grade science teacher, who fancied himself hip, kept badgering the author with, "Is it NPN or PNP?" (You got it, teach.)

The tubular microphone has gone on a bit since those easy days. It is now a felony to possess such a device and use it to eavesdrop. Units in existence today are used for, uh, listening to bird calls.

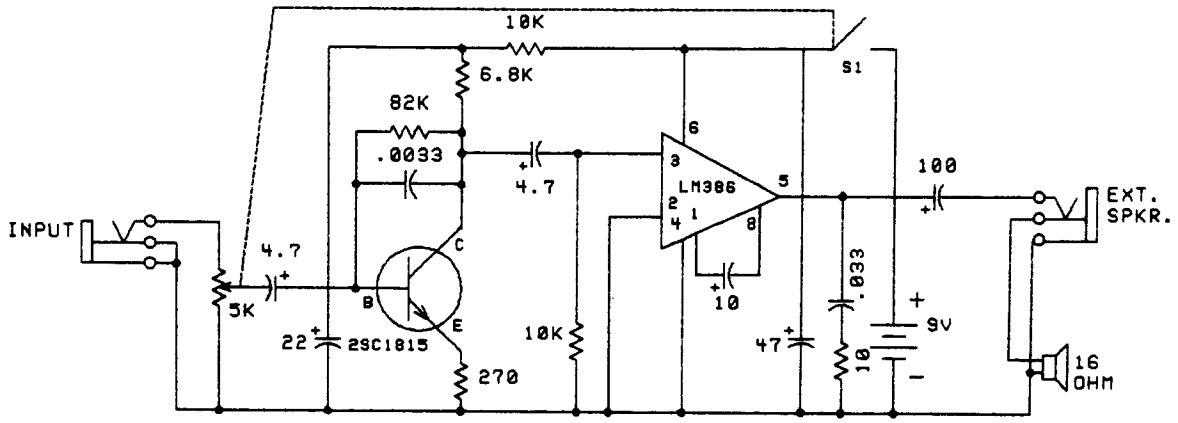
And the shotgun mic is straightforward if tedious to make. Following the original plans in Popular Electronics will rob you of the power of the latest microphones and amplifiers.

Pictorial directions practically explain themselves (but read the kicker at the end of this section before charging out to build a tube-mic). First, make the tube assembly. You will need just under 56 feet of thin-walled aluminum or PVC tubing with an inside diameter of about 1/4". Cut it into 37 tubes ranging from 36" to 1" in length (i.e., one 36", one 35", one 34", and so on down to 1" tubes, of which you will need two to fill out the hexagon).

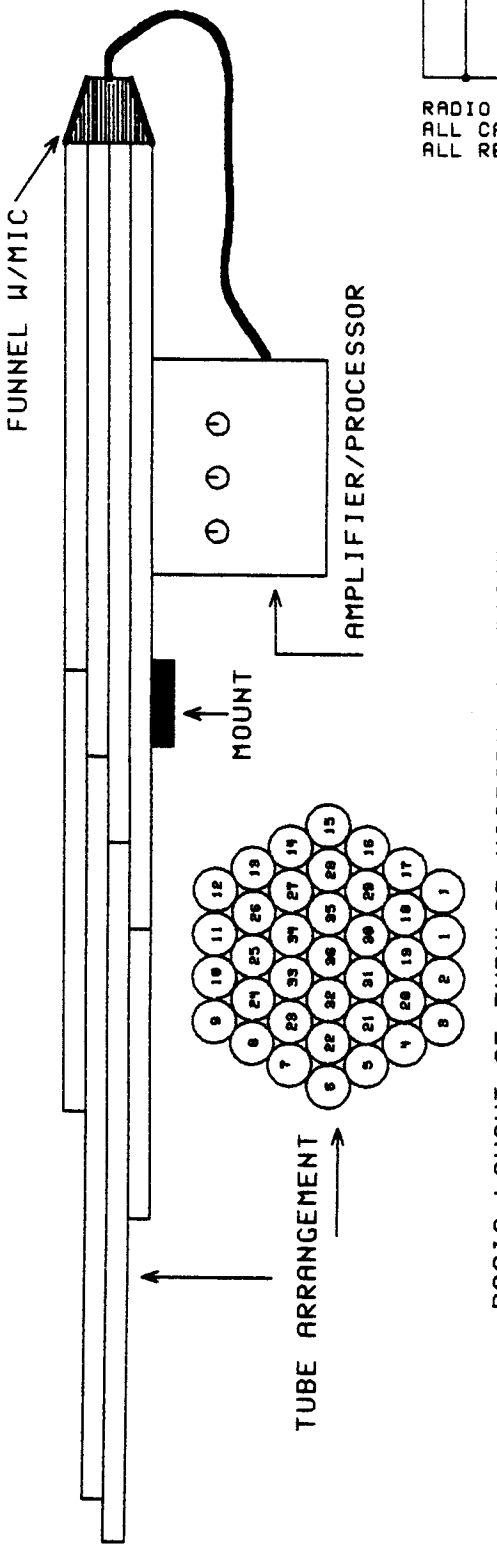
Assemble them as shown in a steadily shrinking pattern, like some demented calliope, beginning with the 36" tube in the center and working outward in a downward spiral. Use one of the fast-drying adhesives, such as cyanoacrylate or 5-minute epoxy, assuming you grasp the hazards of that gunk. The author waited patiently, hours it seemed, in 1964 for then-new epoxy resin to harden. What's more, the sheer bulk of glue required tended to disalign the tubes.

As a safety measure and a cosmetic one for those who use metal tubes, try to cut them off at a clean right angle. If you use a hacksaw, be prepared to file off burrs. You'll get a sharp, menacing edge even if you use a rotary pipe cutter due to aluminum's softness. Anticipate it. Deal with it.

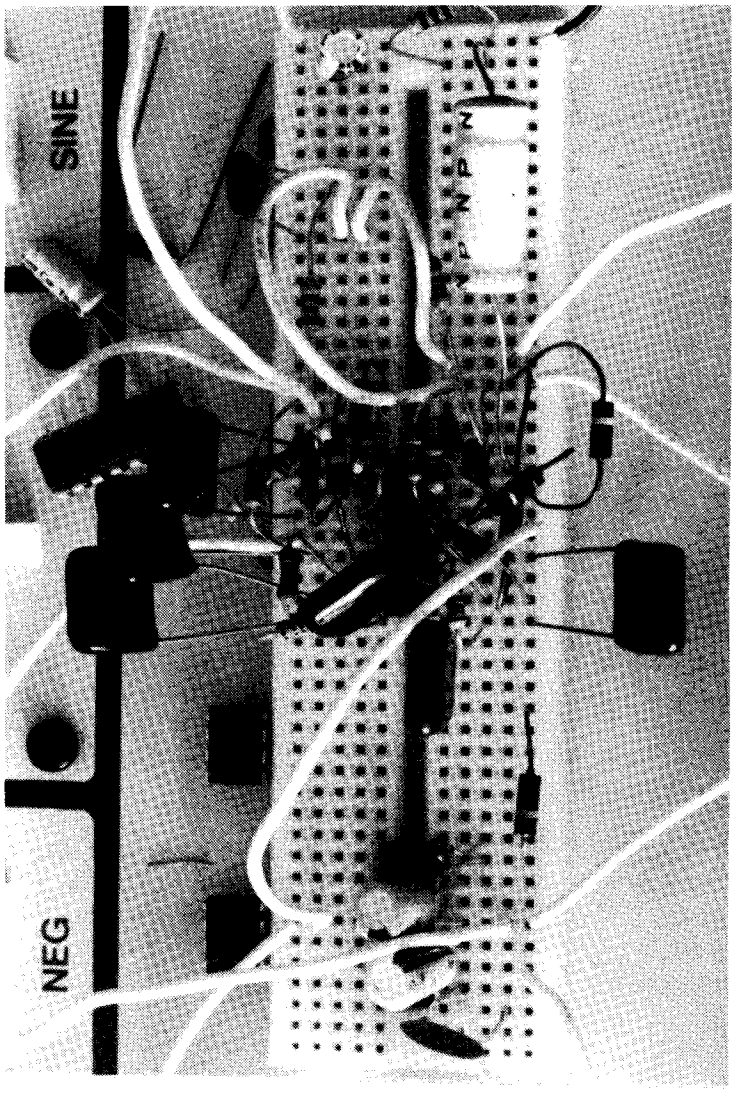
The amplifier: A quarter-century ago, the Popular Electronics article commended Lafayette Radio's 5-transistor all-purpose audio amp, which has gone to some nameless electronic heaven. Back in '64, Lafayette sold 3-, 4-, and 5-transistor jobs. What a time of simplicity: The number of transistors in a device defined its power, price, and worth. That was the era of the Beatles, the Great Society, hot books on drugstore racks (the immortal Sin Suburbia), Lyndon Johnson, Billy Sol Estes, and a host of desperate cultural symbols rarely showcased on Entertainment Tonight....



RADIO SHACK MODEL 277-1008B AMPLIFIER
ALL CAPACITANCES IN MICROFARADS; 10 OR 25 WVDC
ALL RESISTANCES IN OHMS



BASIC LAYOUT OF TUBULAR MICROPHONE (POPULAR SCIENCE, 1964)
EFFECTIVE ENOUGH TO BUILD?



TOP: Schematic of Radio Shack 277-1008B amplifier. LEFT: Diagram of tubular microphone. ABOVE: Breadboarding a simple 36 dB/oct high-pass filter, mating directly to a quasi-18 dB/oct low-pass filter, all using one quad op amp. Don't let those leads touch....

In its day, the 5-transistor job made a dandy piece of gear, but it was noisy. Just powering it up filled your headphones with a roaring hiss that overwhelmed much of what that pathetic mic picked up. (The original used a crystal mic whose impedance, if memory serves, rated 200,000 ohms. It had to be coupled with an impedance-matching transformer.)

Its modern-day counterpart is Radio Shack's model 277-1008B amplifier, whose schematic we printed. Note that it is in essence a two-stage device. the 2SC1815 transistor serves as preamplifier feeding an LM386 audio amplifier integrated circuit. A 10 microfarad capacitor is connected across pins 1 and 8 of this chip, which sets its gain to maximum, other things being equal.

With properly matched impedances (input 5000 ohms and phones of 8-25 ohms; note that most condenser mics rarely top 1000 ohms, so you gain a bit by using an impedance matching transformer for the input stage) this device gives solid performance for its price. It remains cursed by noise in the form of hiss, less than the old Lafayette, but will do for uncritical applications.

We did a bit of experimenting with this amp. First, it is easy to duplicate by making your own PC board (you can copy the traces by hand onto a board smaller than the one that comes with the unit). Second, since you rarely use a speaker, you can do it for $5 in parts, compared to $11 retail. Third, we discovered that feeding the output of one of John Wilson's low-noise preamps into this amp produced an extremely high-gain combination, suitable for directional work, that showed excellent stability.

Back to the shotgun. Once you have the tubes assembled, you must mount a microphone at the rear so as to seal off all sound save that barreling through the tubes. The original article recommended an aluminum funnel for this, and if you can find just the right size with a good lip, it may work fine. But be prepared to use, say, the nearest size PVC end cap and fill the gaps with caulk. It wouldn't hurt to shock-mount whatever mic you have chosen in rubber foam.

Fill out the picture with some type of handle or mount, such as would screw easily into a tripod. The resultant unit bears an troubled likeness to the big raygun featured in the Republic Serial, Radar Men From The Moon, and stands out just as badly.

The principles on which the tubular microphone functions include, in theory, directionality and resonance (a mechanical speech passband filter/amplifier?). Hollow cavities possess the property of resonance at a given frequency. Resonance reinforces sound. The frequency depends on the size and shape of the cavity, and whether it is open or closed. Use the tubes in a pipe organ for comparison. The actual sound of each pipe originates in air blowing past a whistle at the base of a long open tube. The pitch of the whistle and the pipe are matched such that the column of air in the pipe resonates at the pitch of the whistle (or boom, in the case of the bass pedals). No one who has felt in his chest the bass rumble of a pipe organ doubts the power of resonance to amplify sound.

The human voice produces fundamental frequencies over a narrow range, say, 300-3000 cycles per second. For that reason, relatively few tubes are required for a functional tubular microphone.

The second principle is directionality. We can see intuitively that sound entering along the long axis of the tube has a better chance of making it through without reflection or absorption, and this is in fact the case. A single tube will enhance the directionality of a microphone, something applied in "sound-spot" microphones used in studio recording, designed to record sounds from a small area and exclude other nearby sounds.

The microphone element you choose will have a tremendous bearing on the effectiveness and durability/weatherproofing of the finished product. Experience with the crystal mic recommended in the original Popular Electronics article showed that it left much to be desired. It suffered a limited frequency response and lent sounds it picked up a tinny timbre, hardly surprising given that its diaphragm was made of aluminum foil.

Why not take advantage of the sensitivity, broad frequency response and stability of the condenser microphones available through literally all mailorder electronics parts houses? If the objective is to pick up distant sounds and bring them up to audibility, it just makes sense to use the best. The microphone and preamplifier, more than the tube array, determine performance.

After that dour verbiage on the tubular mic, note that the author's effort left him underwhelmed, though the Popular Electronics article detailed catching outdoor conversations at great distances, and some sources tell of these dread tools picking up voices "through closed windows!" at ranges of 40 yards or so. One professional wire-man who'd built 3 tubular mics told the author that he too found the big shotgun both conspicuous and lackluster in action.

(What happened to that squalid tubular mic? The author subjected it to a grim series of destruction tests using extremely powerful Black Cat firecrackers on New Year's Day, 1969, a wanton pursuit utterly devoid of redemption.)

3. SINGLE-TUBE LISTENER

The third project comes courtesy Hands-On Electronics, January, 1988. This single-tube directional listener uses a 3" speaker as its microphone, whose 8-ohm impedance is matched by transformer to that of the preamp, a TL082 dual operational amplifier. One op amp feeds the second op amp, that in turn feeding the LM386 audio amplifier integrated circuit.

Total gain of all stages is 15,000. Its tremendous gain suffers from tremendous noise, as well as certain quirks in the directional mic built around this mic/amp setup described below. We built the model photographed from a set of parts obtained from Krystal Kits (PO Box 445, Bentonville, AR, 72712) for about $40, including all frills.

How well does it work? First, the amp indeed boasts tremendous gain. With properly matched impedances it was almost impossible to prevent feedback through headphones as soon as we switched the thing on inside a room.

Despite thick foam insulating the speaker/mic, anything that thumps the tube will set off a peal of thunder in you ears. At the least, we would insert a limiter between the TL082 and the LM386 if we were to use this circuit for serious work.

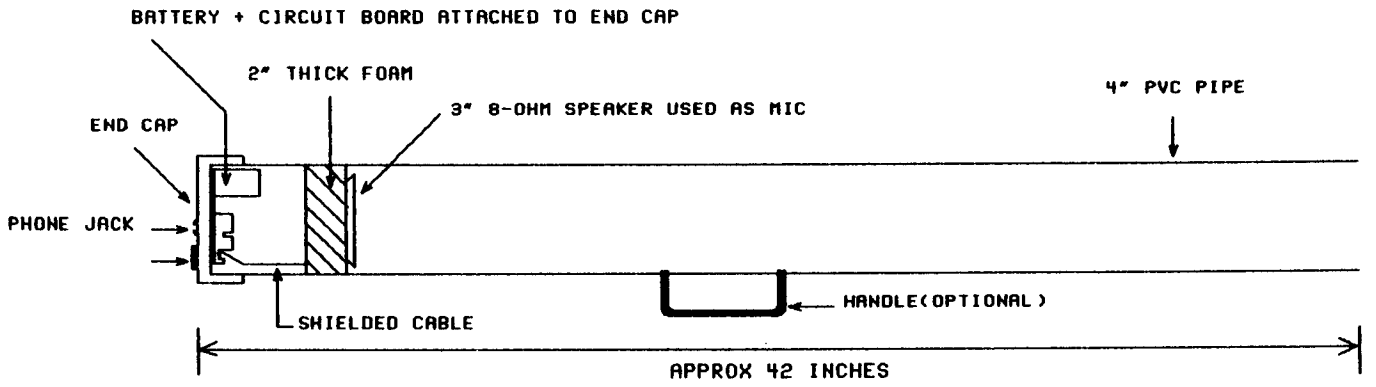
Third, boomy resonances that seem to peak in the 250-350 Hz region plague the device. Take the tube alone and hold it to your ear. It's like listening to a conch shell, whose roar is nothing more than resonance of ambient sounds. That resonance would be fine if it hit the speech band, rather than a hollow, boomy note. Here even a speech passband filter might not help, making the parametric equalizer useful.

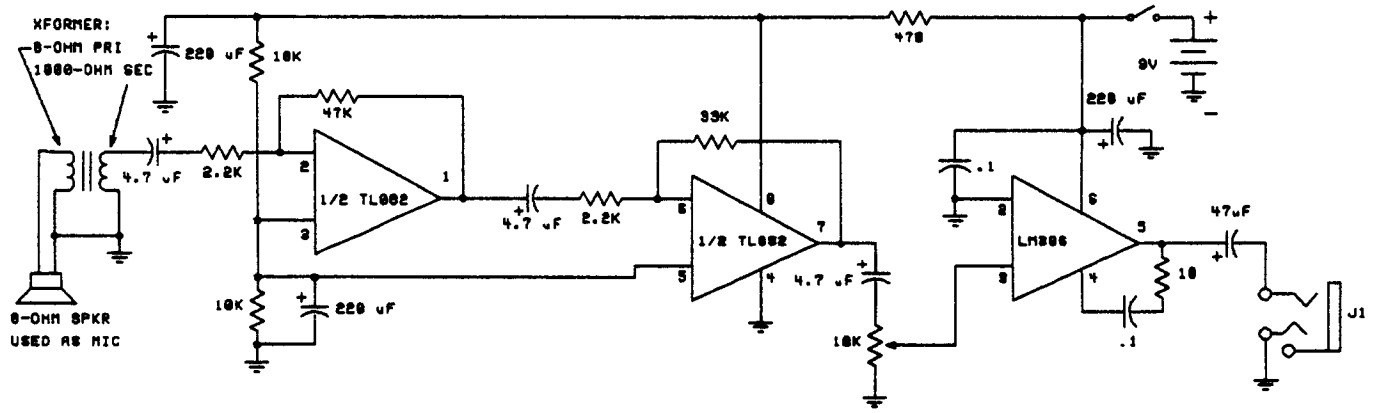
Fourth, the parallel rise of noise with gain is unavoidable. This unit was as noisy as the old Lafayette 5-transistor amp hooked up to a crystal mic, but did give greater gain. Note that the front end of the amp circuit uses a dual op amp, the TL082, which comes in a "low-noise" version, the 072. We purchased an 072 and plugged it into the circuit, with no discernible drop in noise, meaning that the bulk of noise originated in components outside the dual op amp, or that a conventional op amp was too noisy for this application in the first place.

Fifth, 3" speakers were not designed as microphones. Their response profile lacks much in the human speech region.

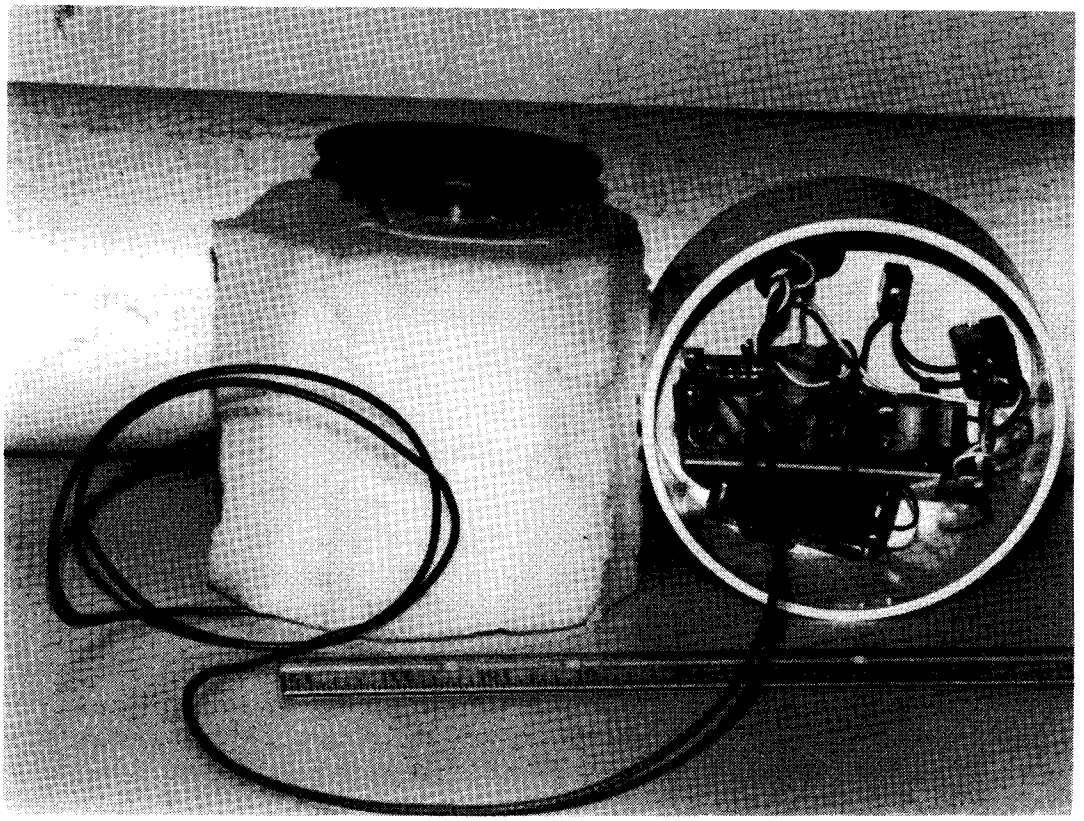
Sixth, low frequencies proved troublesome. You can banish much of them by inserting a 1 uF nonpolarized electrolytic capacitor in series with one of the input leads on the 8-ohm side of the transformer. Since we use a speaker as a mic, we might as well throw in a crossover....

Seventh, at least to our ears, we were unable to improve over what we could hear with the unaided ear. This type of setup amplifies both the target sounds and those we can normally filter by concentration, or do not hear because we have become accustomed to them. Testing this mic inside one's home, for example, proves instantly that the loudest sound comes from the refrigerator. Do not try a test while the air conditioner is running. In fact, testing directional mics inside a dwelling is often doomed to give a poor reflection of performance due to echoes. Test outside whenever possible. (As for drawing attention, well, you had to be there to see crowds at the shopping mall act as if we were aiming a bazooka at them. We split before the police arrived....)





SCHEMATIC FOR SINGLE-TUBE LISTENER AMP, FROM "HANDS-ON ELECTRONICS" MAGAZINE, JANUARY, 1988. COPYRIGHT (C) 1988 GERNSBACK PUBLICATIONS, INC. REPRINTED WITH PERMISSION. KIT OF PARTS FOR PROJECT DIRECTED THAT 4.7uF CAP AT PIN 5 OF LM386 BE REPLACED WITH 47uF CAP.



SINGLE-TUBE LISTENER. TOP: diagram of layout. MIDDLE: Schematic of amplifier. BOTTOM: Photo of unit built by author. Life-size PC-board layout printed elsewhere in this chapter.

4. DISCRETE COMPONENT PREAMP

We got the fourth schematic courtesy John Wilson, Jr, a professional engineer with vast experience in surveillance and countersurveillance electronics, as well as, ah, other areas....

This simple setup served as preamp for an FM transmitter Wilson custom-designed for an enforcement agency embroiled in ongoing drug-wars. Note that it incorporates something of a speech passband filter, showing audio response rolling off below 290 Hz and chopping off the high end around 10 KHz. What's more, it uses a limiter (the double diodes) which keeps the signal from rising above a certain level and rattling your eardrums. Instrumented tests proved it an extremely quiet design. Wilson later re-designed this preamp and coupled it to an output stage to make his current model 6020 High-Gain Intelligence Amplifier plans, which retain the frequency-cutoff and limiter, and facilitate interfacing the unit with phones, an external mic, and line-level gear, such as a tape recorder. Hobbyists set up to build their own printed circuit boards can get exceptional performance from this unit for less than $10 in parts. Of all build-it-yourself amps/preamps the author tested, this unit gave best bang for the buck.

The hobbyist willing to put in time with a breadboard can find a use for the schematic we've printed. It performed well with several types of audio amplifier IC's and served as feed for our early experiments with the uPC1571 chip.

5. SURFACE MOUNT AMP

The August, 1988 issue of Radio-Electronics published an article on building an audio amplifier, which must be the most common electronic project. This amp's claim to glory lay in its adaptability to surface mount components. The PC board for the SMD version is about the size of a quarter. Schematic and PC board template are reprinted with kind permission from Gernsback Publications, Inc., but, due to the special soldering techniques involved in the SMD version, you might want to order that back-issue for a detailed description. Also, check with BCT Electronics (8742 Belair Rd, Baltimore, MD, 21236) to see if a complete SMD kit is still available @ $14.95 plus $1.50 P&H.

* * *

PARABOLIC REFLECTORS

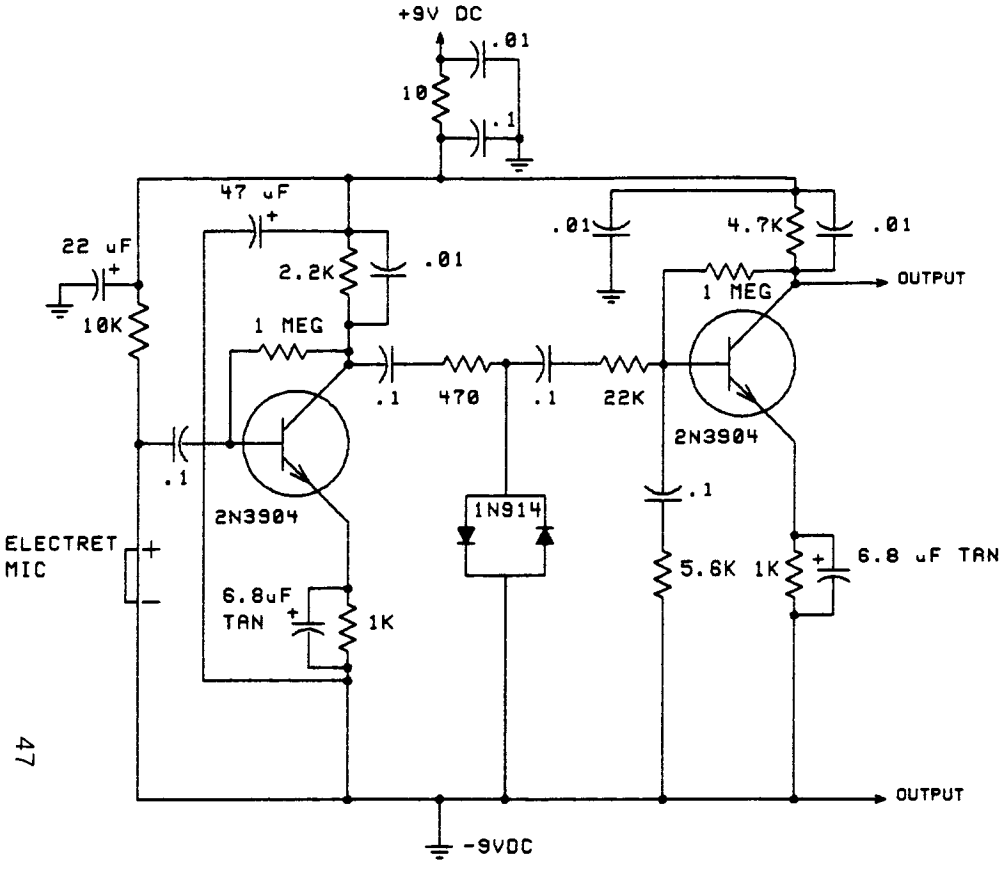
The mathematics of a parabola define it as a curve with special properties. Made into a physical surface, parabolas reflect parallel-incoming signals onto a spot called a focal point. Or, they reflect waves originating at the focal point out parallel to the axis of the antenna in, say, satellite uplinks. A rigid parabolic plastic surface about 18" in diameter, with a sensitive microphone placed at its focal point should magnify sounds and offer considerable directionality, and this in fact happens. Portions of spheres and ellipses reflect and focus sound, too, but have proven less handy than the parabola for directional mics.

Edmund Scientific, for many years a hobbyist's delight, sells both an upscale, full-featured parabolic mic with several bells & whistles (but be prepared to part with several hundred for this gem). They sell plain 18" aluminum parabolic reflectors, too. Information Unlimited sells a 2' plastic dish that may or may not be available a la carte. Make your own amp and choose your mic.

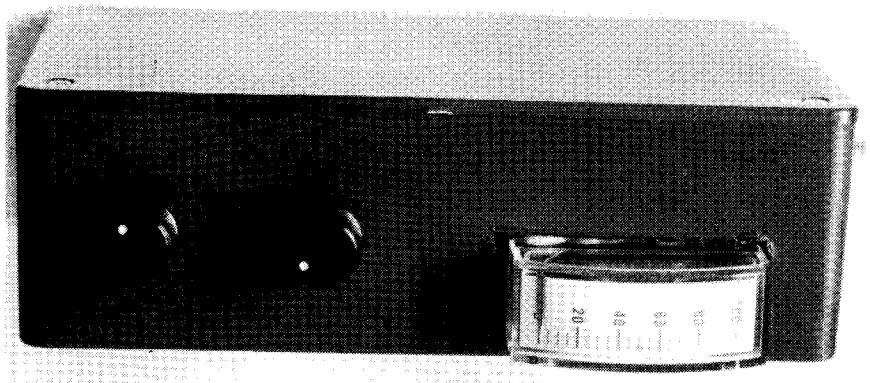
Note that, like lenses refracting light, a parabolic surface does not reflect all sonic frequencies the same way. Practicable reflectors, 1.5-2' in diameter, do not live up to the theoretical potential of parabolas due to their small size. Some sources suggest that a reflector 5 to 10 feet in diameter would fulfill expectations for the parabolic mic in the human speech band. Dead satellite dishes may yet find a use....

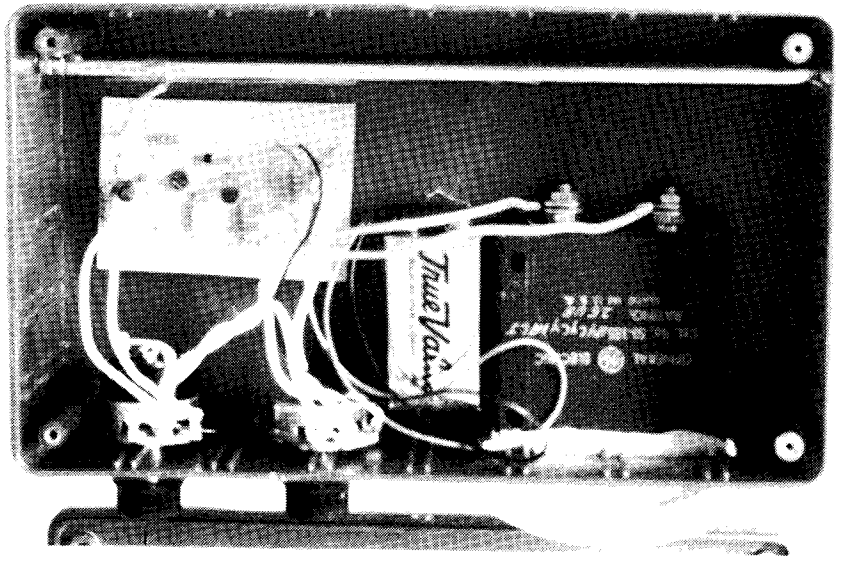
To get a look at parabolic mics in action, simply watch pro football any day of the season. You will see authorized sound men (it's illegal to do this without authorization) roaming the sidelines, taping players, huddles, and coaches. It seems that the soundtracks get matched up with film loops that appear in "NFL Highlights" or some such.

Apart from recording gaffes for the NFL Follies and merry mirth, parabolic microphones can be used legitimately for, ah, recording bird calls—yes, that's it: recording bird calls. Because it's sure as hell illegal to point these sinister dishes at pre-trial litigants to record conspiratorial chats without their knowledge or consent....

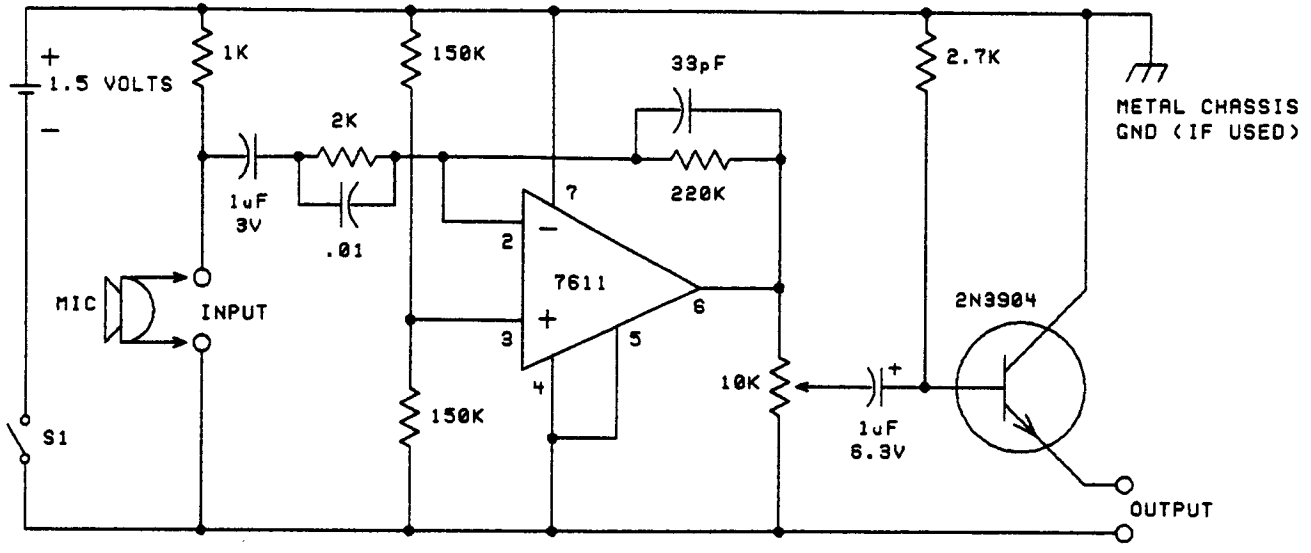


PREAMP DESIGNED BY JOHN WILSON, JR. AS FRONT END OF CUSTOM FM TRANSMITTER. FEATURES LIMITED BANDWIDTH (APPROX 300 Hz - 10 KHz) AND DIODE-PAIR LIMITER. OUTPUT MAY NEED TO BE COUPLED CAPACITIVELY TO NEXT STAGE.

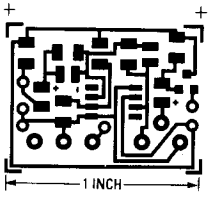


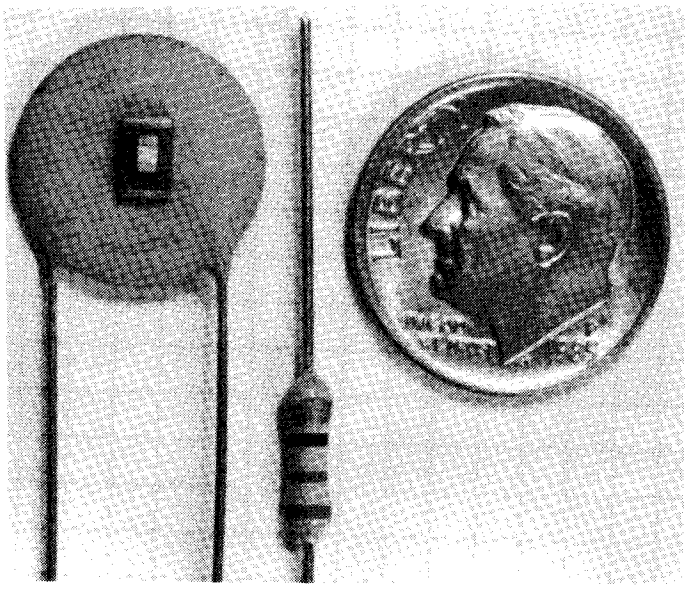


ABOVE: Schematic as described. ABOVE RIGHT and RIGHT: RF-sniffer built from plans designed by John Wilson, Jr. Extremely effective device could be cosmetically improved.



SCHEMATIC FOR AUDIO AMP USING SURFACE-MOUNT COMPONENTS OR CONVENTIONAL ONES. FROM "MICRO-SIZED AMPLIFIER," RADIO-ELECTRONICS MAGAZINE, AUGUST, 1988. COPYRIGHT (C) 1988 GERNSBACK PUBLICATIONS, INC. REPRINTED WITH PERMISSION. SEE TEXT FOR DETAILS RE: COMPONENTS.





TOP LEFT: Schematic for micro-sized audio amp. ABOVE: PC board template TWICE ACTUAL SIZE. Template Copyright (c) 1988 Gernsback Publications, Inc. Reprinted with permission. LEFT: 0.1uF cap and a resistor, along with their surface-mount electrical equivalents. SMD cap rests on standard cap; SMD resistor rests on SMD cap. You'll need a magnifier and tiny tweezers to handle SMDs....

Does the directional microphone have a place in modern surveillance? If it does, the author hasn't been able to find one that would not be better served by planting a small, sensitive mic/transmitter or recorder close to the subjects, so that variables such as wind-shift or overhead aircraft drowning out the sound could be eliminated. The size of most practical directional mics presents prohibitive risk of detection.

On the other hand, some situations offer excellent concealment for the operative, particularly the night, in which the mark is reasonably close.

LOW COST/NO COST

SPEECH PASSBAND FILTER

To make your ten-band graphic equalizer a speech passband filter, simply bump the 500, 1000, and 2000 Hz sliders up to max gain. Leave the 250 Hz and 4000 Hz sliders at zero. Pull the remaining sliders down to max cut. This will give you a roughly 300-3000 Hz passband. In the fortunate event you own a 27- or 30-band equalizer, you can both isolate the speech passband and play with ten slim bands within that spectrum to heighten speech and further cut noise. If the equalizer happens to be stereo, which in the case of home audio gear seems likely, feed the output of one channel into the inputs of the other. This doubles the number of decibels of boost/cut. (Beware that the input and output impedances may vary tremendously in the same unit. Consult the spec sheet, assuming you still have it. You may have to provide a matching transformer for max performance.)

POOR MAN'S COMPRESSOR

Those who own a cassette deck or open reel deck with dbx[tm] noise reduction can try this: Dub the recording, processed and equalized to the max, onto the deck using dbx. Then play it back with dbx switched out. You will hear it compressed 2:1. Loud peaks that battered your eardrums will be smoothed. Soft passages that escaped will magically rise to audibility. You can even repeat the process from a clean enough master for 4:1 compression.

Be aware that dbx applies a sharp treble pre-emphasis, so you should set up to apply hard treble cut to the playback to avoid excessive hiss, though this pre-emphasis may benefit cases where accented sibilants heighten intelligibility.

CHEAPEST PARAMETRIC

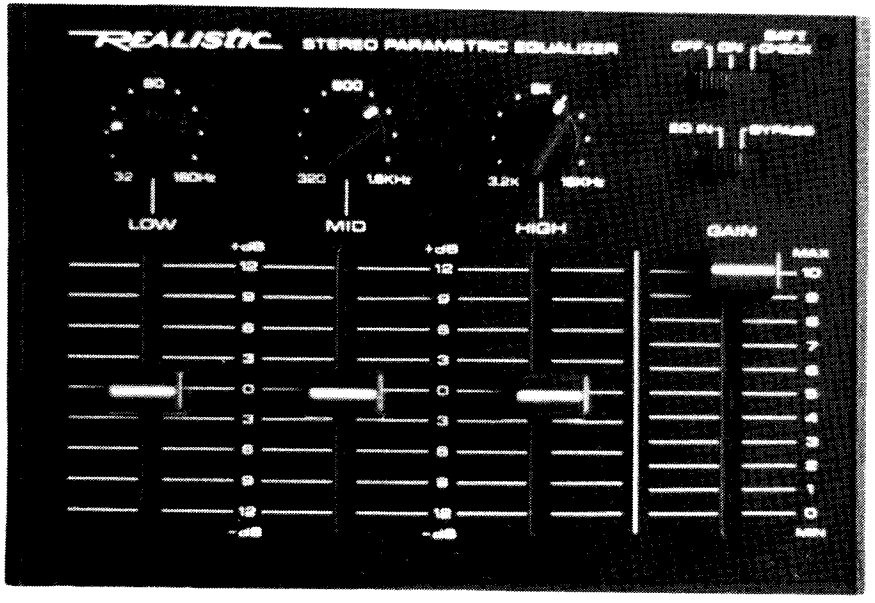
Retailing for $39.95 but available on sale at $29.95, less outboard power supply that adds another $10 to the tab, is Radio Shack's Model 32-1106 3-band semiparametric equalizer. We say semiparametric since the unit lets us adjust center frequency and boost/cut, but not bandwidth. It is not a true parametric, yet our tests proved it useful in post-processing of recorded human speech that had fed through a 300-3000 Hz passband filter and a compressor. The unit runs on batteries, but the power supply saves rubles in the long run.

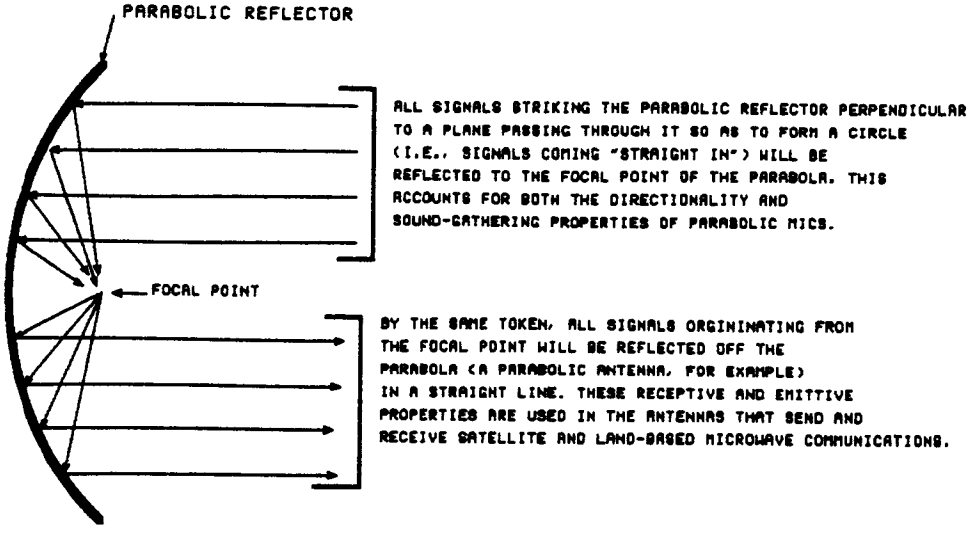
This is a stereo unit. As with a graphic equalizer, one potential mod feeds the output of one channel through the input of the other. This expands the degree of boost/cut, but note that this unit's rated input impedance is 50,000 ohms, its output impedance 250 ohms. That means interposition of a matching transformer; or perhaps not, since some attenuation of the signal may be needed in order to avoid overloading the second stage. Mouser Electronics carries transformers that would match the feeds if needed.

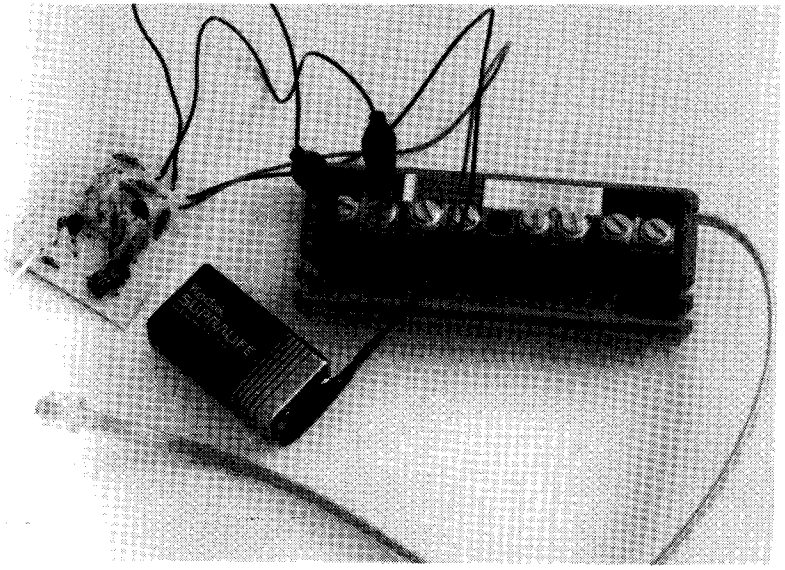
* * *

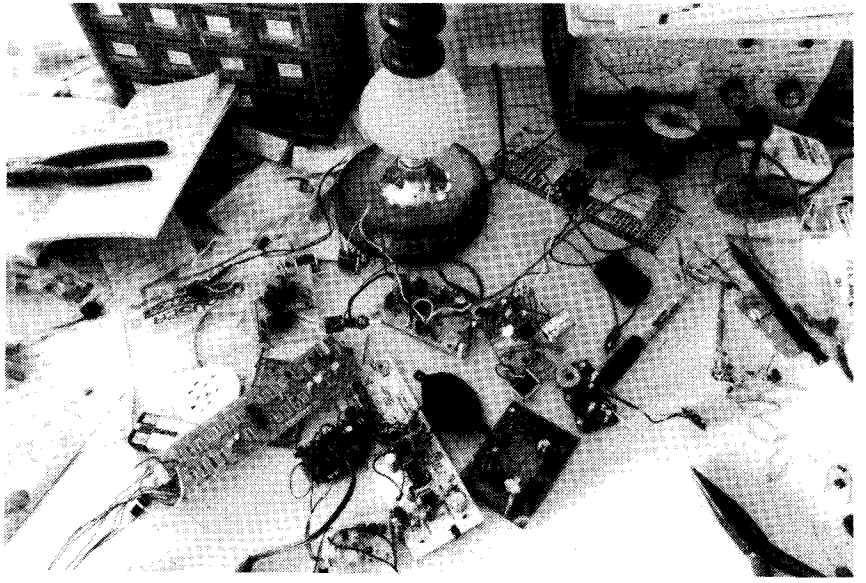
DEBUGGING

A huge business in debugging gear and services exists. It renders some types of bugging harder, but the aggressor has always enjoyed the advantage and always will. A genuinely professional debugging sweep may force snoopers into other modes of operation, but will deter only wimps. Debugging compares with faith-healing in that the buyer gets peace of mind, rather than visible results.

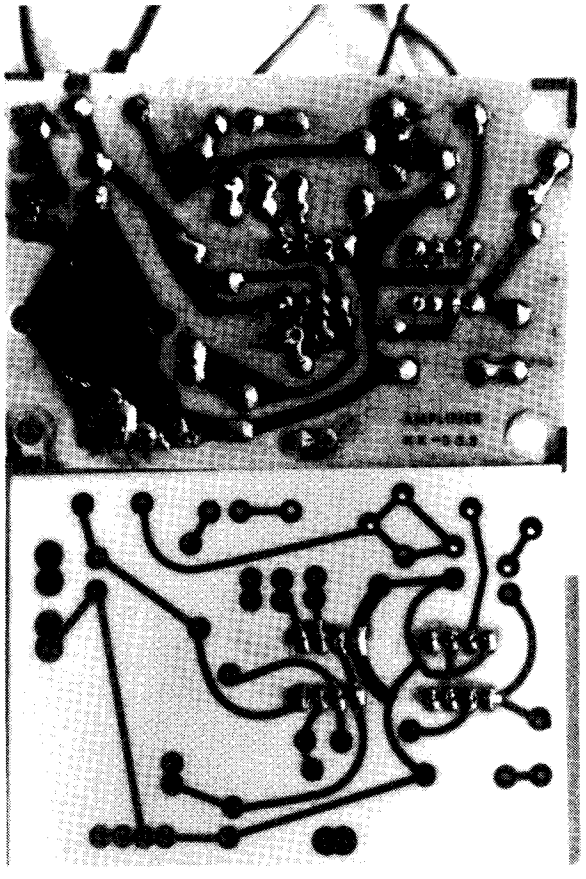


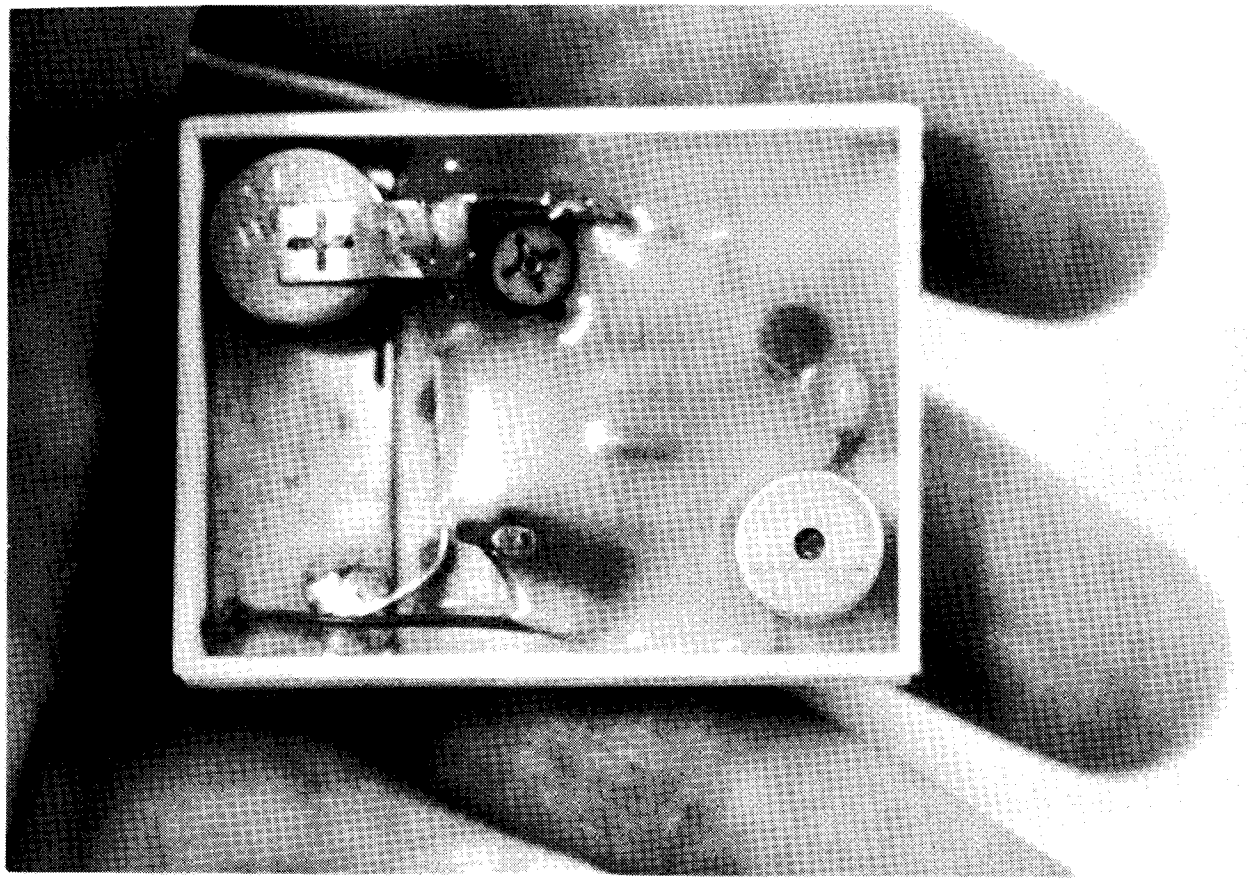






TOP LEFT: Radio Shack semiparametric equalizer. TOP RIGHT: Illustration of certain principles of the parabolic surface. BOTTOM LEFT: Experimental transmitter hooked up to modular phone block. Incidentally, in this configuration, it won't pick up a thing: both clips are on one terminal. Second clip should hook to adjacent terminal (green/red pair). BOTTOM RIGHT: The wages of sin....





TOP LEFT: Top is professionally made PC board for single-tube listener amp; below it is a functional copy made by visual estimation, except for the IC socket pads, transferred by rub-ons. LEFT: Life-size PC template for single tube listener project from January, 1988 issue of Hands-On Electronics. ABOVE: The real thing: custom-made body-worn transmitter actually used by enforcement agents. Unit loaned to us by John Wilson, Jr.

The ease of bugging has changed our behavior, since the most effective countermeasure refuses to expose sensitive information to bugging, and the only way to assure security of some material is not to expose it.

Other spook books have done a superb job of profiling technical aspects of debugging phone lines, residences, and so forth. Rather than rehash that, we punctuate the behavioral changes occasioned by the fact of bugging.

WHITHER BUGGING?

First, think of yourself as a prospective wire-man, in legal contexts only, such as taping phone conversations or taping face-to-face. Discretion will multiply the worth of what you have many-fold. Gather the data, then hold it in reserve until you can use it to defend against betrayal or scurrilous attack. The boss said you'd be VP by 1994? Play the tape for the jury after he has perjured himself.

Never reveal to anyone, including your wife (especially your wife; the divorce rate runs 40 percent and up, and jilted wives can be the most vicious enemies; they'll squeal even to the IRS....) that you have taped conversations. Those tapes hold heavy artillery. Bring it to bear only when the outcome justifies the inevitable stigma of taping. Afterwards, no one, if you do not have to leave town, will speak frankly in your presence.

Now think of yourself as a potential victim. Be careful what you say. It may be going on record. If you later have to swear as to the substance of a conversation that even might have been taped, well, maybe your memory ain't so good, Your Honor....

THE ETIQUETTE OF GETTING CAUGHT

Floods of material tell us how to make and use bugs. Let no one claim that material counsels us well in not having the bug betray us. Those who understand the rote behind detective work see where the point leads.

First, if you left a paper trail showing that you bought parts, kits, plans, or other paraphernalia to make the bug, the cops pretty well understand that you did. A Miami lawyer with the right connections might sway the jury toward reasonable doubt but it would be a close and costly call.

Second, it's hard to assemble a bug without leaving some trace of oneself, particularly since the advent of DNA coding that takes a microscopic mote of skin and matches it with your skin as surely as a full set of prints. Other traces prove less impressive, but no less damning. For instance, if you cut a printed circuit board with a hacksaw, the heat's forensic lab can match the cut edge of the board to the saw...and when the heat snatches the saw itself in a raid, and finds particles of phenolic circuit board and copper on the blade, well, the jig is up. Fingerprints: you might not leave a whole print, but enough partials to offer circumstantial evidence.

Third, will the heat find corroborative evidence in the form of spook books and catalogs of surveillance plans, gear, or raw electronic parts when they come a-knockin' in the wee hours? Have you bragged on to cronies about your electronics prowess? Do your computer files contain references to bugging?

Fourth, do you own a "special" receiver that tunes to the bug's frequency; or some exotic infrared 'scope good for nothing save sucking the audio out of IR radiation? Can you spell "plea bargain"?

Fifth, can the opposition establish that you had access to the bugged premises? That you had a motive for bugging? Circumstantial evidence, but it mounts.

In short, building and using bugs digs dozens of ditches that lead straight to you, should the bug surface, unless you see to it that all avenues terminate in dead ends. This may mean destroying or discarding a great deal of expensive and otherwise useful equipment months in advance of putting a bug to work. Analyze it: the cost of those goodies compared to the cost of defending against criminal prosecution, or the terrible price of conviction on a felony rap. Bugging is illegal. Don't do it.

2
ULTRA AMP

When in doubt, bore it out.
—Harley Davidson

* * *

Researching this book made the author aware of the range of complex and useful electronics that had been shrunk and laid out on tiny silicon slabs known as integrated circuits. Study poisoned his mind with absurd delusions that he might actually make something handy from these ingenious building blocks.

To shorten it, he bought the Heath Basic Electronics Course, along with its breadboard and built-in power supply, and started connecting chips on the board.

Most early projects failed. Each maddening flop exiled the breadboard to the closet until the next attack of delusional grandeur hit, then out it came for another grim try.

Eventually, and mostly through trial and error, rather than the wisdom of texts, chips began to do what they were supposed to do. Those lessons breathed life into what had been hazy knowledge, letting the author successfully breadboard active filters, a graphic equalizer, a true parametric equalizer, a compressor/automatic level control, and several extremely high-gain/low-noise preamplifiers. Note that harnessing the wizardry of chips distilled to rigging circuits, or their empirically derived variants, lifted straight from manufacturers' data sheets. No true engineering was involved. The circuits printed here originated with makers of the respective chips, not the author. He merely swapped components until the chips did his bidding.

The next frustrating round of failures plagued pathetic attempts to mate those individually working blocks into a unit he had begun to call—in a funk of black humor, since it did not exist—"Ultra-Amp."

The idea behind Ultra begged to include in a single device everything the serious spook might want, giving him the power to perform post-processing in real time and in the field, rather than make helpless recordings for later rescue using discrete and expensive bench gear. Put it all in a portable box that would ease the work.

Dedicated preamps, compressors, passband filters, tunable notch filters, and equalizers offer outstanding performance. That surprises no one, since pros engineered the gear and it costs a bundle. Yet so far, no one seems to have packed it all in one case, simple as parts-shrinkage has made that task. High-gain/low-noise audio preamps offer astounding performance on a chip. Choose from the National Semiconductor LM381, 382, or 387; or the Signetics NE542, which the author found pin-equal to the LM387. The NEC uPC1571

compander chip puts 2 channels of compression or automatic level control in a 16-pin DIP (dual inline pin) package. Almost any current-generation, high-performance operational amplifier will serve for brewing those dread active filters (as in "speech passband"), or the parametric equalizer described in Audio IC Op Amp Applications, or the graphic equalizer from Signetics' data sheet on its 5532/5534 series of chips.

The author mentioned offhand this bent concept of the ideal spook amp to some folks connected with Registry Distributing (yes, an authorized dealer for this book), and showed them a crude prototype he had fashioned after playing with breadboard versions for a few weeks. He thought nothing further of it. Six months later, Registry let him know in ominous and secretive tones that their Ultra-Amp model existed. They had molded it in the image of perfection, like some electronic Pygmalion. Did we wish to wring out the unit? You betcha.

Review the block diagram in the last chapter that mapped the electronic path audio follows on its way to discerning ears: input, preamplification, frequency limiting (usually the speech passband), compression, and parametric equalization. Compare it with the more explicit block printed here. There is nothing superfluous to any of these steps. Ask agents who've used, or tried to use, directional mics in the field. Turn up the gain to catch bird calls or authorized conversations, and background noise drowns it. Second-drawer electronics pollute with their own noise, impossible to banish.

In terms of power spectra, about 80 percent of background noise lies far below 300 Hz, the arbitrarily chosen lower limit of the speech band. A filter that eliminates sound below that band isolates the human voice. We needn't put up with the roar of traffic or the boom of surf 3 blocks away. Simply thread the signal through an appropriate passband filter.

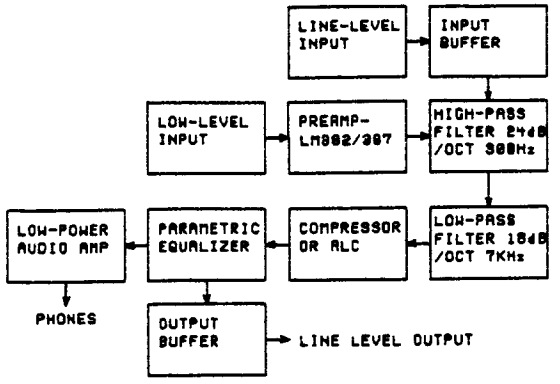
Filters differ in many particulars, one called slope. Slope measures how quickly response drops off below the nominative cutoff, generally taken as 3 dB below input level. Steepness of slope is expressed in dB/octave. For obscure mathematical reasons, this occurs in multiples of 6 dB, each multiple corresponding to one "order." For example, a first-order 300 Hz high-pass filter rolls off lazily at 6 dB per octave below the cutoff. A second-order filter rolls off at 12 dB per octave, and so on up to sixth-order filters that slash an incredible 36 dB per octave. A 150 Hz signal should be 36 dB down, a 75 Hz signal 72 dB down—inaudible in any practical sense—and signals below 75 Hz near-nonexistent after passage through such a filter.

Ideally, we seek infinite slope, impractically attained with real-world electronics. The sharper the roll-off, the more complex the filter design, the more components it needs, the tighter their tolerances, the costlier parts become. Compromises in specs need not compromise performance. For instance, if tests showed that we needed a 300-3000 Hz passband filter with 24 dB/octave slopes at each end to get usable noise reduction, we might try a simpler design with 18 dB slopes, but shift the cutoff points to 500 and 2000 Hz. At press time, we had breadboarded low- and high-pass filters with 18, 24, and 36 dB/octave slopes and found that they performed "as advertised" and behaved well when mated to other parts of the chain, though they do demand attention to details outlined in the Active Filter Cookbook.

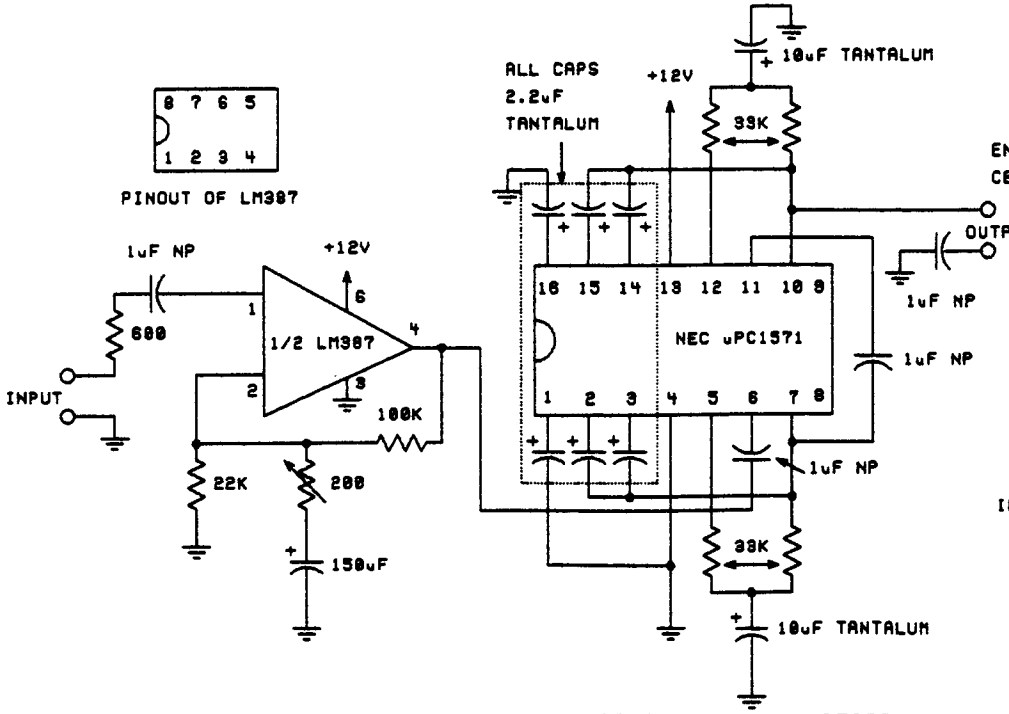
As an experiment, we rigged an LM387 low-noise preamplifier on a breadboard. We fed it with a wide-range electret mic and monitored the output using a pair of high-quality 600-ohm headphones. Note that this IC will drive high-impedance headphones directly, with a few safety precautions; it is probably best not to use low-impedance phones, which the chip might see as a short circuit, not good for it. We configured it for "high gain," on the order of 70 dB in a single stage.

The apartment was dead quiet before we switched on the amp. Instantly, the roar of otherwise unheard traffic passing blocks distant filled the phones. Then the refrigerator kicked in. It screamed like a leaf-blower in the throes of death. As we listened, we became aware of what our spectrum analyzer had foretold: We live in a torrent of high-power low-frequency noise. Wideband amps don't discriminate. They amplify whatever the mic feeds them. Our otherwise subsonic footfalls overloaded the amp with every step. (Incidentally, 70 dB of gain forced us to move at least 10 feet from the mic to stem feedback that pierced the phones like the banshee wail; the phones weren't sealed.)

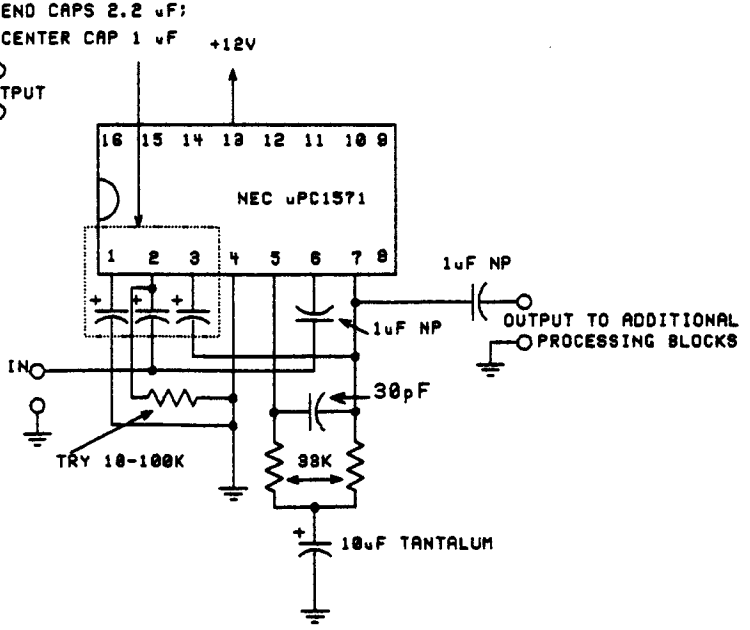
We could hear our own whisper from another room 20 feet away, though the now-overwhelming background



BLOCK DIAGRAM OF THE OMINOUS "ULTRA AMP" FILTERS, EQUALIZER, AND COMPRESSOR SWITCHABLE IN/OUT OF CIRCUIT.



FIRST STAGE IN GENESIS OF "ULTRA AMP," WORKED WELL ON BREADBOARD. uPC1571 CONFIGURED FOR DOUBLE COMPRESSION. 200-OHM VARIABLE RESISTOR TRIMS GAIN. TESTED W/ELECTRET MIC, WHICH GAVE TOO MUCH LOW FREQUENCY RESPONSE. REDUCED BY CHANGING 1uF CAP AT INPUT TO .01-.001; EXPERIMENT FOR DESIRED RESPONSE.



uPC1571 CONFIGURED AS ALC.

noise masked it. The test grew tiresome and painful after less than 3 minutes of that raucous roar. Though the preamp doubtless contributed noise of its own, despite an exemplary S/N ratio, we could detect no noise from it under field conditions, in contrast to some other amps we had tested; they tended to drown in their own noise.

The experiment taught intuitively that removal of sound below 300 Hz would multiply the utility of the setup by muting low-frequency roar. After checking the input capabilities of various integrated circuits—these low-noise preamps will not take more than about 300 millivolts input without overloading, perhaps suffering damage—we decided to add a high-pass filter.

It is hard to overstate the sense of physical relief that filtering brings. Rumbles, roars, and booms made by common appliances and other sources of ambient noise fade to the background, freeing the listener to concentrate on speech-band material.

Experiments with low-pass filters provided a few non-surprises. First, using a filter sloping down at a modest 18 dB/octave, taking 3000 Hz as the cutoff—the speech passband's arbitrarily defined upper limit—reduced intelligibility to some extent out of its muting of sibilants. This was particularly noticeable with whispers. As the last chapter pointed out, consonants contribute most to making speech understandable. To our ears an upper cutoff in the vicinity of 7000 Hz muted hiss without muffling sibilants. Thus, Ultra-Amp's speech passband filter spans 300 Hz at 24 dB/octave to 7 KHz at 18 dB/octave.

Registry designed the filters from material in Don Lancaster's Active Filter Cookbook. We noted slopes they chose for the test unit, but heard them babble insanely about pushing full-bore to 36 dB/octave in production models. Don't hold them to those comments; they smack of gibberish blurted at the height of a bad amphet-amine rush....

GAIN?

Let's clear up a point uncovered in research, but which may mislead the builder mulling which chip to use. National Semiconductor makes the LM381, LM382, and LM387 high-gain low-noise audio preamplifier integrated circuits. Their specification sheets rate them with gains of 112, 100, and 104 dB, respectively—but these define "open loop" gain. Practical audio circuits rarely achieve that. Though stated in spec sheets, open loop gain relates in useful terms only to designers figuring a chip's potential. At open loop gain settings, usable bandwidth slips to the low bass region, usually to subharmonics, fine if amplifying rumble suits the gig. In addition, some type of breakdown, often related to mutual inductance or "stray capacitance," plagues high gain by destabilizing a circuit or shutting it down. The best we could do with an LM382 was rig it per the manufacturer's instructions for 80 dB of wide-range gain in one stage, which closes in on the limits of current audio integrated circuits. This proved more than adequate.

Sequential amplifiers can boost total gain to 120 dB and more, but take it from those who have endured this prodigious feat that situations needing that much gain arise rarely in audio monitoring.

For high gain and low noise Registry used an LM382 set for 80 dB of raw gain. They could have used an LM381 or 387, but perusal of spec sheets showed idiosyncrasies that made this the most versatile and stable choice. It worked first try, with minimum external parts. (And check out National Semiconductor's Application Note 64 on the LM381, from 1974. Do you truly want to wade through that ghastly math?)

As it stood, this combination gave higher gain with less noise than all units we had tested up to that point. But Registry would not rest. They insisted on making life easier by incorporating a compressor in the next stage. They deployed an NEC uPC1571 compander chip, and configured both channels for compression, then fed the output of one channel into the other for double compression. At full gain, we could whack the mic element itself, but the compressor would instantly mute the boom; or quiet the room and hear the circuit automatically boost the signal to catch our most furtive whispers. (Do not repeat the mic-thumping test, especially with high-output crystal mics. It may kill the preamp.)

Initially, a compressor seems to accentuate noise, or at least hiss; but analyze its actions. First, as a complex electronic circuit, it suffers its own electronic noise. Second, in environments too quiet to trigger

its damping, it automatically boosts gain to a set level. This amplifies otherwise inaudible ambient noise, as well as noise in the electronics. As soon as some sound above its threshold clicks in, the hiss mutes, as does the level of the new sound, since the compressor minimizes dynamic range. It will kick whispers up to audibility, yet clamp loud sounds so they don't overload the tape—or your ears. Some prefer manual gain-riding to the compressor, no problem, since it's easily switched in or out.

By altering the circuit a bit, the uPC1571 becomes an automatic level control. Frankly, the subjective difference between an ALC and a compressor seems to be one of speed and degree. The ALC proves relatively conspicuous in its actions: loud tones mute sound output in a dramatic way that takes a fraction of a second to recover—sort of a breathing/pumping effect. The compressor, on the other hand, seems inactive until switched out of the circuit. Then unpleasantly loud sounds resume their noisome level. The author found both circuits useful, and selection dictated by ambient noise and personal taste. Ultra lets the user choose either.

Despite the speech passband filter, noise remaining within the band became obnoxious at the incomprehensible total gain supplied by the preamp and compressor chips in sequence, so Registry inserted a manual attenuator to let the user cut the amount of boost the compressor would apply during quiet periods. The diagrams show a preliminary double-compressor circuit based on the LM387 and the NEC uPC1571 that worked predictably and reproducibly on the breadboard. A second schematic differs only in that the uPC1571 is rigged as an automatic level control. We successfully transferred both designs to printed circuit boards, but considerable reworking will be needed to achieve peak performance of this chip-pair.

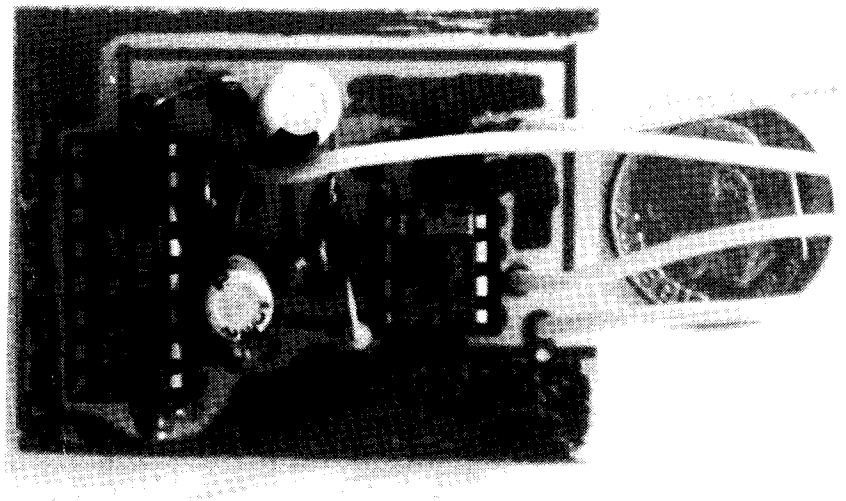
Finally, they recognized that noise in the speech band might need further reduction or speech further boost. So they tagged on a true, 3-band parametric equalizer with overlapping coverage as the final stage of signal processing. Continuously adjustable boost/cut, center frequency, and bandwidth. Engineering that stage proved a bitch, and Registry was undecided whether to keep it, or substitute a graphic equalizer limited to the speech passband. The graphic design cut flexibility somewhat, but required less breadboard engineering to get it just right as the parametric had. But working that true parametric was sweet: It let us literally "tune out" speech-band noise from a refrigerator, and boost the high end a bit to accentuate whispered sibilants.

As if strategic features weren't enough, bells and whistles were added. Ultra-Amp provides for low impedance mic, high impedance mic, and line-level inputs. It offers outputs for high impedance and low impedance phones, and a line-level output for a tape recorder. And it incorporates circuitry to protect it from simpletons, such as the author, who "accidentally" reverse polarity of the power supply.

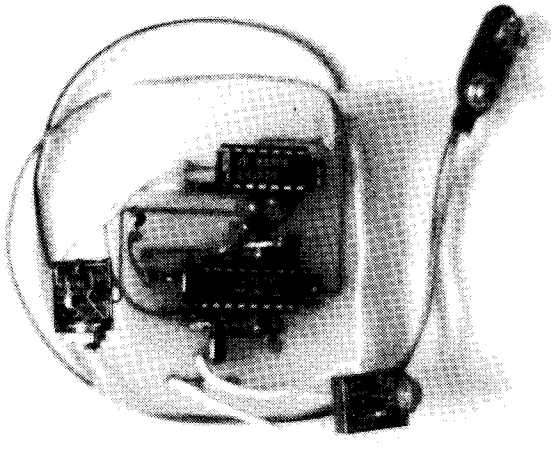
Detailing Ultra-Amp's feats compares with reviewing a Kloss Novabeam 6-1/2' projection TV which, by chance, the author once owned. A magazine review that reported on an early Kloss around 1980 said something to the effect that "It's hard not to sound gushy after watching the Novabeam." Having owned one for 5 years, the author agrees. Putting your vintage 19" color TV beside the big Kloss—the firm now sadly defunct—compares with using an ordinary spook amp in lieu of the great and powerful Ultra.

Writers tend to exaggerate. The author fought that terrible urge as he relates this anecdote, proved not one hour prior to typing these words. He set up the Ultra-Amp fed with Radio Shack's PC-mount electret mic element, and hooked Ultra's output into a pair of AKG-240 headphones. After tweaking the unit, he attached a 20' headphone cable, repaired to another room, shut the door, and whispered the opening lines to Green Lantern's Oath (circa 1962: "In brightest day, in blackest night....")—and heard the words easily, unmistakably through the headphones. As Will Sonnet used to say, "No brag, jus' fact." The divorcee in the apartment above was entertaining company. The author curbed the urge to scan that sinister conversation, as audible as if she had been in the room, this without resorting to a spike mic or pinhole mic, merely amplifying sounds that seeped down through the woodwork. Then he recharged his power ring and sprang back to the word processor....

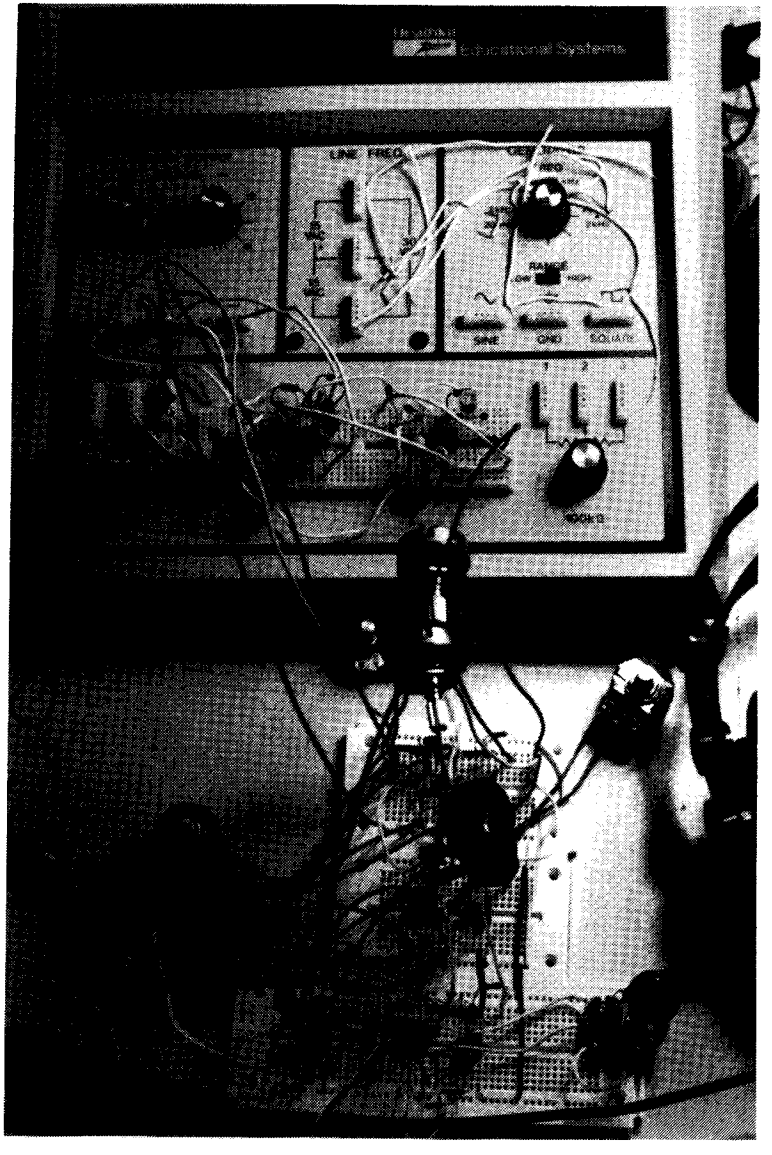
Even in prototype, Ultra-Amp impressed the author as the audio equivalent of "Robocop." In days that



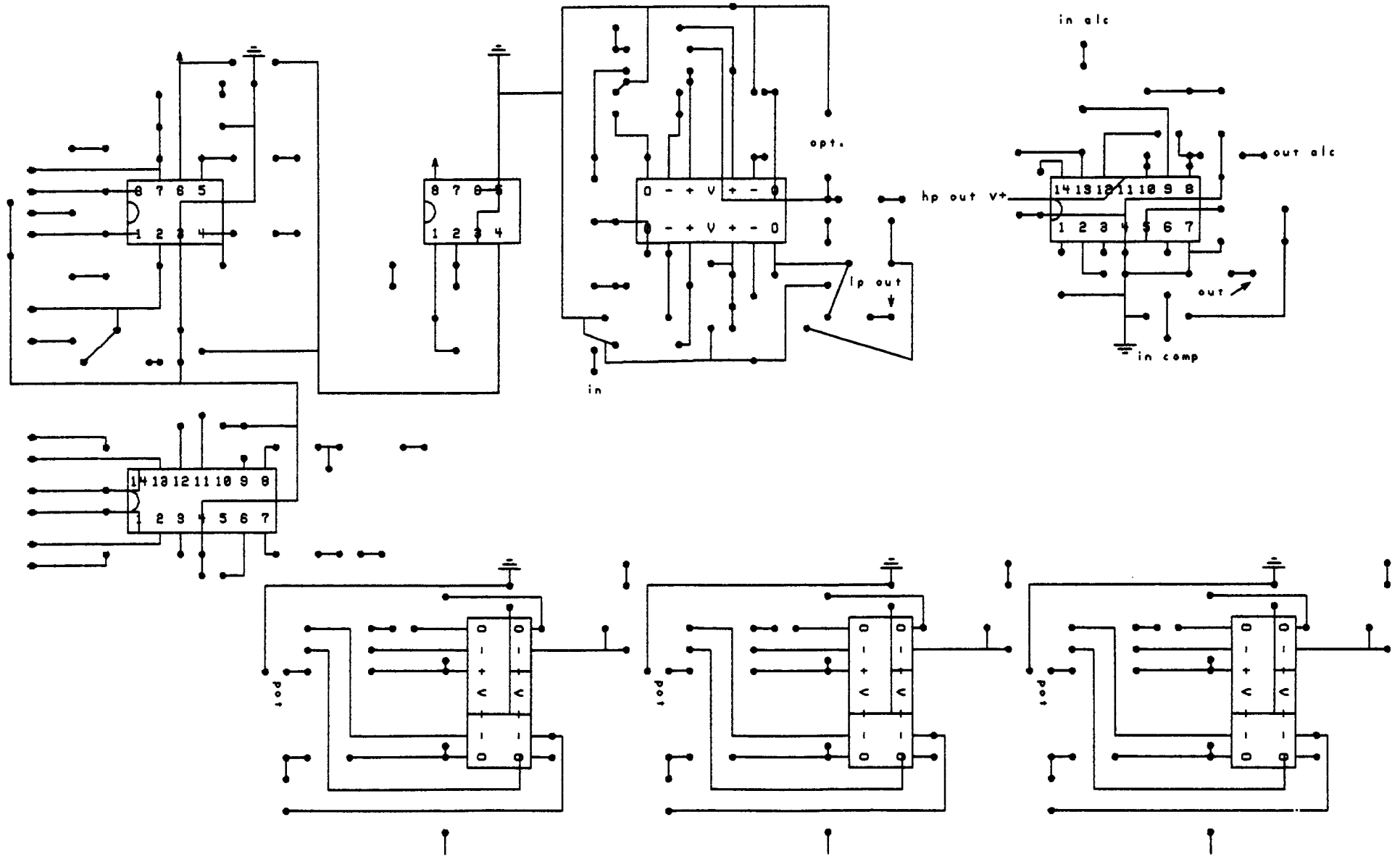
"Pre-Ultra" #1: LM387 feeding uPC1571 configured as automatic level control. Note tiny PC board. Tremendous performance for its size.



"Pre-Ultra" #2: LM382 feeding uPC1571 configured as double compressor.



First working version of complete Ultra-Amp on breadboard. On main board, from left to right, are preamp, speech passband filter, and compressor/ALC. Triple breakout board with potentiometers everywhere is a true 3-band parametric equalizer.



Computer Assisted Design program facilitates layout of PC board for Ultra-Amp, shown here about twice life-size. This first approximation still needs power supply and grounding routes, bypassing power supply at each op amp, limiter, and input/output buffers for parametric equalizer, but illustrates utility of electronic design aids. Far easier to change circuit electronically on screen than by erasure of pencil-drawn diagram.

followed, he tested it outdoors with several types of directional mics. The amps that had offered high gain and too much of their own noise simply couldn't keep up with a unit that let the operative tailor all aspects of performance on the spot: adjustable gain, selectable compression, speech passband option (most always left in), limiter when needed, and a true parametric equalizer for tweaking to peak thrust.

If devoting a chapter to a product in development seems extravagant, it's merely indicative of the disparity in performance between other units we had bought or built prior to exposure to the awesome power of Ultra-Amp. It gave greatest gain, versatility, features, and utility under field conditions.

As this goes to press, Registry Distributing has not finalized Ultra-Amp's design, but is gearing up to sell it in either assembled or kit form (they haven't finalized that, either), with all parts, a professionally etched and drilled printed circuit board with solder mask (a coating between pads that prevents solder bridges), and enclosure. They may offer sealed headphones to retard feedback and mask ambient noise, and other goodies they asked us not to speculate about. For latest information on Ultra-Amp's availability, write: Registry Distributing, 1616 17th St, Suite 372, Denver, CO, 80202.

* * *

AFTERTHOUGHTS ON ENGINEERING ULTRA-AMP

The bane of genuinely bad Math keeps most of us out of electronic engineering, at least engineering in the true sense of crafting a device on paper from knowledge of its behavior expressed in numbers—in essence calculating what should work before moving on to parts and boards. A professional engineer told the author that equations always come to life on the breadboard, a journeyman stage on the way to production, because what works in theory must prove itself in hardware.

What a twist that plug-it-in-and-see engineering leads inexorably back to that dread Math to solve problems in empiric design. Ultra-Amp proved a case in point. We had begun with a single-minded goal of incredible gain, achieved easily after a few false starts. But with that gain we met unanticipated problems knowledge of math would have alerted us to well in advance. For example, blocking: overload internal to the preamp that gave harsh, raspy sounds, produced by common room noises, such as footfalls or a refrigerator. With gain set high enough to capture whispers from behind a closed door we had to suffer blocking caused by louder ambient sounds.

A passband filter would not help here, since we could not place the filter in front of the preamp. Preamps excel at handling low-level, microphone-output signals—on the order of microvolts to a few millivolts. Some op amps used in active filters can handle low-level signals reasonably well, but filters aren't optimized for that task. They feel comfortable working with "line-level" signals, on the order of 1 volt peak-to-peak (P-P). We needed to cut low frequencies at the input, using a passive component: a capacitor.

Speaker crossovers use capacitors to pass high frequencies and block low frequencies. We can calculate the point at which signals pass or block based on a knowledge of the impedance and capacitance involved. In Ultra's case, we began with the manufacturer's recommended 1 uF input cap for flat response—far too much bass—and went to progressively lower values. We found that a polypropylene cap of 0.01-0.0022 uF cut bass response acceptably. Note that slope here rates only 6 dB/octave, such that we had to start rolling off response several octaves above the problem region, at the cost of some speech-band signal. But since we had a plethora of gain to start with, this proved no hindrance.

It turns out that chip-makers have designed their preamps to allow a modest degree of frequency-shaping. Though we cannot achieve the spectacular roll-off rates of active filters, in many cases we can adjust the high and low frequency response at the input to reduce system noise and eliminate other bugs, such as blocking. At first glance, Application Note 64 on the LM381 looks like a nightmare out of some college math text. On closer inspection we find: A) that those grim equations tell exactly what value of components will alter gain and frequency response, and B) that the average financial calculator makes duck-quiche out of solving them. Equations hide the power built into a chip. Math unleashes it. It hands us the quickest solution to what would otherwise prove a problemito.

But that was only the start. Total harmonic distortion of our compressor chip rises exponentially as its output tops 1 volt. That meant we had to engineer it not to exceed that to avoid a horribly distorted sound—which in turn meant we couldn't feed it all the gain available from the preamp, whose output can swing supply voltage minus 2 volts, P-P. Assuming a 15-volt supply, it can give us 13 volts output. The compressor/ALC squeezes just so much before it has to break the 1-volt output barrier, at which point the signal takes on serious elements of repugnance, along with raspy overtones of Tom Waits.

Then the active filters saddled us with gain problems. As this is typed, we have on the board one incarnation of Ultra that uses a high-pass filter with a 36 dB/oct slope, mating directly to a low-pass filter with a 12 dB/oct slope. This unavoidably boosts gain well over 15 dB. The chips handle it in stride. The snag? To switch the filters in and out of the signal path without a sudden lurch of 15 dB in level we must place resistors at strategic spots to drop the signal back to input level.

What of the parametric? We specifically designed it to have overlapping frequency coverage. In theory, we could choose an identical center frequency for all 3 bands, and boost the signal at that point 12 dB per band, a total boost of 36 dB. Given a 1-volt signal to begin with, that means an output near 64 volts. The chips won't take it. Here again, we must anticipate the occasional need to reduce gain to allow extremely powerful but narrow-band boost if needed.

It became clear that lower first-stage gain made an attractive option in this design that offered so much signal processing capability. The first stage would ease the mic-level input up to line-level, rather than boosting it into lunar insertion orbit. We can apply as much added gain as we wish at the end of the processing chain.

We haven't covered limiters, buffers, shielding, "bypassing the power supply," impedances, and so forth. It's all in the references cited at the end of the book.

Ten different engineers handed Ultra's aims would probably approach it 10 unique ways—all successful. Preliminary designs sketched here represent one approach, and a naive one at that. But we can't downplay the results: This crude project turned out a more powerful and flexible spook amp than any commercial unit we have seen.

3
VIDEO

The ineluctable modality of the visible.
—James Joyce, Ulysses

Smile! You're on Candid Camera!
—Allen Funt

* * *

Two types of visual surveillance gear bland in comparison to exotic and expensive night-vision devices are ordinary cameras and the latest generation of video camcorders. Since, on a percentage basis, we gather most material during daylight hours, it makes sense to examine these admittedly prosaic tools. Veteran photo buffs can skip this.

Cameras are devices that project an image onto a segment of film for a brief period, usually a fraction of a second. This changes the film such that chemical treatment will bring out the image in a way that we can use, and stabilizes the image so that we may access it in years to come.

In order for the image to be useful, it must have well defined edges and texture, i.e., must show sharpness and detail. These depend mainly upon: 1) focus, 2) stability of the image during exposure, and 3) inherent grain of the film. Assume that we can achieve proper focus. That leaves movement of the image and film grain as the major factors in sharp pictures. We'll return to focus when we meet lenses that challenge our ability to focus.

SHUTTER SPEED

The picture blurs if the image moves during exposure. But how much can the image move in the time it takes a shutter to click? Plenty. Enough to render the shot useless. With 50 mm lenses, commonly called "normal" lenses, since most 35 mm cameras come equipped with a 50 mm lens, the rule of thumb calls for 1/30th of a second as the slowest shutter speed that will not visibly smear the image, at least with reasonable care and hand-holding.

That rule applies only to 50 mm lenses. Lenses of greater focal length magnify the image. In so doing, they amplify the effect of camera-shake, and demand proportionately higher shutter speeds to assure a sharp image, assuming a still subject and hand-holding. Moving photographers with moving subjects call for still faster shutter speeds.

As a rule, the shutter speed should be no slower than the inverse of the focal length of the lens. If you are

using a 250 mm telephoto lens, shutter speed should not be slower than 1/250th of a second when hand-holding. Ideally, you would use a considerably faster speed if lighting conditions allowed. (Another ideal, often impractical in field work, calls for use of a sturdy tripod. Pros brace the camera with whatever is handy, since this added support heightens sharpness.)

FILM SPEED

A a film's speed measures its sensitivity to light. Slow film rates less sensitive, fast film more sensitive. A series of relative numbers designates speed. For example, 25 speed film takes 4 times as much light to give the same exposure as does 100 speed film.

Speeds of film available to amateurs ranges from 25 for ultra-fine-grain color slide film, to 3200 for color print film (Konica SR 3200; other vendors will probably match this speed soon; Fuji markets a 1600 speed, and Kodak has had a 1000 speed out for several years). Kodak just brought in its T-Max 3200 B&W film, which may be exposed over a range of 800 to an incredible 25,000 speed, though speeds above 3200 require special processing.

In most cases, we trade grain for speed: the faster a film, the grainier its image, the less it tolerates enlargement. It takes a professional eye to spot differences in grain between Kodak's 100 and 400 speed VRG color print films processed at the local drugstore and printed 4 X 6; yet grain is instantly apparent on Kodak's 1000 speed film and other, faster brands.

As with audio surveillance, we seek utility, not portrait quality. We will gladly trade a grainy image for the lens and shutter speed needed to snap the mark in flagrante delicto...whatever that means.

Recalling this business of shutter speeds, film speed relationships work this way: Let's say we have a brightly lit outdoor scene we wish to shoot from a distance of a quarter of a mile. We must hand-hold, and will be using a 1000 mm lens with a speed of f16. (F-stops are like film speed, a series of relative numbers to designate the amount of light a lens admits. But note an inverse relationship: The lower the number, the faster the lens, the more light it transmits. F16 is a slow lens requiring fast film, bright light, or both.)

Assume that our camera gives automatic exposure, since it is hard to find one without that feature today.

If we load 200 speed film in the camera, set the camera for 200 speed (we must tell its exposure computer what speed film we are using), and focus on the scene, we see that a shutter speed of 1/60th of a second will give proper exposure. For this telephoto lens, even using a tripod, that's too long. The image will be properly exposed but hopelessly blurred. We need a minimum shutter speed of 1/1000.

Mental calculation: changing to film speed 400 would give us a shutter speed of 1/120; film speed 800, shutter speed 1/250; film speed 1600, shutter speed 1/500, and film speed 3200, shutter speed 1/1000. We need 3200 speed film. What a relief that it's available, grainy but usable.

PUSH PROCESSING

You've loaded 400 speed color print film in the camera, but metering shows you need 1600 to achieve a shutter speed compatible with your telephoto lens and ambient light, in order to avoid effects of camera-shake.

Go ahead and set the camera for 1600 speed film and make your shots. But when you get them developed, you must go to a custom lab and tell them to "push the film to 1600" or "push the film two stops." Since the film was designed to give proper exposures at 400 speed, and since you took them as if the film could handle 1600 speed, you have underexposed the film by two stops. (A change of one "stop," up or down, refers to doubling or halving, respectively, the amount of light the lens admits.)

The lab can compensate to a degree by overdeveloping the negatives two stops. This leads to shifts in color, usually inconsequential in surveillance work, as well as noticeable degradation in detail. But that doesn't hassle us as long as the image remains usable.

Custom photo labs know what you're talking about when you ask for push processing. It would be risky to write "push two stops" on the photo envelope at the drugstore and ship off your roll. Mass processors tend to perform well with common films, but may bungle special requests.

If a given roll of film contains both normal and pushed exposures, you must decide before processing which ones to save. As a rule, the entire roll must be processed at once, meaning that alterations will affect all exposures. Normal exposures will be overexposed two stops by push processing the same amount.

Film varies in the amount of pushing it will take. Inherently fast and grainy films may take little, while fine-grain medium speed films, such as Kodak's recently introduced T-Max B&W film, 400 speed, tolerates considerable pushing.

TELEPHOTO LENSES

You will take most surveillance photos with a telephoto lens. If you have used binoculars or a hand-held telescope, you have seen that the greater the magnification, the harder it becomes to keep the image still. If you hand-hold a camera, or with extreme magnification and a tripod-mounted camera, the movement caused by the tripping shutter can blur the image hopelessly.

Subjects usually don't want to be photographed and the agent wants to escape detection, a combination problematic for the use of conventional cameras, lenses, and film for surreptitious photography. This demands use of telescope-like lenses. We must reconcile the power of long lenses with the laws of physics. These lenses pay a price for the you-are-there perspective they offer. They admit substantially less light, typically 1/4 to 1/64th as much, than "standard" lenses used for taking pictures of the reunion. The less light, the longer the shutter must remain open, the greater camera-shake, the more likely the image will blur into surreality.

We saw in the example of film speed above that increasing speed up to a point will let us use a slow, telescope-like lens. An alternative which only professionals or well heeled amateurs can afford calls for a faster lens, i.e., one that admits more light. Cost of a telephoto lens rises exponentially with its light-gathering power. Big-time lens makers market 400 mm telephoto lenses with speeds down to f2.8. Cost runs $2000 to $4000+, depending on quality, even at a discount. They are so big they require a separate tripod, and a sturdy one at that. Hand-holding is near impossible, and they mark the agent as badly as the bazooka directional mic.

THE CURSE OF CATADIOPTRIC LENSES

For genuinely long-range viewing with a lens of manageable size and modest cost, it is hard to beat the catadioptric ("cat"), or mirror lens, in essence a miniature reflecting telescope. The photo shows a 500 mm f8 cat with 2X teledaptor, which increases focal length to 1000 mm but drops speed to f16 (i.e., doubles magnification, but lets in only a quarter as much light).

The cat forces a trade-off. These lenses possess no usable depth of field. Depth of field refers to distance in front of and behind the focus point in which images remain focused. Depth of field of conventional lenses increases with smaller apertures. Focused on a subject 20 feet away, we might a get depth of field of 1 foot from a 50 mm lens with an aperture of f1.4 (wide open). An aperture of f16 on that same lens would put everything from 8 feet to infinity in focus, a huge depth of field.

Not so with mirror lenses. Even at extreme range, depth of field is almost nonexistent. Focus must be dead-on or sharpness will suffer. That and their notoriously small apertures make these lenses cruel and unforgiving for hand-held work, particularly using a moving automobile as a platform. As a field experiment, we attempted to capture scenes with a 500 mm cat whose nominal aperture was f8, this with 1600 speed film and the shutter set on 1/1000. Conditions were bright sunlight. We found it all but impossible to keep targets in focus while the vehicle moved. Thus, despite a bright sunlit day, fast shutter, and extremely fast film, proper photos were rare, none of them worth printing here. This changed when we stopped the car, focused carefully, and braced the camera on the car door.

If you own one of these lenses, try this experiment: Place the camera on a steady tripod. With 2X multiplier

500 mm catadioptric lens w/2X multiplier attached, a deadly combination of camera and lens for long-range work on a budget, but with strict limitations. See text.

in place (1000 mm focal length, aperture f16), focus on a distant object, with no film in the camera. Set the timer to trip the shutter, then keep your eye glued to the viewfinder. It will blank momentarily as the mirror comes up before the shutter clicks, but when it drops back you will see a marked shake in the picture. It may oscillate for more than a second, depending on how the camera is mounted. Also, have an assistant walk normally past the setup, if the floor is made of wood, and note how the highly magnified image jiggles.

These lessons teach that despite use of a tripod, you still have to use shutter speeds fast enough to keep the image from smearing out of camera-shake induced by the movement of the mechanism; and that vibration imperceptible to the operator will smear the picture.

Many who buy the 500 mm f8 cat become disillusioned with it quickly because of its drawbacks. Yet nothing comparable offers so much magnification in a small, lightweight package, for less than $200. By observing the rules of fast film, sturdy tripod, haze filters, and fastest possible shutter speed, these lenses can produce images usable in field work, the only criterion of worth when considering what gear to buy.

A 2X multiplier is available for this lens, which brings its focal length up to 1000 mm but drops the aperture to f16. We were able to take hand-held shots, but only with 1/1000 shutter speed, stationary targets, and lots of time to focus. We obtained best results using a tripod.

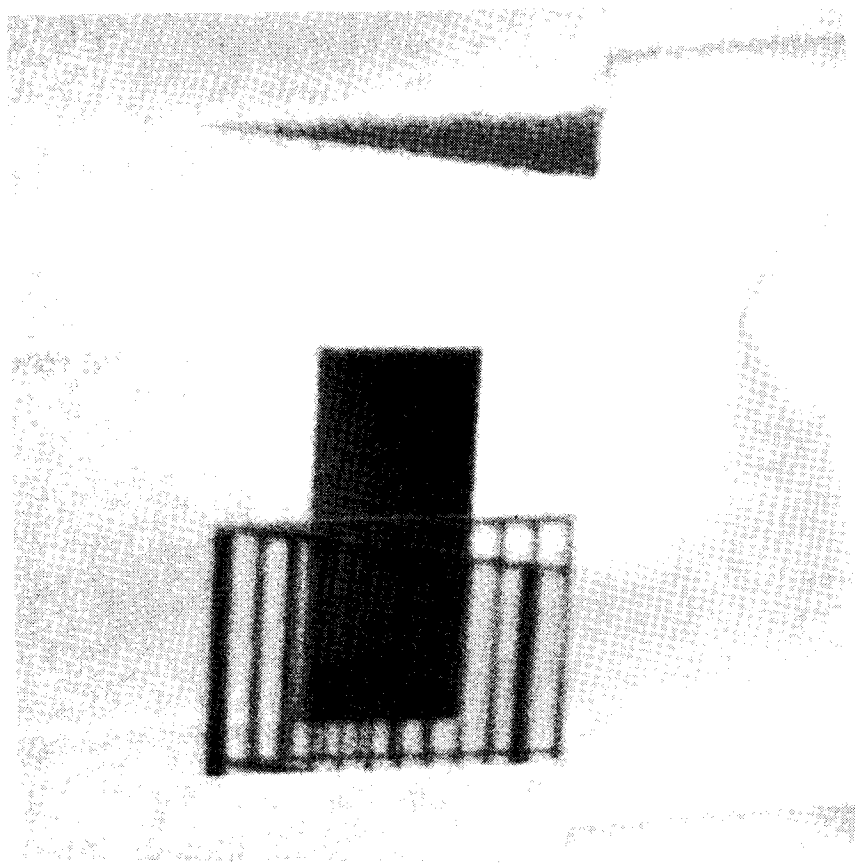
The CCS catalog lists a 4800 mm lens (f27.5; that's one dim image). Camera shake generated by the shutter alone, even with the whole setup double-tripod-mounted, would leave us with unnaturally blurred photos. At that tiny aperture it's doubtful you could get by with shutter speeds slower than 1/1000, needed to obscure the effects of camera shake.

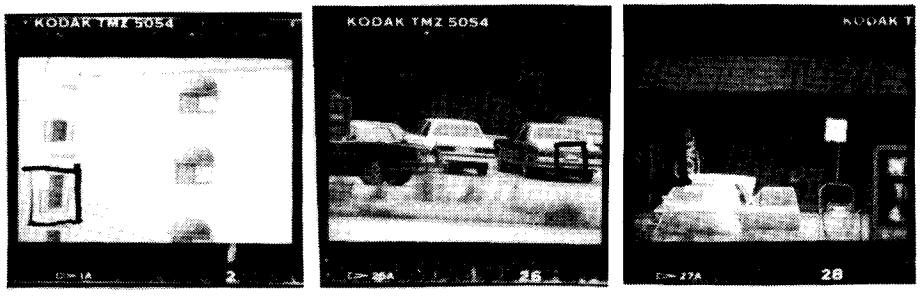
Kodak's recently introduced T-Max 3200 speed B&W print film has breathed new life into long/dim lenses. Using special developer, a custom lab may push this film to 25,000 while maintaining "surveillance quality" images. Realize that film this sensitive calls for special handling. Ideally, shoot and develop a test-roll prior to any serious work. We were a bit conservative in our experiments, exposing a roll at 6400.

The high speed proved to be both a blessing and a curse. Our camera, an old but trusty Canon A-1, rates a top shutter speed of 1/1000. With the 1000 mm f16 lens mounted, shooting in bright sunlight, we needed a faster shutter often. Most current top-of-the-line cameras will go 1/4000, and one of Nikon's latest models will hit 1/8000. Alternatively, we could have used a polarizer, which cuts light transmission by roughly 50 percent, or a neutral density filter of whatever strength needed; or we could have stuck a few fingers in front of the lens to reduce incoming light; or we could have exposed the entire roll at 3200, but we wanted to see what this film would do in the middle of its rated range. If only the cat could stop down (i.e., tighten its aperture on command from the camera to get proper exposure; one vendor does sell a cat with this feature; check the ads in the back pages of the photo magazines). At present, Kodak T-Max 3200 is the odds-on choice for telephoto work where low light and/or a slow lens figure into the scenario.

An alternative to high-powered low-speed lenses calls for a shorter tele capable of a larger aperture, say, f4, with slower, less grainy film. Your photos will lack that immediacy of the high-mag lens, but you are dealing with film of finer grain. Four-hundred speed color print film performs well with an f4 lens, particularly in bright sunlight. Even slower films, with correspondingly finer grains, become practical as the amount of light admitted by the lens rises. Their images will tolerate far greater enlargement than those of super-high-speed films. You will be able to get greater depth of field (almost any lens, even at maximum aperture, gives greater depth than the cat), with the option use slower shutter speeds and smaller apertures as demanded by the situation. These lenses also let you use a polarizer with greater ease than with a cat (see below).

Ordinarily, one would think night-scenes, which may call for exposures of several seconds, prohibitively dark, even with the sturdiest of tripods. Assuming the subject to be inanimate and immobile, that ain't so. One maneuver especially suited to night scenes involves mounting the lens on the sturdiest tripod you can get—weight it with sandbags if needed—then meter the scene. Let's say it requires 4 seconds to give proper exposure. Take it from those who have tried this that camera-shake produced by the shutter opening and closing will smear the image hopelessly. A plain black card provides the solution. Set the shutter to open for, say, 6 seconds. Press the delay button, and watch your timer. Hold the black card directly in front of the





Examples of photos taken with 1000 mm f16 cat and Kodak T-Max 3200 exposed at 6400 with proper push processing. Match frame w/enlargement. Balcony shot taken from 1 mile, hand-held 1/1000; enlargement showed it to be slightly out of focus. Other shots taken from 1/4 mile, hand-held, overcast, shutter 1/750. Note grain. You can almost read the license plate....

lens. When the shutter opens, wait a breath, then remove the card. This lets the otherwise imperceptible camera-shake subside before the exposure starts. Keep your eye on your watch. Replace the card a second before the shutter closes to prevent the less violent but still potentially ruinous shake as the shutter begins its path shut. The improvement in image quality will surprise you (and the marks, when you produce those startling photos in court).

STEADYCAM AND THE NEW TECHNOLOGY

The camera tracks Rocky Balboa as he sprints up the stairs of Philadelphia's Independence Hall. Bill Conti's soaring music swells in the background. It's as if we were running alongside Rocky—yet our vantage remains rock-steady and level, never bouncing with each step as his must.

The then-new instrument that let director John Avildsen track Rocky so smoothly was known as the Steadycam: a mechanically stabilized hand-held camera mount. Before its introduction, film-makers had to erect tracks on which to dolly their cameras to allow smooth following. The balanced camera mount let cinematographers hand-hold without marring the finished scene with that newsreel-like jarring we had come to expect from hand-held shots.

What has this to do with spooklore? Ask any telescope owner how useful a genuinely powerful instrument would be without a firm mount. It's impossible to steady it enough to make sense of what is seen. Or take the 500 mm catadioptric camera lens, often souped up to 1000 mm with a 2X teledaptor. It, too, provides almost prohibitive magnification for hand holding and usable images.

But what if our still, movie, or video camera were servo-stabilized? We could up magnification, hang visually onto live targets at ranges beyond their ability to see us without field glasses.

Steadycam is a right expensive piece of hardware. But you don't have to buy. You can rent for a few hundred dollars a day in limited section of the country, usually those whose denizens play the spook game and can afford to travel, whatever the fare.

The military uses this principle in the nose cameras of aging B52s and the new B1-B to let them see threats at near-radar range. Word is that we have the sensors and magnification to peer in on objects at spy-satellite distances, but practical limits in aircraft arise in not being able to hold the viewer still enough to attain a useful image at more than 50 miles.

The Japanese continue to show us the way. The latest generation of home video cameras—that term becomes hazier the faster tech advances—incorporates tiny servo-actuated motors to move the image sensor, a charge-coupled or MOS device, to compensate for jitters in the holder, just like Steadycam, only the works lurk inside the camera. An image sensor the size and mass of a nickel made this possible, with extremely low energy drain. Managing the same feat with older tube-type cameras would have proven economically impractical.

Resolution of video recorded images, at least short of high-definition TV, has not come up on par with that of the finest films, which are usually too slow for surveillance work. The classic, Kodachrome slide film, rates 25 speed, this compared with 3200 speed in the latest color print film. Of course, Kodachrome and similar slow slide films offer stunning color and detail. Print film of 1000 speed and above produces prints noticeably grainy, even when drugstore-processed. These do not tolerate enlargement well.

Note that electronically recorded images, whether moving videotape or the latest electronic still cameras, give us electronic signals which lend themselves to digital enhancement without the interstep of digitizing a print or slide.

CONSUMER VIDEO GEAR

We have reached an age in which common consumer video gear will serve genuinely useful roles in surveillance and other security related applications. The inside back cover of a recent issue of International Combat Arms contains an ad from Panasonic for its model WV-D5000 video camera: CCD sensor, workable down to 0.7 lux, 1/1000 shutter, auto white balance, etc. Newer cameras can drop shutter speed to

1/4000, enough to "freeze" extremely high-speed action. Others incorporate crude digital processing used mainly for special effects, though some get to the heart of the matter and enable taping in semidarkness.

Sony's recently introduced cigarette-pack-sized black and white camera mounts on a peephole. We needn't put our eye to the viewer. We can look at a hand-held LCD screen in some other part of the house to see what breed of werewolf has come a-knockin'. The image could be fed through an 8-hour cassette recorder for maintaining surveillance of areas over long periods. Digitally superimposed time and date are de rigueur.

Pinhole cameras—the ones that poke through tiny holes in walls to serve FBI sting operations—have been outmoded by a camera whose pickup will fit inside a lipstick case. Trailing a sinister black cable, it uses MOS sensors to provide resolution in the VCR class. It looks to be one tenth the volume of a unit shown in CCS catalog, with potential for concealment in almost anything—including the ladies' lipstick case.

It will not be long before video sensors become so small that previously impossible visual invasions will become commonplace. Dick Tracy's 2-way wrist TV will have become reality.

AUTOFOCUS

This feature has just begun to appear in lenses, some zooms, that approach useful tele focal lengths, 210 minimum. The various mechanisms have yet to prove themselves in surveillance work, since they might choose the wrong moment to focus on the windshield of the car, rather than the target two blocks ahead. Manually focused lenses may demand constant attention, but at least we know where they'll be locked when the shutter clicks.

TAKING PICTURES FOR REAL

Questions: What, or whom, do you want to photograph? Under what conditions? With the subject doing what? These and countless other variables dictate your camera, film, lens, and technique.

Practical tests on persons in public places quickly pointed up the major prerequisite for successful surveillance photography, assuming adequate technical skill: patience, and lots of it.

You may have to sit, stand, crouch, or kneel for hours with your eye glued to the viewfinder just to catch the subject in conditions that have worth to you or your client (for example, the pigeon and a female companion, framed in the doorway of Motel Delicto, just down from the Slow Club on Route 7....). Try to snap that shot in hot, muggy weather. Note how quickly you break a sweat, and how abysmally it fogs the viewfinder. Feel the muscles in your face and neck tighten to dull, aching knots. See how hopeless it becomes to hold the focus of a genuinely long lens. This explains why PI's charge $100 an hour for photo work....

Though many gigs don't let us use a tripod, be aware of the existence of rifle-stock-like camera holders that steady your aim considerably. Appropriately enough, they trip the shutter through a cable attached to a trigger.

HANDLING FILM

Film has a limited shelf-life. Exposure to light triggers chemical reactions that are happening right now, but so slowly that several seasons may pass before color-shifts and other tawdry changes render the film useless.

We will learn in a grim expose' of pyrotechnics that chemical reaction rates double for every 10 degrees C rise in temperature. That means that storing film in the fridge prolongs its shelf-life. High-end photo shops that serve professionals keep pro film in the fridge out of this very consideration. Since faster film, the type most useful for surveillance work, is most subject to these changes, it benefits most from a cool environment. Film targeted to the non-pro market is designed to "age" as it sits on the shelf at room temperature. Refrigeration stops this aging, which explains some authorities' advice not to cool non-pro films.

Remember that moisture condenses on cold surfaces. When you remove caches of film from cold storage, leave them in the unopened boxes at room temperature for at least an hour before loading the film.

It goes without saying that impounding film in your car's glove box on a hot day kills it as dead as Raid kills bugs. And if you left the camera in there too, kiss its microelectronics goodbye.

Though you can safely load most films in ordinary room light, it pays to play safe by doing so under the darkest conditions feasible. All film cartridges leak light to some extent. The briefer the exposure the less likely you are to lose prints.

Once exposed, get the film developed as soon as possible. In addition to yielding best results, this practice minimizes the odds of a loss or theft. For genuinely important film, bypass the drugstore for a custom photo shop: Nobody assumes liability for loss except as to replace the film. Your pix may be gone forever. Some mass photo labs have become notorious for losing customers' film. (And if the subject-matter is delicate, either go to a reliable custom processor out of town, or front for your own darkroom....)

AUTOWINDERS

The trend today leans toward built-in autowinders in most mid-to-upper-level 35 mm cameras, with continuous shooting modes that range from 1 to 5 frames a second. Outboard autowinders are available for most older models, at modest prices.

For surveillance work they are worth their weight in Haagen-Dazs. That quick flip of the thumb to advance the film and cock the shutter usually takes the subject out of the viewfinder and may wreck the focus if you are using a cat.

EXTENDED FILM MAGAZINES

Those who have dabbled in surveillance photography find it axiomatic that the incriminating shot escaped while they were reloading film. Thirty-five mm film cartridges sold in most camera shops hold 36 frames, tops; yet pros know that there are available magazines that will hold 100 frames or more. Be aware of the existence of these larger magazines for situations that call for a prolonged and unpredictable series of sequential shots.

FILTERS

Amateur-going-on-serious photographers discover that their photos bear a washed-out look compared with profession pix, or that pictures taken with outdoor film under indoor lighting affect an unnatural orange cast.

The solution to these and a host of other problems lies with filters—transmissive plates screwed onto the front of the lens. For long telephoto work, especially with the requisite high-speed film, the most needed filter will be the UV/haze, which filters ultraviolet light. The human eye cannot see ultraviolet spectra, but these rays tan/burn sunbathers. They happen also to expose film, even though we cannot sense the wreckage as it happens. This leads to a fogged image. A UV filter remedies this and offers a plus in that "haze"—the longer the distance the greater the atmospheric haze—magnified by telephoto lenses, contains much ultraviolet, reduced through use of this filter. (When using B&W film and shooting from extremely long range, the ultimate haze-killer is a red filter.)

The UV/haze filter is almost a must for several reasons. Some high-speed films show higher-than-average sensitivity to ultraviolet light. Second, long distances bring atmospheric haze in as a problem to be reckoned with. Finally, UV/haze filters protect expensive lenses from spatters and dirt that would otherwise shorten the lenses' lives. Some hold that a UV filter should be bought with every lens and left in place more or less permanently. Better that you should clean a cheap filter than a $600 multicoated lens.

As an instructive exercise, take your 35 mm camera and some 400 speed color print film, and get a UV/haze filter (about $10 for a generic brand, unless you want to shell out more than $50 for a Nikon). Set up a tripod and take pictures under a variety of outdoor settings, and indoors with flash, both with and without filter. Use a long telephoto lens for outdoor work if you have one. Even with computerized commercial processing which tends to compensate for some glare, you will notice a distinct heightened clarity of the filtered product. As a freebie, these filters do not reduce the amount of visible light transmitted, as most other filters do. That means no slowing of the shutter speed in fast-moving gigs.

LEFT: Target all but obscured by reflections off glass of car window. RIGHT: Polarizer reveals true intent of its helpless victim, now fully visible. Lens was Canon 70-210 f4 at full zoom; camera was Canon A-1 set on auto.

WARNING: THIS DOCUMENT HAS BEEN CLASSIFIED SCC RG T POSSESSION OF IT BY UNAUTHORIZED PERSONS IS A FELONY PUNISHABLE BY UP TO TWENTY (20) YEARS IN PRISON, AND/OR CONFINEMENT UNTIL THE MATERIAL IS NO LONGER CONSIDERED SENSITIVE.

This is page 34 of 217. Report missing pages immediately to the Office of the Deputy Director. Make no copies. Recipient's eyes only. Destroy if unable to secure from hostile possession.

[continued]
found that a pulse of 300 milliseconds duration at 50 percent intensity penetrated a full quarter inch of armor plate with only minimum spatter of molten metal; however, full-power pulses vaporized metal explosively and presented an unacceptable hazard to an unshielded operator standing less than five feet from the target, as well as a local fire hazard.

ACCIDENTAL OVERPENETRATION
When using the hand-held laser, the operator must consider the results of unintended full penetration. The beam of the weapon will melt common metal, such as car bodies sheet metal, at ranges of up to 800 meters, and can cause blindness at rages in excess of two miles. For that reason, it is recommended that the weapon be used as a matter of last resort, only by personnel familiar with its special properties, or under conditions in which an unintentional burn-through will be absorbed by a suitable backdrop, such as non-flammable wallboard at least 0.5 inches in thickness.

FIRING MODES

The DeathRay, Inc. hand-held free-electron laser can be fired in several modes to let it accomplish a variety of tasks.

I: MANUAL PULSE MODE
Pulse mode is adjustable in 100 millisecond increments from 100 milliseconds to 800 milliseconds by means of a circular click-detent dial on the left hand side of the weapon (Fig. 12). Only a single pulse will be delivered with each pull of the trigger (unlike the shoulder-fired version, with its greater energy reserves, pulses will not be repeated unless the trigger is released fully, then pressed a second time; the shoulder fired version automatically repeats pulses at a rate dependent on the selected pulse duration and power level available, and time to recycle the capacitor bank).

In addition to duration of pulse, the intensity is also independently adjustable, in 10 percent increments from 10 to 100 percent.

II: AUTOMATIC PROGRAM MODE
Automatic Program Mode selects dispersion, intensity, duration, pulse or continuous, and optimizes these variables to the nature

Average example of B&W document photography. Note that this is enlargement of a half-frame. We shot two 8.5 x 11 sheets per frame. Text is easily readable in this 5 x 7 enlargement.

On occasion a polarizer may be valuable. To explain it simply, light reflected from many but not all surfaces becomes polarized as a result of the reflection. The glare off windshields, water, and many plastics, particularly when viewed from certain angles, consists mainly of polarized light. Filters exist which will screen the polarized component. Thus, if glare on a window were keeping the suspects hidden from your camera, use of a polarizer on the lens might let you peek in where glare had kept your probing eye out.

But at a price. Polarizers halve the amount of light reaching the lens. That means faster film, wider apertures, or both, to allow for quick shutter speeds.

The polarizer rotates on the lens, since we must adjust it for maximum filtration of unwanted reflections. Some lenses rotate the front of the barrel as they focus, meaning that re-setting the polarizer must follow each change of focus.

Some types of reflections are not polarized, rendering this filter useless in killing them.

PRACTICAL DOCUMENT PHOTOGRAPHY

—yes, but do we need a Minox to get legible photos of documents? That question begged for an experiment.

We obtained apocryphal copies of the field manual for the hand-held laser weapon made by DeathRay, Incorporated (their motto: "Death to your enemies!"). We laid out two sheets side by side and photographed them with three different cameras and films. To no one's surprise, we got best results with the A-1 and T-Max 400 speed, though prints from an ancient Yaschica GSN using 400 speed color print film, and from a small autofocus Canon Shure Shot using 400 T-Max, were readable. We tried also the T-Max 3200 exposed at 6400 in the A-1. Prints were grainy but readable. The photo (unscreened) shows an average shot from the lot.

Naturally, a dry run is in order prior to any serious copy work. Make or get documents as similar in appearance to those that need to be copied. Select your film and speed, set the camera, and go to work.

But make it realistic. Time yourself. As a rule, the quicker you get done, the less the chances of capture. Make sure you have fresh batteries and film (look at the expiration date for both on the cartons; do not skimp here.)

Make the spots, develop the pix. For photographing black type on white pages, you will probably get best results with a 2-stop overexposure in available light. Flash pictures tend to overexpose anyway, such that no compensation should be needed, but make a trial run to check it. Electronic cameras are made to give proper exposure relative to "gray." If you photograph a white page with slide film, the camera chooses an exposure that prints gray. Therefore, you must overexpose to get true white. But there is no need to guess. In your trial run, do a normal exposure, a 1 stop over, 2 stops over, and so on. Set the camera to the one that gives best results.

Now, don't expect to read one or two pages per frame in a 4 x 6 print (especially not black and white; most labs do much better work, and get your prints back quicker, with color). You may have to go for 8 x 10s or larger. Depending on the sensitivity of the documents, a special photo lab or—better—your own may be needed.

If the material proves particularly sensitive, use Polaroid Polagraph HC (high-contrast black-and-white) slide film. You develop it in an inexpensive processor and mount the slides yourself. (The manual processor is inexpensive; the motorized processor is not.) Simply project the slides. With the right projector and lens, you can make them as big as you need to read the fine print. This film is rated 400 but tests showed optimum results in available light if the camera was set for film speed 100, which gives a 2-stop overexposure and very nice results indeed. Set for 400 speed if using flash.

4
LOCKS

Lemme in!
—the Big Bad Wolf

* * *

Spooklore will always save a spot in its heart for picking locks. There is something intriguing and visceral, almost sexy, about penetrating the forbidden, which is what lock-picking is all about. Too bad that describing locks, works, and the picking process, all while skirting the depths of boredom, proves no mean feat. Good news lies in the fact that mastering 10 percent of picking technique lets us defeat 90 percent of locks in use today.

Much published material on this tricky item assumes the student will make the commitments of a professional. Top pros can in fact bypass extremely stalwart locks—but their approach mirrors their professionalism. For rough cases, they learn the make and model of the lock in advance, buy a lock identical to the target, disassemble the mechanism to check its pick-resistant features. They practice defeating the lock under bench conditions to learn what will and won't work; and, critically, how much time it takes or noise it makes. They procure any necessary tools, such as a vibrator pick, lock-aid gun, and spinner wrench. Then they install the lock in a mockup of the actual objective and rehearse the operation under near-field conditions and under time pressure. In some cases, where the situation permits, they practice defeating the target lock as some sordid foreplay to the actual caper.

This professional approach keeps all options in mind. A genuinely superior lock and bolt mechanism will turn a pro's attention to defeating the door-jamb, the door itself, or drilling the mechanism—or to another avenue. An inside assist will supply the key on those truly high-priced jobs.

Common house-thieves enter through a door or window whose soft wooden jamb they have pried open with a crowbar. Speed makes up for this dreadful lack of finesse. Picking the lock never comes up.

Much of lock-picking's horrid lure lies in the way we unconsciously reverse-read its lore: How can we use what it tells to protect ourselves and our possessions? As a basic principle, make it so difficult, and therefore risky, for the common thief to get inside our home or business that he does not consider the target seriously. Deadbolt locks with pick- and drill-resistance, installed in metal doors and frames, positioned such that prolonged attack would draw attention, perhaps backed up by an alarm system—all would mean a full night's work on something that was not a sure thing. Common burglars hit soft targets.

THE VERY BASICS

We have many different types of locks, but covering any but the most common pin-tumbler variety quickly takes us to the point of diminishing return on effort. Before we can defeat a lock, we must understand its principles. At the risk of oversimplifying or wasting space for those already familiar with locks, let's re-invent the pin tumbler:

Consider a steel cylinder 1/2" diameter, about an inch long, with a flat handle attached to one end to let us

turn it, and some type of linkage at the other end, to connect to the actual "lock," since this describes only the lock cylinder, the point we attack when picking.

Second, consider that this solid cylinder fits inside a hollow steel cylinder whose inside diameter measures just over 1/2" so the smaller cylinder turns easily inside it. But since it turns, we have no lock. Now take a 1/8" bit and drill down through the outer cylinder into the inner, then insert a nail through the hole. With this nail in place, the inner cylinder will no longer turn. It is "locked" in place.

Change things a bit. Instead of a nail, let's use a brass pin just under 1/8" diameter. Further, assume we have cut a vertical opening that runs the length of the inner cylinder. We can access the brass pin through this opening. We have, in essence, a 1-pin tumbler lock. Any key or tool that will lift the pin to the level between the two cylinders—called the shear-point—opens the lock.

Now, with this gizmo set up such that gravity (or a spring) keeps some part of the brass pin blocking the shear-line, the plug will not turn. But if we insert a tool, or key, into the front opening and raise the pin, we reach a point at which its lower end clears the way. The cylinder turns, the lock opens.

Further complexity: Assume that we have used two brass pins, one on top of the other in the cylinder hole. Now all we have to do is raise this pin-pair to their break-point, where it lines up with the gap between cylinders, and the inner cylinder turns. In this we have a 1-pin tumbler lock.

Such a lock would be awfully easy to open with some slim tool, any tool, that let us reach in to raise the only pin. Practical locks attain a measure of security by employing multiple pins, usually 4 or more, and arranging for different heights for the shear-point. A key is a tool which raises each of several pins to its preferably unique shear-point. The intent of the lock is not to open to anyone who does not use the correct key; yet understanding the mechanism lets us formulate ways to make it open without use of a key. This practice is commonly known as lock-picking.

A pick may be considered any instrument inserted into the lock to let the operator manipulate the pins. The photo shows several standard pick outlines. Their names correspond to shape: diamond, circle, double circle, lifter. The ones with squiggly ends are known as rakes, or, in some texts, snakes.

Note also an ancillary tool we must always use with the pick: the tension wrench. This tool applies torsion to the plug while we manipulate the pins. The basic idea behind picking calls for raising all pins to their shear-points, at which point the lock will open. Rotational tension applied by the wrench keeps "picked" pins from dropping back into position.

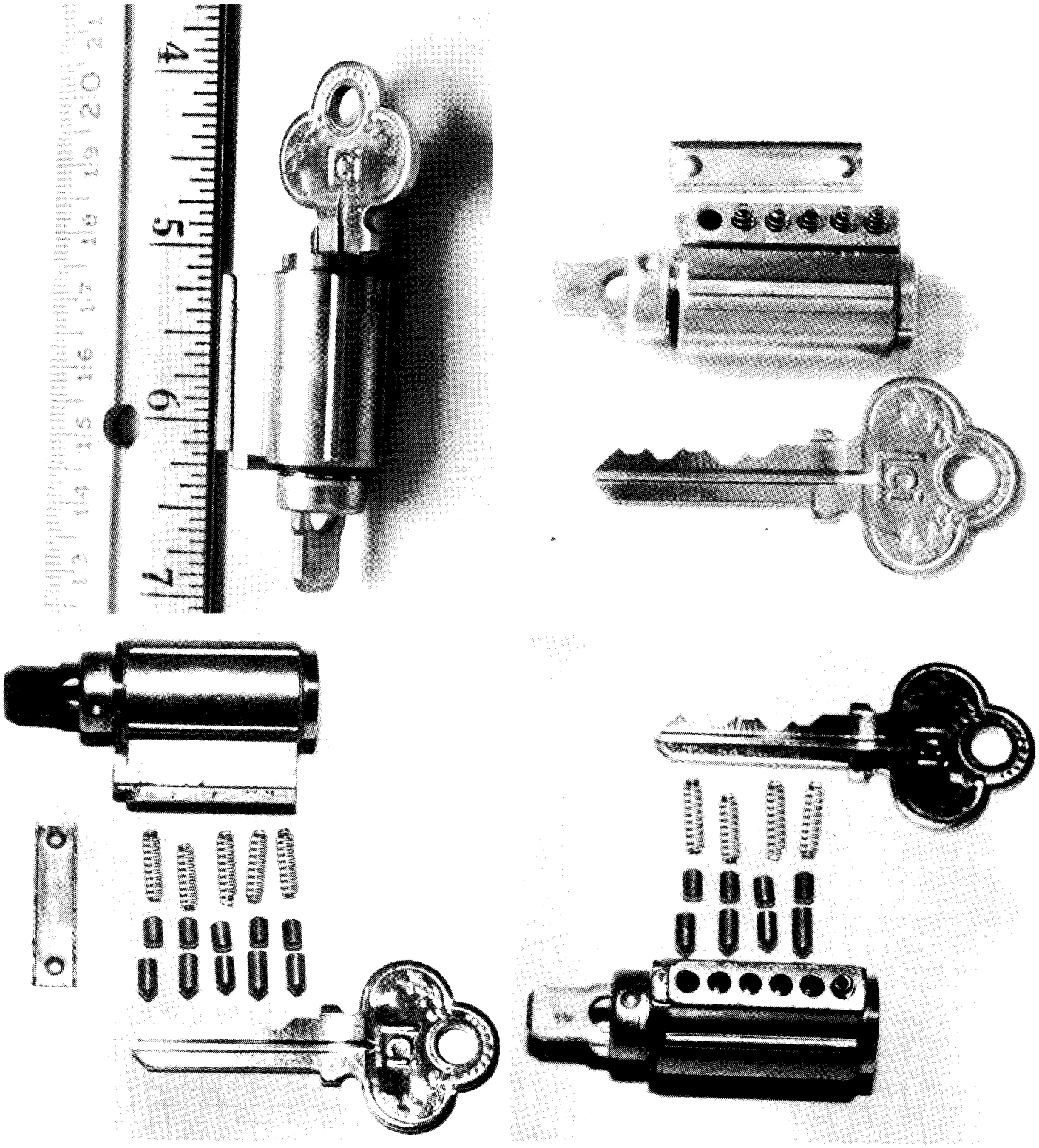
Picking rests on the existence of tolerances. Space must exist between pins and their pin-holes, and between plug and outer cylinder to have a useful lock, one not too tight. Dimensions never exactly match specs. Even if off by only a thousandth of an inch, they let us pick the lock.

The pin that binds first will "pick" first, followed by the next thickest, and so on; or at least that's the theory of picking by attacking pins one at a time.

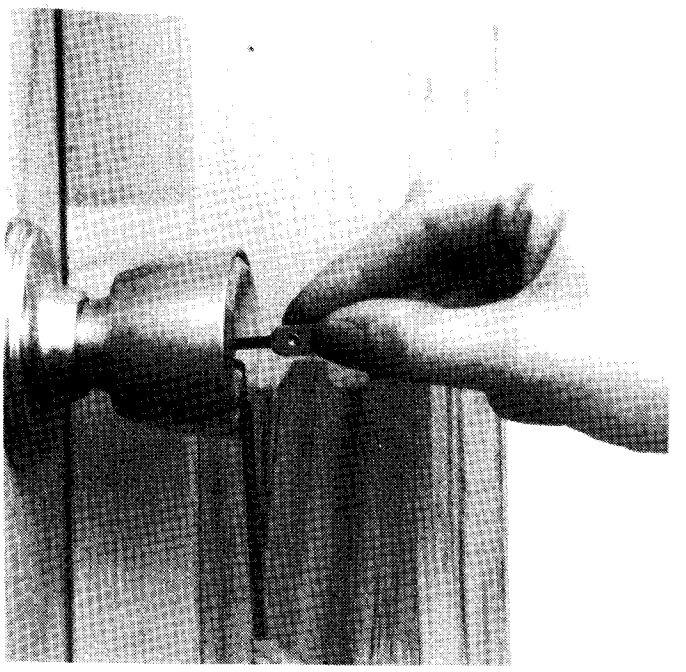
Disassemble the picking process. First, insert the tension wrench into the keyway, then insert the pick. Apply light tension (as used here, "tension" means torsion: a turning force), then begin lifting pins in turn. A pin-pair lifted to shear-height at which there exists slight play in the mechanism will separate. It is then said to be picked. The top pin won't fall because the cylinder has turned ever so slightly, but enough keep the top pin above the shear-line. Then on to the next pin—it's impossible to predict which—until all are picked, at which point the cylinder will turn and the lock will open.

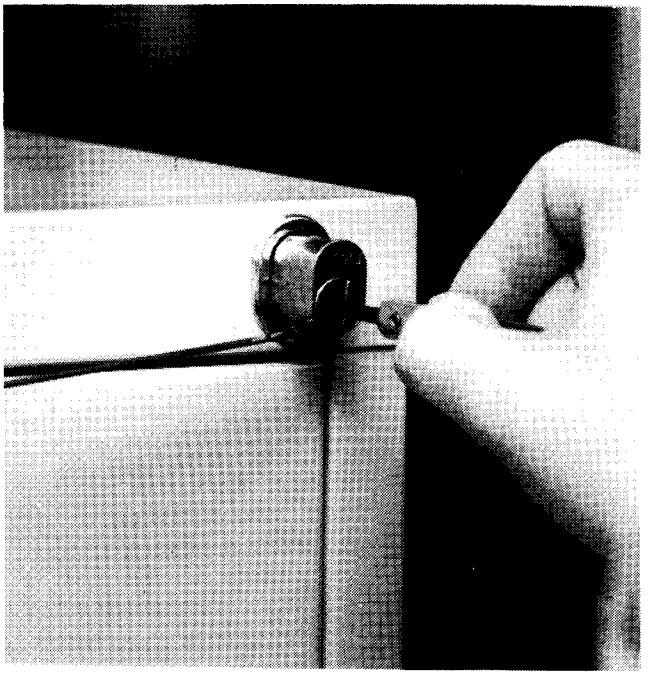
BEGINNING

Educators agree that repeated failure at a task turns the student off. Playing a game of chess with a computer that thinks for 2 seconds per move is usually much more enjoyable than one that thinks for 3 minutes a move, since the latter case makes it so powerful it can beat most players. And so it is with lock work. Start out on an upscale Master[tm] padlock, and failure will turn you off the trade quickly.



TOP LEFT: Assembled cylinder. TOP RIGHT: Retaining cap removed to expose springs that lie on top of pins. Note that this lock could hold 6 pins but came with only 5. BOTTOM LEFT: Fully disassembled mechanism showing bottom & top pins, springs, retainer, cylinder, and key. BOTTOM RIGHT: Pin 1 has been replaced. Put retainer back on and start practicing.





TOP LEFT: Middle-aged mother of two in grimly determined attack on helpless 5-pin tumbler lock.
TOP RIGHT: Picking technique: overhand grip.
BOTTOM LEFT: Picking technique: pencil grip.
BOTTOM RIGHT: Attacking lock on file cabinet. This particular lock proved far more resistant to picking than did 5-pin tumbler.

The student should begin with these wretchedly simple 5-pin tumblers that fairly fall apart in one's hands. But the best way, and a method that imparts important insights into the workings of pin-tumbler locks, demands buying a simple 5-pin tumbler, removing the cylinder, disassembling it, reassembling it selectively, and working on it alone.

Some texts suggest mounting the works in a doorway. That method certainly offers a degree of realism. But, as the photo shows, a simple C-clamp will serve to hold the cylinder for this introductory phase.

Take the lock apart, always remembering which pins go in what holes, so the lock will work with the key when you reassemble it. Refer to the photo set. (It may not be visible in the photos, but each pin has been scribed with a line to indicate its sequence in case it is forgotten, as it always is.) Also, take care when you remove the retainer strip over the line of pins and springs. Unless you cover it, the springs will pop out and into permanent exile in the limbo of your carpet.

Once you have taken the lock apart, reassemble it with only one pin. The first pin (the one closest to the keyway) is an appropriate place to start, since you can see it. You know intuitively that, if you apply a twisting force with the tension wrench and lift the pin with a pick, the cylinder will turn when it reaches the shear-point. Mount the setup and try it. You cannot fail. You will use only a simple "lifter" pick and a tension wrench.

Picking a single pin proves so easy you may be tempted to move on before you have milked the exercise for other lessons it can teach: feel, for example. What does lifting the pin feel like? How does it feel when it picks? What effect does altering the tension from light to heavy have on feel? Does it make a difference whether you apply torsion clockwise or counterclockwise? Slowly pick the single pin several times with your eyes closed to help with feel. This simple lesson will return to aid you with difficult locks.

Remove the first pin and repeat the exercise with the second pin only, then the third only, and so on. Each will offer different feel and will accustom you to working with pins deeper in the lock and having different shear-points.

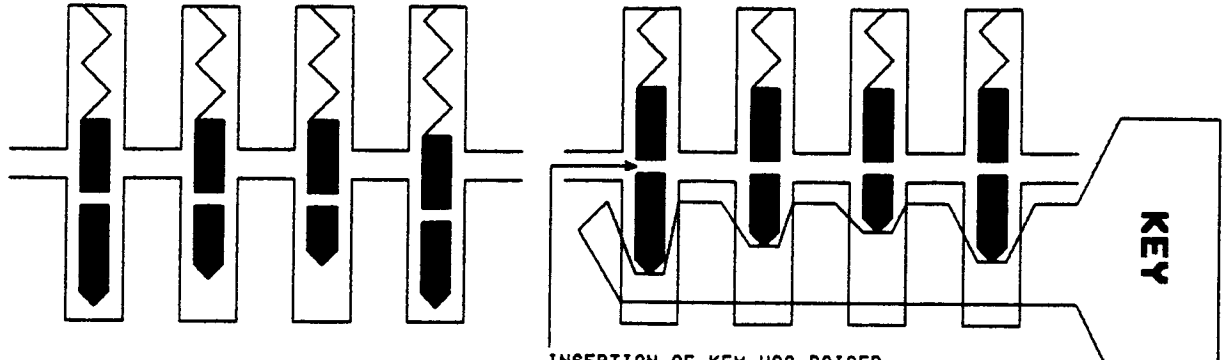
Now reassemble the mechanism with two pins. This time you'll have to lift one pin until it picks, then go after the second, at which point the lock is yours. Notice that the order in which you pick the pins may well make a difference. Pick in the wrong order, and you do not leave enough play to pick the second pin. This is a valuable lesson: The order in which you pick the pins can make the difference between a rough and an easy pick.

Picking two pins proves so easy that the beginner is tempted too soon to move on to more pins without extracting valuable lessons from fewer. Remount the lock with all possible combinations of two pins: 1&2, 2&3, 1&5, etc. With each, you will notice a distinctive feel. This is one of the quickest ways to learn intuitively that the order of picking the pins can make a great difference. Do not skip this step.

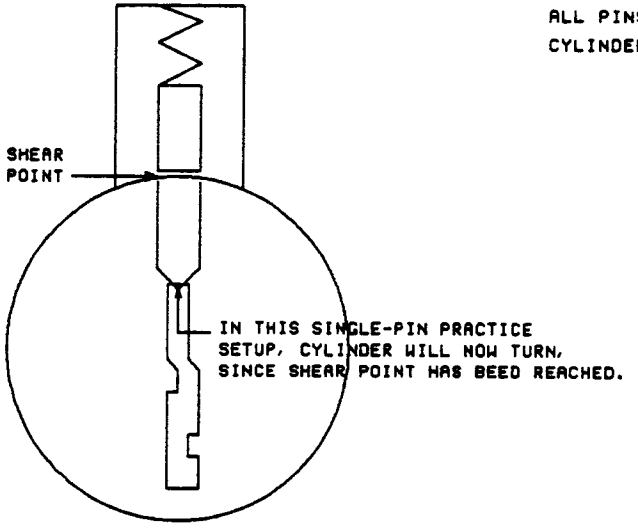
Now move up to 3 pins, applying the same exercises. Mount 3 pins in all combinations, pay attention to feel and the order of picking that opens the lock fastest. Pick both clockwise and counterclockwise. As you reach three pins and up, be patient with yourself. One of the commonest beginner reactions, impatience usually terminates the practice session. And you cannot learn to pick locks without practice.

Move up to 4 and finally to all 5 pins. Although these locks are so easily picked that the author taught a middle-age mother of two to open the 5-pin tumbler in the photos in less than half an hour, the serious student might well spread his practice over several sessions, several days, to work up to 5 pins. (The author has lost touch with the middle-age mother of two who modeled for the photos, but it would not surprise him that she now carries a small pick-set in her purse. Has Women's Lib gotten out of hand...?)

Stop here to reward yourself, if only mentally, with the notion that you have pretty well mastered basic picking technique for the common 5-pin tumbler. Though you will find quirks among different brands, understand that you can now pick 90 percent of the locks in the country. That includes wafer locks that protect droors and filing cabinets and burglar alarm boxes, as well as most apartment and house locks.

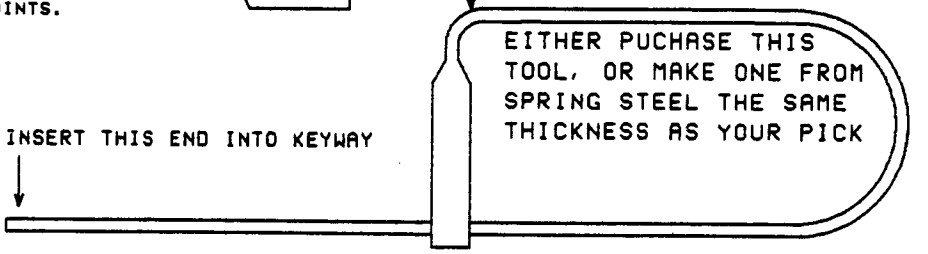


INSERTION OF KEY HAS RAISED
ALL PINS TO THEIR SHEAR-POINTS.
CYLINDER WILL NOW TURN.



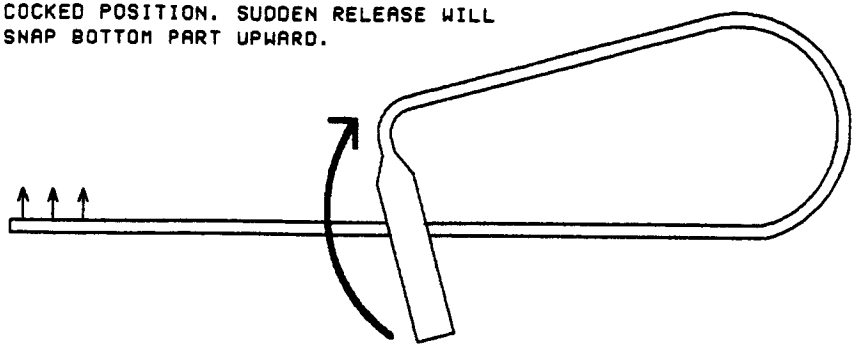
IN THIS SINGLE-PIN PRACTICE
SETUP, CYLINDER WILL NOW TURN,
SINCE SHEAR POINT HAS BEED REACHED.

USING YOUR THUMB, COMPRESS THIS
SPRING-LOADED PORTION, THEN RELEASE
SUDDENLY, PRODUCING UPWARD "SNAP"



SNAPPER PICK. TO OPERATE, INSERT END INTO KEYWAY ALL THE WAY.
"COCK" THE MECHANISM BY PRESSING DOWN THE SPRING-LOADED UPPER
PORTION WITH YOUR THUMB. LET GO SUCH THAT THE CATCH "SNAPS"
THE DISTAL END UPWARD SHARPLY, WHILE APPLYING TORSION WITH
THE WRENCH. EVEN MUSHROOM PINS MAY NOT RESIST THIS FORM OF ATTACK.

COCKED POSITION. SUDDEN RELEASE WILL
SNAP BOTTOM PART UPWARD.



TRY AGAIN USING A DIFFERENT PICK

Once you have worked up to 5 pins, using only the lifter, have gained proficiency and confidence, you may experiment with other picks in your set. Try the diamond and compare its feel to that of the lifter. Try the rake/snake or the circle. You may find that different picks work better with different locks. Ideally, repeat the mounted-cylinder exercise pin by pin with each new pick. Try the two basic types of tension wrenches (thin and thick, for different size keyways).

Try other methods of applying tension. Some authors recommend using a rubber band, one end attached to a thumb-tack stuck in the door, the other hooked on the end of the wrench, to maintain fairly constant tension. Others advocate attaching small weights to the end of the wrench. A closet lock-student since 1977, the author has never had to resort to these techniques, though some highly qualified people commend them.

COMMON MISTAKES BEGINNERS MAKE

First, different locks demand different technique, certainly. But for the bulk of non-resistant locks encountered in condominiums, office buildings, and lock boxes, these rules work well:

Use proper grip. Hold the handle firmly, and move the entire pick up or down, as needed, rather than attempting to pivot the pick. When working a single, rear pin with a lifter, pivoting may be the only way to avoid upsetting the pins in front of it. But as a rule, the best technique keeps the long axis of the pick parallel to the bore of the lock. This demands a firm grip that quickly cuts your flesh if the pick lacks a rounded or padded handle.

Second, do not let the pick twist. This is easier with thicker picks than with thin ones, but you will probably find the thin picks more effective because they fit into cramped keyways. Twisting side to side defeats the lifting action, and, if you happen to be raking, galls the metal. So, not only must you tense the muscles to hold the pick rigid in a horizontal plane, you must not let it rotate while you lift the pins.

Third, early successes, especially with rakes on the 5-pin "beginner" locks in bench testing, will tend to condition you to lifting the pins all the way. As long as it works, fine. But you will meet locks whose shear-points hit with only slight lifting. That means that pushing them higher will only frustrate you. The lock used on the filing cabinet shown in the photo, a simple 4-pin or wafer, was of that type. It finally yielded when the lock student altered his approach to lifting just a little, rather than all the way.

Fourth, beginners become frustrated easily. Their reaction is A) to sweat, B) to tense up, and C) to bend the tension wrench into a bow from which it never springs back. Getting tense, making jerky movements—experience shows that these never succeed. Patience does. If things aren't working, change your approach systematically: pick the center pins, then the rear, then the front, or some combination other than the obvious back-to-front. Alter tension. If using a rake, note that it's likely to have different actions upside down, so turn it over. Persistence pays off, as does adaptability. You lose nothing by altering your approach.

Fifth, change the tension wrench. Most small sets give you a thick wrench and a thin one. For some locks, the thick wrench won't let the pick maneuver. For others, the thin will be too small to apply any force at all. If one doesn't seem to work, try the other.

The photos are posed, obviously, but the woman who belongs to the hands picked each lock she attacked. If she can do it, so can you. The locks to the alarm box (4-pin), a desk drawer (ditto), the office back door (5 pins, but they practically pick themselves) and the mailbox (another 4-pin) are yours for the taking, even with suboptimum tools, should you accidentally lock yourself out. (As a proper solution to that, secrete spare keys where you can get them quickly in case of a lockout.)

BUT WHICH WAY DOES IT PICK?

Those who have taken on locks know that they prove impossible to pick in one direction, often the "unlock" direction, yet open fairly smoothly in the other, or "lock" direction. That means that, unless you know which way the brand picks to open, you should give both directions a good go before slipping the bumper-jack into the doorway.

So what if you should successfully bypass the lock, but in the wrong direction? Bring in a rotary spinner. This coiled spring-steel device has a blade-like tang on one end and a handle at right angles on the other. Insert the blade into the keyway of the picked lock, then apply a hold so that the cylinder will not spin. Then turn the handle to build up spring tension, like a watch mainspring (they used to make watches that ran mechanically, on the power of a spring....). When you let go the spring, it spins the cylinder rapidly in the other direction, so fast that the pins do not have time to fall back into place as it passes the upright position.

A spinner is not a bad tool to have. The author tried manually spinning a cylinder he had picked, in the wrong direction, and found his hands too sluggish....

Mechanisms used by Master on its high-end padlocks like the one shown in the photo belong to a different breed than the common 5-pin tumbler. Though only 5 pins, these locks have earned their reputation for pick-resistance. Of course, even a Master padlock proved no match for a pair of killer bolt-cutters, the preferred method for defeating exposed metal of about 1/2" or less when time is tight and money (the cutters cost well over $120) means nothing in relation to the worth of the objective....

THE CYLINDER IS NOT THE WHOLE LOCK

So you've mastered a simple 5-pin cylinder. Congratulations. It is time to learn that picking the cylinder does not mean picking the lock. A rigidly mounted cylinder provides a distinctly different feel than that same cylinder in a door-handle or deadbolt. The mechanical linkages offer so much resistance/play that you may pick the lock in thirty seconds, but not know this because of the spring tension on the handle. That means it is wise to pause every few minutes to apply significantly stronger tension to the wrench, or try to turn the handle. It isn't uncommon for the cylinder to have turned only a few degrees, yet the handle will then turn all the way and you're in.

Work out on some real targets: the lock on the drawer in your office desk should be the proverbial piece of cake—but here you will learn that even simple locks have their idiosyncrasies, and that simplicity of design or lack of pick-resistant features does not necessarily mean it will open more easily than a 5-pin tumbler. Try the push-in lock on the filing cabinet. It looks easy, but picks hard, at least on the two the author has tackled. How about the 4-pin wafer on your mailbox? Try them all.

Check out the photo of a steel door fit with two locks, one a deadbolt. Anyone who lives behind that impenetrable barrier must feel pretty secure, eh?

It took the author exactly 70 seconds to pick both locks, first try. The locks happened to be keyed alike and were master-keyed to boot. The author once dwelt behind that door. He has long since moved, but after the pick-trick, had a locksmith install a high-security Medeco cylinder in the deadbolt.

The 5-pin tumbler you mastered is ubiquitous. Look around, start paying attention to the number of homes and businesses protected by this now meaningless obstacle.

As an additional ego-booster, something that offers thrills and more practice, pick a 5-pin tumbler that is in service; but here you must exercise caution. In some jurisdictions mere possession of lock-picks by the non-locksmith or bonded locksmith student is illegal. Second, insertion of your pick into someone else's keyway without their permission could constitute a crime. Third, laymen who see someone working a lock tend to freak out and call the police. The poor cop who's done nothing but hand out traffic tickets the past three weeks will tend to respond with unnatural verve if he spots you at outdoor practice.

So practice on your own locks, or, if you must use others', make certain they are present to back up your story. If your jurisdiction restricts possession of picks, buy into one of those mailorder locksmith courses and have the proper credentials on you.

PICKS

Catalogs from companies selling locksmith supplies usually offer pick sets that range from about 8 items (2 tension wrenches and 6 picks), on up to sets of a hundred pieces, with picks, wrenches, tiny saws, key-

extractors, and other goodies. The question comes up, What use is there for this varied selection? Experience with a small set showed that only two tension wrenches ever saw use, along with only three picks: the rake, lifter, and diamond, thin ones at that. The remaining items served well as ballast in the pick case, and served no purpose other than impressing dates.

All books on lock work publish the standard pick outlines: lifter, diamond, rake, and so on. We have included a photo of a handful of HPC[tm] picks. They could be used as guides for manufacture; but for all save experienced metalworkers, it will prove easier to buy a pick-set.

The beginner's pick is the lifter, a simple curved end with a flat tip. It lifts pins one at a time. The shape stems from the need to get up under other pins in front of the target-pin without disturbing them. Large pick-sets come with lifters of variable reach and height.

The diamond takes its name from the triangular shape. Most designs lack the curve of the lifter that lets the pick reach the back pins without disturbing those in front. Despite the nomenclature of picks, the diamond may see better success with raking than the rake.

Ah yes, the rake pick. They call it a rake because it is, supposedly, suited to the raking technique discussed shortly, yet it seems to see greater success in non-raking pick techniques. Some authoritative texts have suggested the diamond for raking.

Others call rakes "snakes," out of their serpentine profile. That makes them almost like a segment of key—and in fact and by chance alone, they will function that way with 2 to 4 pins, depending on the breaks. Simply inserting the rake and lifting, at the right spot, may pick a handful of pins, something that might otherwise consume tense minutes. With those out of the way, and they might have been bitches to get with a lifter alone, the rest pick like the proverbial piece of cake.

This explains the presence in some of the larger pick-sets of rakes having distinctive contours: different depths and angles of "cuts" on the rake, different distances between cuts, more or fewer cuts. A failed snake in one lock may open another in seconds.

Note too that the character of the rake changes depending on which edge faces the pins. That gives one rake an entirely different personality simply by using its opposite edge.

BAD TOP PINS

Known as mushrooms or spools, out of their diabolical shape, these pins provide false shear-points that, once hit, force the student to start over. Refer to the diagram. Applying conventional picking technique, note how the mushroom cut will let the cylinder turn past normal tolerances, yet stop it cold at that point.

Raking, the lock-aid gun, and vibrator picks have a rep, at least in spooklore, for defeating mushroom pins. We dunno. We've raked several serious locks in the past 10 years, have tried every trick in the books, but they have yet to pick....

TWISTING PINS

Medeco's high-security locks incorporate bottom pins that do not terminate in a point. Rather, they end in a bevel. The key has a matching slot at each cut, such that, once inserted, it both lifts and rotates the pin. This action in turn allows a side-bar to slide out of the way (if it didn't, the cylinder would still refuse to turn even if you had picked the pins). This adds to its pick-resistance. One locksmith the author questioned stated that Medeco would cut keys only for the original purchaser of the lock, which adds some measure of security that at least the bonded locksmith down the street wont duplicate the key from an impression (do those bevels show up in the impression?) or even from the original, unless the customer can produce a special ID card that says he owns the lock.

MULTIPLE ROWS OF PINS

Sargent's Keso cylinder has in essence three rows of pins, all of which must be picked simultaneously in order

for the lock to open. Instead of the "cuts" of common keys, it is pock-marked by what appear to be drilled pits of a set depth. The pits line the top and two sides of each key. This design reputedly allows for multiple levels of master-keying without sacrifice in security.

Note in addition that Sargent and some other makers of high-security cylinders will cut keys only at the factory, and only for registered owners of the lock.

Couldn't we just insert a stick of metal on the end of an electric toothbrush, apply tension with a wrench and hope for the best? Yes, and who knows what could be made to work?

RAKING

It's easier to describe raking than it is to visualize what it does. Raking refers to a picking technique designed to defeat locks equipped with one or more spool or mushroom pins.

To rake is to insert the pick all the way, (and here authorities differ: some recommend the rake pick, others go with the diamond) apply light tension, then rip the pick out of the lock snappily while pushing upward fairly hard on the pins. That jerky extraction is raking.

But what does it do? Performed with verve, it flips all pins up past their shear-points in a split second. As they begin to fall, some will catch at their true shear-points, since those will hit the shear space before the mushroom or spool cut.

A single rake won't usually do it. Texts suggest 10 or 12 in a row, varying the tension a hair with each series. If a dozen won't go, ease off, change the tension, and start again.

Another technique refers to holding the pick as if it were a pencil, and rubbing it back and forth very quickly while varying tension on the wrench.

Metals rubbing together exhibit a special type of friction commonly known as galling. Picking locks, especially raking, tends to gall the works. In addition, the target lock may not have seen frequent use or lubrication, and out of neglect alone have fallen into a state of helpless self-galling.

This calls for lubrication. Oil is messy. Often we cannot get it into the upward crevices that need its soothe the most. Extremely fine graphite can be had in tiny tubes, equipped with matching needle-nozzles to spray the works with this dry and comparatively neat lubricant.

The author hesitates to pass judgment on raking, since he has had no success with it. Non-pick-resistant locks pick faster, in his hands, with conventional techniques than with raking, and he has never had to face a genuinely pick-resistant lock. Some highly qualified people endorse raking, however.

We did not see a professional thief portrayed so well by James Caan in the film, Thief, pick a lock. He used a dent-puller to rip out the whole damn mechanism in seconds. If time is tight and noise no problem, that method certainly beats all brands of finesse.

In truth, the only pros who bother with lock-picking are locksmiths of a singular cult, and professional criminals whose modus operandi demands quiet access to premises without evidence of forced entry. Low-end crooks, the type of street-slime likely to bust into your house while you're cruising the mall with Mavis, will use the typical means:

1) pry open a wooden door or window with a screwdriver
2) use and dent-puller to rip out the lock mechanism
3) put an automobile bumper jack in the door-jamb, pry it apart
4) break a window to unlatch it
5) kick in a bottom door-panel and crawl in
6) use big bolt-cutters to trash a padlock in less than 3 seconds
7) other brute-force methods

MAKE OR BUY?

Most texts on lock-picking depict the same set of pick templates, then tell the reader how to make them, with different levels of sophistication. For the purist that surely must be the way to go.

But be practical. The beginner would be advised to purchase a small set to conduct the familiarization exercises. (Can you pick more locks with that huge set that goes for $150? An expert might. But you? Save your dough until you know you can use those fancy picks.) An adequate beginner set costs about $25 and is not something to flash or brag about. It makes you too much of a suspect when your clandestine skills come to mind in the wake of some dark, unsolved B&E. To avoid the privacy-invasion, give the invaders no reason to target you. Spreading it about that you do lock-work waves a red flag in the face of the Enforcement Community. Knowledge of lock-picking is considered strange in most circles. When the author questioned a locksmith and made casual reference to spool pins, spinners, and the like, the proprietor squinted like Clint Eastwood and came back with that blunt classic from Three Days Of The Condor: "Are you in the trade?"

PICKS: COMFORT MEANS EVERYTHING

Look at the double-ended picks in the photos. Marvel at their economy of space. Then try to use one for longer than a minute. Your fingers will start to blister, then bleed, at the bearing points. You will not be able to keep the pick from twisting, and the rake or diamond on the other end will bite into your flesh.

A better design has a handle, but it's of the same thickness as the pick. Clearly, easier to use than a double-header, but still rough for locks with stiff springs. Those non-sharp edges sure begin to feel sharp after about five minutes.

Now look at the model with stainless steel handles about an eighth of an inch thick. This type proves most practical for the beginner. Bulkier, for sure, but infinitely easier on the hands. Using it compares to the difference between hauling heavy concrete blocks using bare hands, or hands protected by tough leather gloves.

Some picks can be had with plastic or wooden handles, and, of course, the second variety mentioned above could be wrapped with tape for better control and feel.

MECHANICAL AIDS

Mechanical aids have evolved to make up for sloth on the part of many lock students. They are designed to do what raking does, but with greater speed and efficiency. The oldest of these helpers is the snapper. This simple piece of bent spring steel, or piano wire of suitable thickness, substitutes the raking movement with a sharp upward rap that flips the pins upward more efficiently and consistently than manual raking.

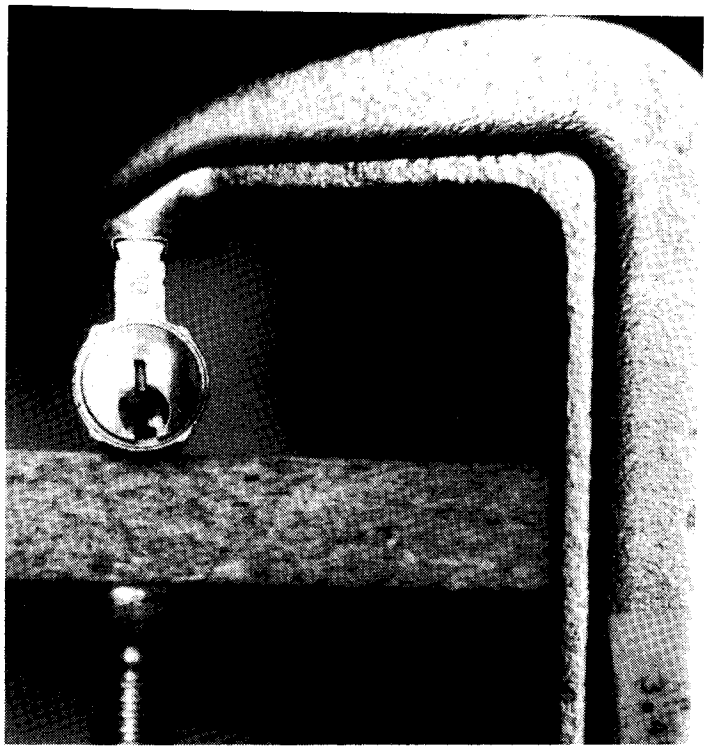
Another example is the legendary lock-aid gun, often called the police lock-aid gun, though it has seen little media exposure. One version pulls (rakes) the pick at a speed far greater than human hands can apply, while another is no more than a glorified and rather expensive snapper.

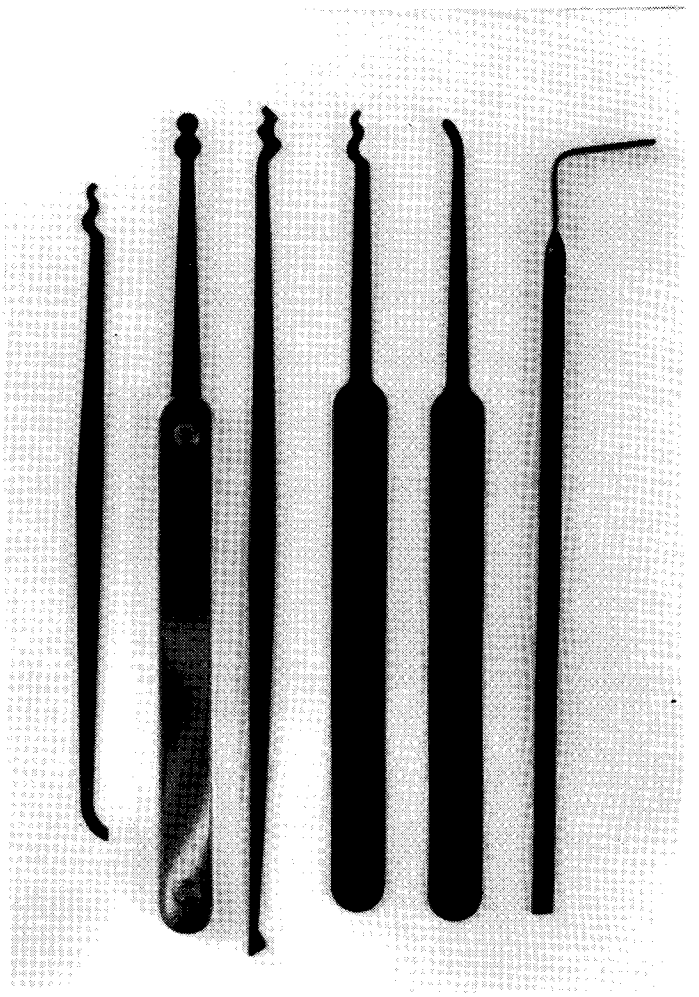
The latest version attaches one of several picks to an electric jiggler of sorts. It provides a vibration/agitation that jiggles the pins into place by chance alone.

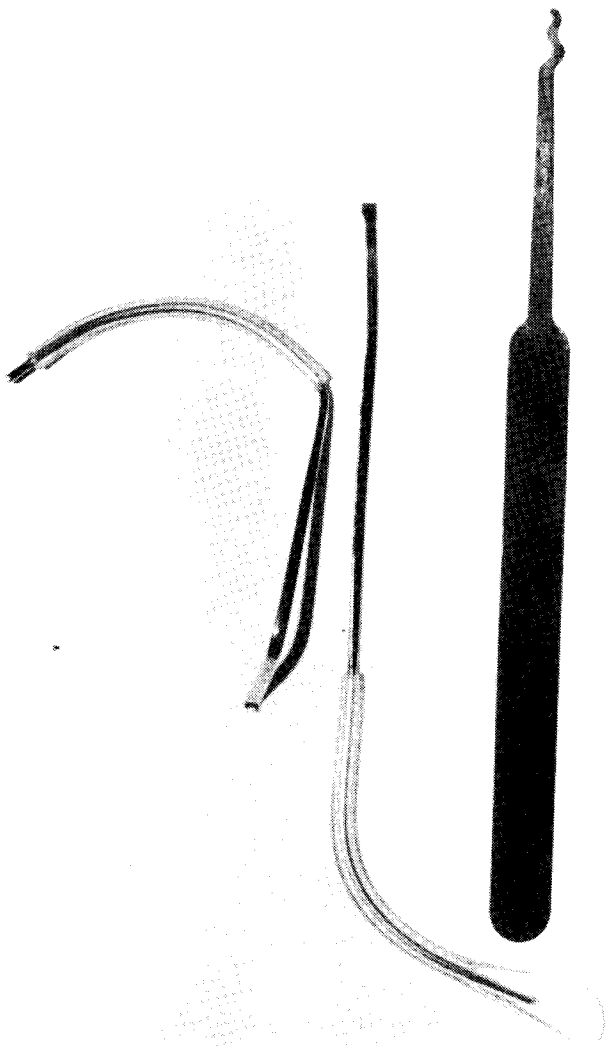
The point is not to wise up the bad guys. They get graduate-level instruction on any inner-city street or in the joint. Rather, it's to show the reader what illusory protection even 7-pin, pick-resistant locks provide. If all they would ever face were manual picking—fine, sleep soundly. But they're at the door with mechanized, proven aids that fairly beg for something like a Fox Police Bar that means you have to force the door out of the jamb.

PRACTICAL USES

The author bought his first and only set of picks in 1977, ran his first picking drills in 1978, but did not have call for these dread skills until 1983. He accidentally locked a filing cabinet similar to the one in the photo. No one could find the key. He locked the door to his office (what would the company secretary have thought had she seen him picking a lock?) and set to work, using the thin tension wrench and a diamond







TOP LEFT: Cylinder set up for practice.
ABOVE: Part of standard pick set. From L to R: double-ended pick w/lifter bottom, rake top; double circle w/comfortable handle; another double-ended pick—extremely uncomfortable to use—diamond on bottom, different design of snake on top; single-ended snake w/thin handle; single-ended lifter; tension wrench.
LEFT: Mementos of determination and a bit of technique. These are the actual glasses frames that the author used to pick a 5-pin tumbler. Far left is tension wrench, next lifter pick. Standard rake pick shown for comparison.

pick. He felt the pins picking, but the darned thing wouldn't open. Then the idea hit him to press inward on the plunger while picking. That proved awkward: pressing the plunger with the left thumb, applying tension with the little finger of the left hand, picking with the right hand. But in 15 minutes it worked, and the files were his.

The second practical deal went down in the summer of '85. The author locked himself out of his house. Fortunately, its door bore a cheap 5-pin tumbler, exactly the kind he had mastered in practice. Unfortunately, the picks were in the house along with his keys.

First he tried paper clips as pick and wrench, but they bent too easily. Nothing else handy seemed adaptable to picking, until the author removed his custom sunglasses. Their wire frames were practically pick-stock in terms of shape; but using them would mean trashing the frames. To cut the story short, he did, they worked, and he kept the frames/picks as mementos, true symbols of the power of persistence. (Incidentally, it took almost 20 minutes. The lock picked in 5 minutes, but in the wrong direction. To open in the correct direction, the center pin had to be picked first, then the others picked easily. When attacked later with standard picks, the lock opened in less than 30 seconds.)

IMPRESSIONING

Impressioning is one method of getting a lock to cooperate that has found success in trained hands. This refers to making a key for the lock, starting from a key-blank and some common tools.

We will need a blank (the beginner will need several; this is no mean trick to learn); a pair of "Vise-Grip" or similar pliers, or a stout C-clamp; a soft-face hammer; and a selection of small files that bite like metallic piranha. Pros or others who do this often may want to go in for a portable key-cutter.

Start by clamping the handle of the keyblank in your pliers, clamp, or other holder. Insert the blank into the keyway. Apply hard turning force, though not enough to bend the keyshaft. The purpose is to bind the pins so they won't move during the next step, which is to shake the whole mass up and down hard, or rap it sharply with a hammer on the top and bottom of the handle.

If you have done this properly, the blank should show marks along its top edge, left by the (commonly) brass pins. Since the marks may be difficult to see in any case, once you have unequivocal pin marks, it may be helpful to scribe a line at the level of each pin, on the flat side of the blank, perpendicular to the long axis of the key, so you will know after removing metal and repeating the rap where new marks should appear.

Next, take a file and cut away metal over the center of each mark. Don't take off too much; you may go too far on one cut, then you would have to start over. Remember that, in most locks, the difference in length of one pin from the others in the set varies by a set distance, a common example being 0.05 inches. Experience and knowledge of a particular brand's idiosyncrasies may let you estimate closely the amount to cut that approximates one increment in its pin-series.

Repeat the marking process. Whenever a cycle leaves pin-marks on your evolving key, take off more metal. Also, it may be necessary to widen the sides of the cuts, just as with a conventionally cut key.

Stop filing at a given point when a trip through the lock leaves no mark. Assume that you have that cut at proper depth, that it raises the pin there to its shear-point. It is always easy to take off metal if you are wrong; taking off too much from any pin-point will mean starting over.

These marks can be blessed hard to see. Some advocate blacking the blank with lampblack or some other dark powder, or holding it briefly in the flame of a lighter or candle, which will coat it with soot. If you use an aluminum blank, it may be easier to see marks made by brass pins, but be aware that aluminum keys may not hold up under full torsion, and break off. Then that key-extractor in your satchel will finally pay for itself.

Impressioning has found use in the automobile repossession business. In many states it is legal to "steal" a car back from an owner who is behind on his payments, so long as the theft causes no ruckus. As auto-makers

have hardened their locks (particularly ignition locks; car-stealing for real is big business), repo operatives turned to impressioning as an alternative to a destructive attack on the ignition mechanism.

For cars whose door-keys match the ignition, an easy course may be to remove the door lock (getting the door open is child's play), disassemble the lock and make a key by measuring the pins. Most manufacturers' pins come in a sharply limited number of sizes of top and bottom pins, making this comparatively simple, and surprisingly quick if your repo-van carries a key-cutter.

As part of its anti-theft measures, one American auto-maker began using bottom pins with a broad, flat surface that faced the impressioner with misleading cues (see diagram).

Impressioning increases in difficulty with security measures, such as beveled bottom pins requiring beveled keys. The impression will not tell you the proper angle for the bevel.

TUBULAR LOCKS

Once you grasp the common pin tumbler design, the tubular lock presents nothing new, merely rearranges things so that the pins surround the plug and are oriented coaxial with it, rather than perpendicular as is the case of a common pin tumbler.

But how often do we have occasion to defeat this type of lock? Yes, there's a pick for it ($129.95 from Phoenix Systems), and it can be drilled, or, if enough of its mechanism is exposed, pulled or sawed. But these locks have become standard features on vending machines, alarm switches, and so forth, targets only criminals think to attack. And certainly, no would-be criminals read this book.

BUT WHAT ABOUT THE LOCKS ON CARS?

This specialized field shares much with common pin-tumbler locksmithing, but departs in that it interests mainly A) locksmiths, B) repo men, C) car thieves. In addition, many of its standard techniques involve destruction of the mechanism or require use of tools so rarely needed by the amateur that it isn't worth it to keep them on hand.

Detroit, the Europeans, and the Japanese have not ignored security in the plan of their machines; yet, in something that is 20% glass by design, no determined thief will be held up more than a few seconds by smashing a side window to gain entry to the vehicle (though, among repo specialists, this destructive attack is considered amateurish, a last resort, since the cost of replacing the window cuts into the repo fee).

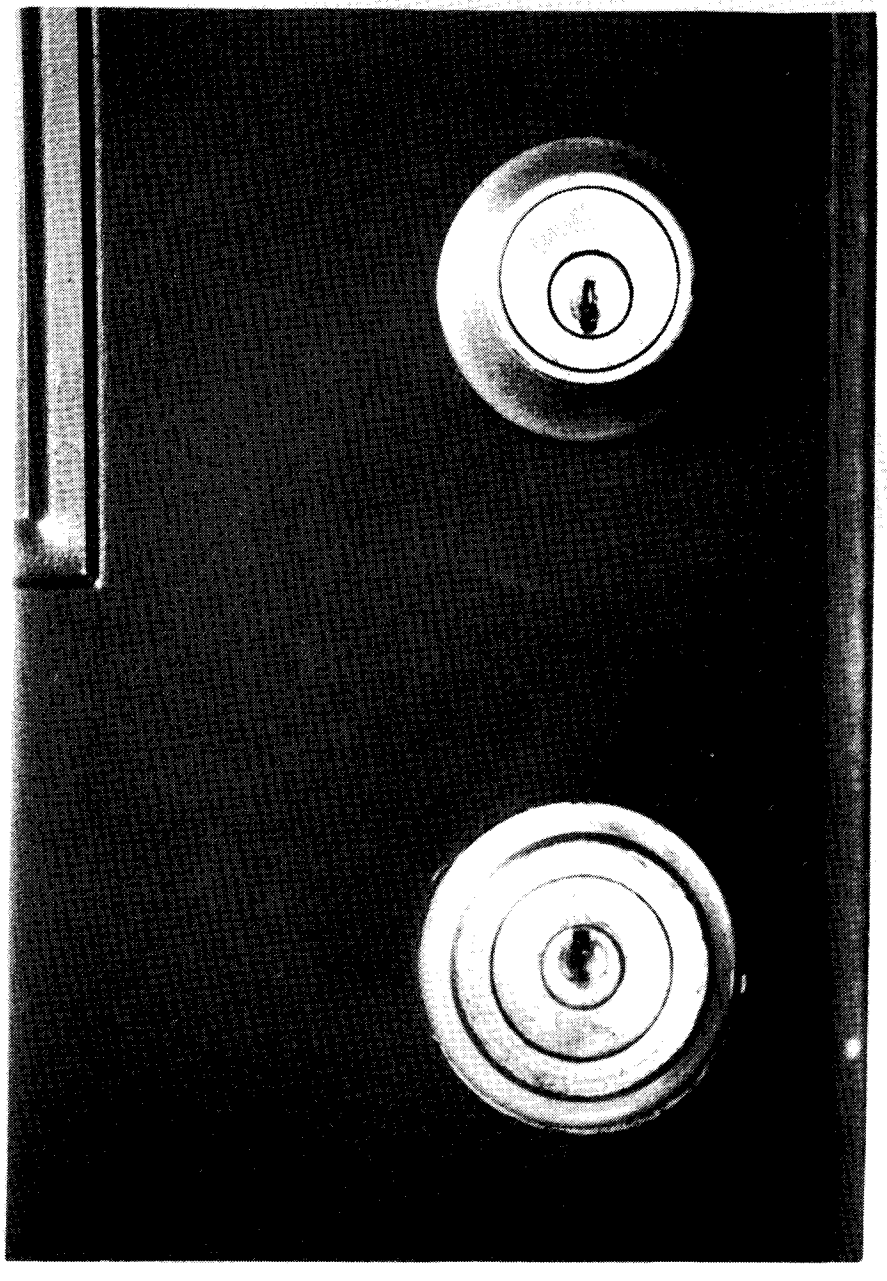
Locksmith supply companies sell sets of "try-out" keys for certain automobiles made during certain periods and by specific manufacturers. Often one of these keys will open or start the car, or at the least serve as a superior pick.

ATTACK THE LATCH

Since locks may be resistant, and the latching mechanism more accessible than the layman might think, much of what falls under the rubric of automotive locksmithing has to do with attack on the latch itself, using a tool usually known as a shim or slim-jim. Designs vary among their target-autos. As with other lock tools, the amateur would do well to buy a professionally made sample before embarking on a costly and time-consuming construction program.

Slim-jims work by letting the lock student manipulate the latch directly, bypassing the lock connected to it. The path to the latch usually lies between the weather-stripping and doorframe and window. Finding the latch is a matter of experience for pros, trial and error for the first-timer.

They call it a slim-jim because it's slim enough to slip into the allowable space between the window glass and the weather-stripping. (Fords are notorious for having two layers of weather-stripping. The jim must go between the correct two layers, or it will not reach the latch.) Slip it in and probe. A sign that you have connected with the latch is movement of the locking button in cars whose buttons are visible from the outside. Now all that has to be done is depress, raise, rotate that mechanism, or move it front-to-back. The slim jim contains a variety of cuts and facets that allow multiple functions.



LEFT: Steel door w/deadbolt lock and handle lock. Anyone behind that stout barrier must feel totally secure.... It took the author exactly 70 seconds to pick both locks, first try. In addition to being master-keyed, they were keyed alike, 5-pin tumblers, of course. The author once dwelt behind that door. He has long since vacated, but, after the pick trick, installed a Medeco cylinder in the deadbolt and the landlord be damned. ABOVE: Top key is "bad:" 4 of 5 cuts on same level. Bottom key, which fits a Master padlock, shows wide variation in cuts, no two of which are the same. Excellent key.

It may be necessary to bend the jim before using it, out of vagaries in designs of various autos; and it won't work with all. The more seductive driving machines, such as Corvettes, have their locks protected by metal enclosures, along with alarm systems, bars that lock steering wheel to brake pedal, infrared bumper beacons of the type carried by potential kidnap victims....

The old coat-hanger method still works, if the locking buttons have flanges that leave the loop on the end of the coat-hanger enough purchase to pull up the button.

HANDCUFF LOCKS—AND KEYS

Although it is possible to fashion an expedient tool to open most handcuffs, the most efficient means is to buy and secrete one or several handcuff keys on your person. Keep one where it is likely to come in handy, such as the inner lining of the front and back of your belt (if you anticipate that a bounty hunter will cuff you).

MASTER-KEYED LOCKS

Conventional 5-pin tumblers have a limited number of possible combinations of key cuts that give unique keys. Tolerances limit the subtlety of a cut that falls outside normal machine tolerances. For some 5-pin tumblers, this can mean fewer than 10,000 unique keys.

Look at master-keyed locks. These locks will open with either the owner's key, or the masterkey. The reason lies with additional top pins. The cylinder will open at the "regular" shear-point, or at another set of shear-points created at junctures of additional top pins.

Now, because the number of workable shear-points may double with one level of master keying, these locks pick easily, other things being equal.

Some locks include two, three, sometimes more additional top pins to allow for higher levels of master keying. For example, an apartment complex owner may wish to give master keys to only one of four buildings to the maintenance person in charge of each, while reserving the grandmaster key, the one that will open all locks, for himself.

DRILLING

First, if you must drill, you have probably encountered a pick-resistant lock. That means it likely sports drill-resistance as well.

The end of drilling is to create a new shear line that will let the internal cylinder turn. A proper drill point cuts straight through the existing line of pins and is wide enough not to leave pin fragments large enough to impede turning.

What kind of drill do you need? You'd think a damned powerful drill—at least 1/2", and the more horses pulling the better—along with a set of carbide-tipped bits, since you will have to drill through one or more layers of carbide to get to the pins (in fact, some of the pins may be carbide, judging from what the author saw in a locksmith's Medeco box of replacement pins). Yet one lock authority endorses a rechargeable drill and soft pressure, so as not to strain the drill or break the bit. He finds its slow speed easy on the bit.

Holding the drill yourself for the hour or so it takes will wear you out. Remember James Caan's trick in Thief, that magnet-mounted drill press? Neat; but surely you will not be drilling a safe....

With drilling we encounter a recurrent theme in spookdom: There exist just so many sources of carbide bits, big drills, magnets or clamps, and other engines of sin. The routine of tracking down the purchaser(s) occupies most of detectives' time, but it pays off. The circumstantial evidence of proving that you bought a combination of tools used to commit a certain burglary is enough to trigger a very detailed check as to your whereabouts on the evening of the perp. Better fabricate a hermetic alibi or, better, hire a Miami lawyer....

PADLOCKS

As a rule, if you plan to defeat a padlock, and do it quickly, get a pair of bolt-cutters that will fit the size of the hasp. Sure, picking, rapping, springing and so on may impress us with their finesse; but finesse is very different from results. And bolt-cutters can do double-duty if you have to fade through a chain-link fence after the caper....

CHOOSING AND USING LOCKS

Locks provide at best an illusion of security. They symbolize territorial barriers whose strength or flimsiness is defined by the determination of those who keep them and those who would break them. Criminals' determination, more likely recklessness, has risen, while locks have lagged.

First of all, match the lock to the door, and vice versa; and match both to the security level of what's behind the door. A seven-pin tumbler that would prove a bitch to drill and a nightmare to pick will remain untouched when the felon jams a car bumper-jack in the doorway and pries the jamb away from the lock.

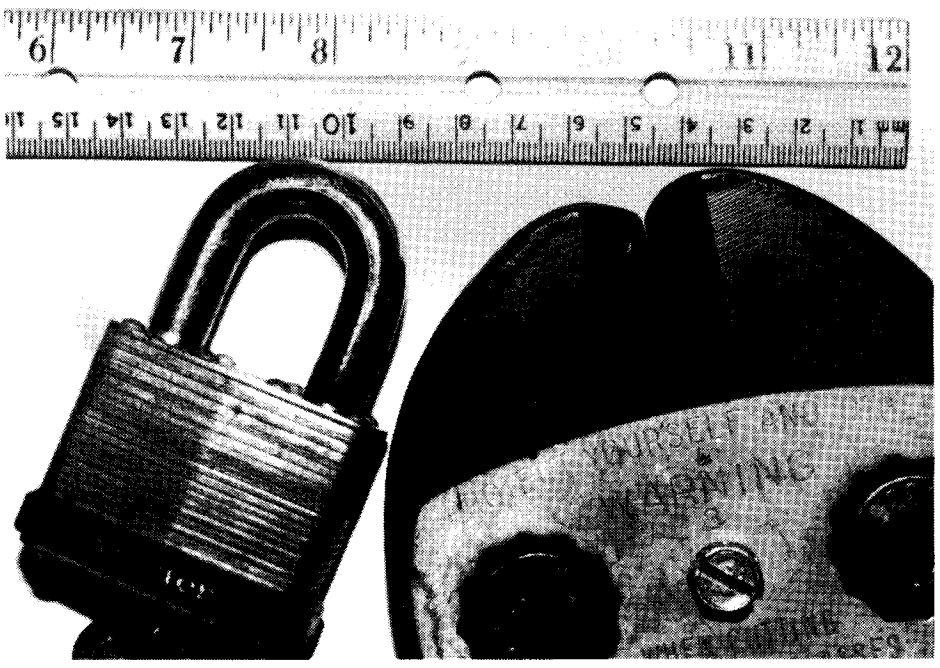
Next, make unobserved access difficult. The discount stores have been flooded with passive infrared devices hooked up to a pair of sockets for floodlights that bathe a prowler in glory (the burglar will shoot out the lights with a BB gun before the B&E...).

The critical elements of premises security provide for difficulty of access, either through too much effort to get in in relation to the worth of the booty, or too great a risk of capture.

MICROTRACES

Letting yourself into your own home, office, or mailbox via picking, because you lost the key, will not prompt an all-out manhunt and mobilization of the FBI crime lab. But those who would break into genuinely secure premises with picks should be aware that A) microscopic bits of pick-metal will be left in the lock, B) microscopic bits of lock- and pin-metal will be left on the picks and the operative's fingers (and in his nostrils and hair, and on his skin and under his fingernails; in the fabric of clothing worn during the crime). The compositions of these alloys can be determined with utter certainty, and bits of lock metal under your fingernails or on a set of picks found in your possession is awfully wicked evidence to tie you to a felony....

The same principle applies to carpet-fibers adherent to the soles of your shoes, particles of dirt indigenous to your driveway found on the floor of the target room, and a wealth of semi-invisible traces science can gather, analyze, and tag to a person or place: pollen, hair, blood, saliva—even your kiester-print lifted off a toilet seat.



5
SECURITY

Now it's dark....
—Frank Booth, Blue Velvet

* * *

The rare reader indeed has not screened a recent film whose closing credits bore the distinctive double-D logo of Dolby Laboratories, Incorporated, to signal that the film's soundtrack was recorded in Dolby Stereo[tm] and that selected theaters will play it back with that proprietary effect. Note that those selected theaters have hung speakers around the sides and rear of the hall, this for the so-called surround information. In addition, they hide left, center, and right speakers behind the screen.

To deliver stereo surround sound, selected theaters must use a device known as a decoder, which lets them extract four channels of sound from the two optically coded ones on the film print. For years, long before stereo became widespread, all prints, including films recorded in mono, have borne two separate soundtracks. Four channels blend into two in the final mix—excluding the discrete six-channel Dolby format—with the addition of specific phase-shifts among them. A surround sound decoder detects phase-shift, then uses that coded information to feed signals to the correct speakers.

And it's amazing what they've planted in the mix. Take the soundtrack from Star Wars, a seminal film in surround sound out of the massive boost it gave the concept. Feed the two-channel signal into a Fosgate Research Tate II 101-A decoder, a device that reigned briefly as the Cadillac of decoders in 1983, still with a dedicated following among multichannel buffs. Balance the input, set the matrix for "surround," then roll a stereo copy of Star Wars. During the attack sequence on the Deathstar, kill the power to the front channels. Listen closely to the rear channels and you will hear the unmistakable whistle of a toy train twice tooting its herald as Darth Vader's private ship, flanked by two Imperial fighters, zooms into the screen away from the viewer. Dialog just prior to that shot says something like, "...Gold Leader. Move into position..." as the rebels prepare another quick and deadly pass at the target. The sound man must've been in a pixie mood that day, mixing these cutely anachronistic hoots with sounds of advanced technology warfare...or maybe Vader had a thing for trains....

Information hides too in ordinary FM-band radio signals. It uses either a 67 KHz or a 92 KHz subcarrier. We can extract it with a decoder that sells for less than $40 in kit form. As with cable TV, it may be illegal to receive these signals without paying a fee. However, pirating of such signals, long a known practice, cuts little into the intended market for them (background music in supermarkets, pharmacies, and doctors' offices) and thus has not drawn heavy fire from vendors.

Assembly of FM subcarrier decoders challenges only the true beginner, but finding the correct place in the radio to hook the decoder demands some working knowledge of the unit, preferably a schematic.

OCTE Electronics (formerly ETCO?), Box 276, Alburg, VT, 05440 sells a subchannel audio kit for $39.95, plus $9.95 for a power supply. They offer also a directory of hidden signals for $8.95, as well as an assembled portable FM radio with SCA-decoding capability built in for $89.95. Panaxis (Box 130, Paradise, CA, 95967) offers an SCA kit without mention of power supply for $29.95.

The examples illustrate coding. We don't know what's there until we dig it out. In these two cases, the proper decoder brings forth hidden information whose presence we would not otherwise suspect. Coding of other types keeps us from getting at information known to be present. Examples include encryption of radio transmissions and computer files, as well as the most irksome form of coding, cable and satellite TV scrambling.

PAY TV AND THE SPECTER OF SCRAMBLING

GENESIS OF SCRAMBLING AND DESCRAMBLING

Forgive the pun, but it's hard to lock on to this subject, fluctuate as it does from month to month in all arenas: legal, technical, perhaps even spiritual. Encryption and scrambling safeguard information perceived as valuable or secretive during storage or transmission. Human nature being what it is, it also poses an irresistible stimulus to unscramble. Humans cannot resist a puzzle, a challenge. And it appeals to the dark side of human nature, the side that wants something for nothing.

This explains a focus nothing short of frenzied on theory and hardware of descrambling cable and satellite TV signals. In a recent issue of a nationally distributed electronics publication, 37 out of 105 classified ads pertained in one respect or another to cable TV, satellite TV, descrambling coded signals of both, or defeating the latest scheme to copyguard videotapes. That same periodical contained 8 large space ads for similar products, including two whose construction the publication had detailed.

On top of which, the descrambler underground has surfaced with its own journals, videotapes that show hands-on defeating of the dread VideoCipher unit, and a free phone line updated weekly (see transcripts of selected Scramble Facts below).

SECURING PREMIUM SIGNALS

To delineate a structure known to all, cable TV franchises buy rights to sell programming from nationwide distributors who use satellites to dish out the product. Distributors, in turn, pay producers for programming, and in growing instances produce original programming. It all costs money, and nobody works for nothing. At each step, from pre-production to home viewer, somebody has to get a cut of the action. If viewers had a choice, most would prefer not to have to pay to get cable or satellite TV services.

Providers feel that free interception of their signals constitutes a theft of sorts. Many viewers hold that the airwaves are free. The solution adopted by suppliers, at multiple tiers, involved altering signals such that, though easily intercepted, they could not be viewed in digestible form.

It is worth noting that bitter ongoing controversy plagues scrambling at the several levels of distribution. Providers at any tier offer the stock response: protection of revenue sources. Some claim total yearly losses of $600 million from simple failure to terminate service to subscribers who've dropped it, never mind what's lost to those who illegally access pay services.

The other side sees it differently. They allege that scrambling "killed" the satellite TV industry, citing a drop of 90 percent in private satellite dish sales after scrambling began. They have hinted, too, that program-providers constitute a monopoly and have violated anti-trust laws. They insinuate that local distributors who refused to scramble premium services have been denied franchises. They accuse certain trade associations of "blacklisting" those perceived as "video pirates."

Two major bodies of literature and hardware and jargon deal with two different sectors of scrambling: cable and satellite. Before we can discuss either with any surety, we must get a simplified grip on the strange and mystic nature of the TV signal.

UNDERSTANDING THE NTSC TELEVISION SIGNAL

—ain't easy, especially for the novice. Getting picture/brightness outlines (i.e., a simple black-and-white picture), color information, sound information, and now stereo sound information coded into standardized radio waves was no cinch. The National Television System Committee adopted what has come to be known, surprisingly enough, as the NTSC format for use in the United States. Several other countries have standardized it, while most European states use other systems, known as PAL and SECAM, that we won't try to explore. Understanding the basics of the NTSC signal is essential to grasping even the simplest scrambling/descrambling schemes.

First, as anyone who has looked closely at a TV screen can tell, the picture is composed of discrete horizontal lines. An electron beam moving across a phosphor screen in a horizontal line causes the phosphor to glow in proportion to the intensity of the beam, which is modulated by information in the video portion of the NTSC signal.

The NTSC system uses 525 horizontal lines per frame, but for reasons explained momentarily, even the best television sets display only 300-330 of them. The remainder of the lines carry information needed to reconstruct a picture from the video information.

The moving electron beam crosses the screen left-to-right to write one line—but it must somehow get back to the left of the screen without being seen before writing the next line, otherwise its return path would streak the picture. This created the need for the horizontal blanking interval, a period during which the electron gun shuts off as the now-invisible beam returns to the left of the screen to start its next sweep. The diagram illustrates the horizontal blanking period.

Now, instead of writing a whole picture in one pass of 525 lines, the original engineers chose to use what is known as an interlaced picture; that is to say, 265.5 lines write to the screen every 1/60th of a second. Every other set of lines writes between the last set. That gives us 30 complete pictures each second.

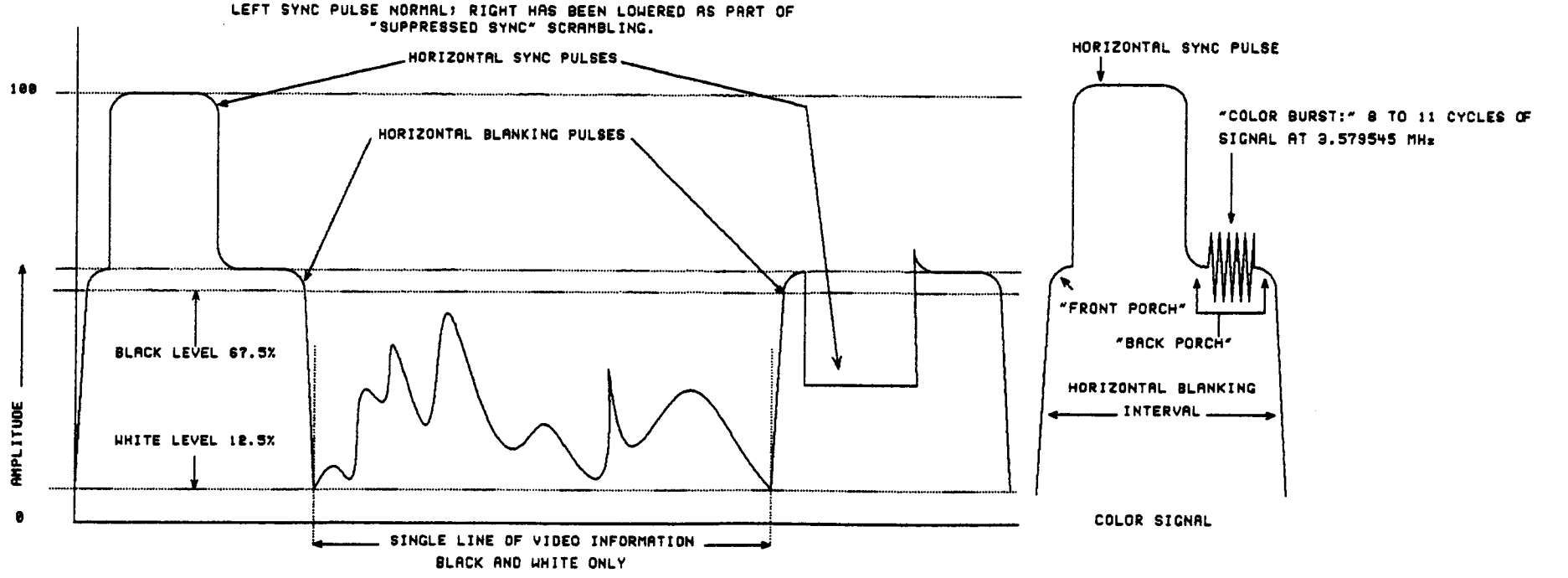
The timing involved calls for microsecond-accuracy to display a stable picture. That demands precise synchronization of all events: scanning of the beam, its brightness within a line, turning it off as it returns for its next sweep, and so forth. Thus, the NTSC signal devotes considerable space to what are known as sync pulses to keep timing on mark.

Sync pulses are significantly higher in amplitude than the video detail information to let the receiver distinguish the two easily. Refer to the diagram. The tall, narrow plateau is called the horizontal sync pulse. Everything else keys to it. The broader plateau on which it sits, and whose amplitude lies above "black level," is known as the horizontal blanking interval. During this period, the scan beam turns off to return to the left side of the screen and begin a new scan line. Without horizontal sync, the picture "tears" side to side. Screw up the horizontal hold control on your set to see what it does.

Actual video information lies between each horizontal blanking interval. Note that the signal between two HBIs represents only one line of video information. It takes 525 lines to build a single frame of video, thirty frames displayed per second.

And that's just the B&W picture. What about color? Mixing variable degrees of the three primary colors—red, green, and blue—can generate any color. For that reason, color television sets contain in effect three electron guns, one targeted to a red, one to a green, and one to a blue set of phosphor dots on the screen. All three beams scan as if they were one, save that the relative intensity of each beam varies during a scan line so as to generate the desired color. The mechanism of cramming color into an already cramped signal is just too complex to discuss in a text of this limited scope. All that's important now is to note that a color TV signal differs from a B&W signal with the addition both of color information and what is known as the color burst sync signal, which appears on the "back porch" of the horizontal blanking interval. This burst tells the receiver where to pick up the color information relative to the timing of the burst.

One more point: In addition to horizontal sync, vertical sync must be present or the picture will roll. These pulses appear during the vertical blanking interval, that black stripe seen between pictures that are rolling (such as copyguard-encoded tapes played through cheap TV sets). The vertical blanking interval holds room for much additional information, including captions for the hearing impaired, digital data, internal color reference signals, and so forth.


LEFT SYNC PULSE NORMAL; RIGHT HAS BEEN LOWERED AS PART OF "SUPPRESSED SYNC" SCRAMBLING.
HORIZONTAL SYNC PULSES
100
HORIZONTAL BLANKING PULSES
BLACK LEVEL 67.5%
WHITE LEVEL 12.5%
AMPLITUDE
0
SINGLE LINE OF VIDEO INFORMATION
BLACK AND WHITE ONLY
HORIZONTAL SYNC PULSE
"COLOR BURST:" 8 TO 11 CYCLES OF SIGNAL AT 3.579545 MHz
"FRONT PORCH"
"BACK PORCH"
HORIZONTAL BLANKING INTERVAL
COLOR SIGNAL

Where's the sound? It's encoded in an FM audio subcarrier centered 4.5 MHz above the theoretical (don't ask) center of each NTSC channel. The audio subcarrier can hold additional information, and has proven a handy place for scramblers to hide data removed from other parts of the TV signal.

The video part of each NTSC television channel, whether channel 2 in the VHF range or channel 79 in UHF, occupies about 4.2 MHz of bandwidth, or radio-frequency space it uses to convey information. Each channel is allotted 6 MHz, but the unused spectrum forms what's known as a "guard band" to prevent interference between adjacent channels.

SCRAMBLING/DESCRAMBLING PART I: CABLE TV SIGNALS

We start with cable because, in general, it uses schemes simpler than those employed by satellite TV. Understanding cable methods smoothes the transition to highly sophisticated satellite machinery.

1. HASH SIGNALS

Early scrambling schemes injected one, sometimes two "hash signals" into the upper end of the scrambled channel. Authorized subscribers were supplied with "notch filters"—extremely narrow-band filters that removed the hash signals and left the TV signal alone. (Well, sort of. Hash signals impinged on both the upper part of the video information, where sharpness and detail lay, and the lower portion of the audio subcarrier. Notch filters removed a good bit of sharpness from the video, despite the fact that the cable company would usually boost that part of the signal in anticipation of notch-filter effect.)

The hash signals bore a standardized relationship to the center frequency of the channel, lying 2.25 MHz, or 2.225 and 2.275 MHz above it in the case of dual hash signals.

Most notch filters supplied by cable companies came in sealed metal tubes. This made it tough for experimenters to learn what was inside. Determined hackers, particularly those with proper test gear and a knowledge of TV theory, were able to determine the hash frequencies and build notch filters to purge it.

Probably the least secure of all scrambling systems, it still finds use in small towns whose subscriber-base will not support more complex systems.

Electronics magazines carry ads for tunable notch filters. Some vendors will let you try them before buying. There is no way to know, without expensive test gear, what band(s) need to be notched out, so it reduces to a process of trial and error.

As a matter of desperate importance, as well as a rude lesson in the perils of descrambling, note that placement of hash at the upper end of the video signal let subscribers manually detune their sets such that the hash cleared enough to catch clear, black-and-white video, but with loss of sound, since the audio subcarrier lay above the hash. In 1981 the author fell prey to a helpless vice for women wearing unnatural amounts of lipstick when detuning exposed him to the shocking video antics of Aerobicise....

2. PLAIN VIDEO INVERSION

Take the entire NTSC video signal and turn its amplitude upside down and you have complete video inversion. The resultant signal will paint nothing worth watching. Cable companies that used this scrambling method supplied subscribers with converters that re-inverted all signals, thus restoring them to usable form.

Here again, we deal with a feat that, in electronic terms, qualified as tuna casserole. Hackers found little trouble buying or building video inverters. The system has faded, the fate of all defeated methods.

3. SUPPRESSED SYNC

This gets into schemes that call for basic grasp of the TV signal. Suppressed sync cut the amplitude of the horizontal sync pulse by 6 dB. That stuck it down in the muck occupied by the active video information, and made it impossible for the TV set to get a grip on the horizontal hold. The result was a picture torn sideways.

How did decoders work? The sync information remained, but had slithered into a hiding place where ordinary television sets would never find it (the audio subcarrier in some systems; an "unused" portion of the FM radio band in others). Different versions moved it different places; it serves no point to list them all. All the decoder had to do in an electronic sense was "know" where the sync information lay hidden, retrieve it, re-insert it, and its job was done.

Hackers dug out the locations of the buried sync pulses, built "black boxes" that restored sync. Many were sold commercially, and Radio-Electronics magazine featured an article detailing construction of a suppressed sync decoder in 1984. That unit is still available in kit form at this writing, though the single suppressed sync system has begun to fade in the heat of defeat.

4. MORE SUPPRESSED SYNC

Known in some circles as tri-mode sync suppression, this version randomly suppressed horizontal sync by 6 dB, 10 dB, or 0 dB, even though the 0 dB suppression "looked" like it had no sync. The randomly shifting level of sync suppression obsoleted the old suppressed sync decoders, limited as they were to handling only 6 dB of suppression.

The sync information was encoded into the audio portion of the signal. A tri-mode decoder featured in Radio-Electronics in 1987 first filtered out the audio carrier, then extracted its buried sync information, then told three separate boost circuits how and when to boost the sync 6 dB, 10 dB, or not at all.

The photo shows this descrambler. It did not work with the author's cable signals, even though they bore the look of tri-mode sync suppression, perhaps because the sync had been moved outside the audio subcarrier...or maybe the author killed an MOS-chip or two during assembly....

5. SSAVI

Things got genuinely ugly when sync suppression mated with active video inversion, which is what the acronym SSAVI means. Active video inversion infers that video inverts or not depending on any number of control factors a scrambler may select. It may occur in relation to overall scene brightness; it may occur every other line, leading to an extremely dim image; or it may occur in response to specific digital pulses, stuck in the vertical blanking interval, that tell which lines to invert and which to leave alone.

For a long time, SSAVI remained one of the most secure systems. Not that it lay beyond the reach of dedicated hackers, for black boxes to defeat it soon appeared. But it began to reach the point of diminishing return in terms of effort needed to defeat the system compared with simply paying for services and a legal decoder.

Lately, though, and in some units only, it's been found that astonishingly simple changes to a single chip and removal of one resistor will defeat the SSAVI decoder. The secret lies in attacking the chip that tells the SSAVI circuits which channels to descramble, rather than trying to duplicate the descrambler's functions. This theme has come to the fore as scrambling methods have improved and the decoders have become dependent on control instructions.

6. ADDRESSABLE DECODERS

The latest generation of cable TV boxes descramble or not depending on what digital codes the cable TV company programs into them. The companies can now identify each box over the line by its unique digital mark, and tell it periodically what to receive and what not, just in case it has forgotten, or somehow been reprogrammed.

It's almost like having Big Brother in your living room. Cable TV companies can get information about you, what your are watching, receive signals from you if requested, all from that innocent black box....

7. UGLINESS AND FOUL DEEDS

This business of buying a cable TV decoder and either modifying it to descramble, or using an outboard

descrambler, seemed to remove the user from the realm of theft—at least in a spiritual sense, and in his own opinion—such that few saw themselves as thieves. It was simply a game of viewer versus greedy cable interests. Some used the high and climbing price of premium services to justify wetting their beaks for free.

Others took affirmative action that pretty well marked them as slime. For example, they would identify the massed cable input to their apartment building, trash its usually pathetic padlock, then either connect their apartment line to a live feed, or cut an active feed going to another apartment, install a two-way splitter, restoring service to the legitimate customer but giving the thief a free sample at about 4 dB down (splitters halve the signal and involve insertion losses as well; 4 dB loss is usually tolerable).

Cable companies began to install electronically controlled switches out on the pole that would activate a given customer's line, but some super-aggressive thieves climbed the pole and tapped directly into the main feed.

The pay TV industry at all levels views theft of service as theft, period. It has gotten state and federal laws erected on its side...and enforcement of a federal violation falls upon the FBI....

Hazards have begun to plague illegal viewers. One cable TV repairman told the author that he carried gear in his truck that would let him "spot illegals from the street," meaning that signals emanating from your residence and detectable for some distance would provide hard evidence of getting services without payment.

As noted, the newer cable boxes can receive instructions from the cable office, and can give status information as well. If you had substituted your own decoder, one not equipped to return the proper pulses, and the company ran a spot check on your unit but failed to get the right return code, they would want to know why. They might send a repairman out, accompanied by the police if need be, to "fix" your problem....

THE FUTURE

Some cable TV decoders can descramble satellite signals. The Oak series is one of them, meaning that the cable company receives the signal at its dish, then pumps out the unmodified scrambled signal. Your box will handle it if you're authorized. This saves money for vendors, but probably signifies that cable TV is headed for the type of battle now being fought by General Instruments in the satellite arena.

SCRAMBLING PART II: SATELLITE TV

The hard stuff, intercepted by satellite dish owners (referred to generically as TVRO—television receive only), takes a computer to decipher. The unit that houses it is known by the trade name, VideoCipher, the most pervasive being VideoCipher II, or VC2. General Instruments makes the VC line of descrambling products. Both VideoCipher and G/I have earned a place in infamy among descramblers, as well as those whose satellite businesses allegedly died as a result of scrambling.

Note that several other schemes exist to encrypt satellite TV signals, including Videocipher I, Satguard, Orion, MAC, and Polaris. Some of these apply digital or "hard" scrambling to the video as well as the audio. This text treats only VC2, since it has become the de facto standard, at least for the time being.

Here VC2 designates also the particulars of scrambling. The video signal is scrambled to a moderate degree of security through cable-like means. The audio portion is hard-scrambled through analog-to-digital conversion, then encryption through the DES algorithm. The true security of the system lies in the resistance of its audio to any practical direct attack.

It was widely believed, or at least touted, that no one could defeat the VC2, based as its audio was on the Digital Encryption Standard. Possession alone of a VC did not guarantee that it would descramble. The pay TV service had to authorize each customer to receive its signals. It did so by providing code keys, entered into the VC by the user and changed every 30 to 90 days, that told the processor whether to unscramble a given signal. If proper codes were not entered on time, the changing data stream disabled scrambled services. Identifying customers was easy because each VideoCipher contained a unique electronic signature that made it addressable.

But the VC fell rather quickly to attack by determined experimenters driven by the hacker mentality. Had they struck the DES side of it their efforts might have dashed against impenetrable defense. Instead, they analyzed the pathways through which the VC's internal computer told its other components to descramble. These commands lay buried in chips containing computer programs of sorts, known as EPROMS (erasable programmable read-only memory). Hackers extracted the programs built into the chips, disassembled them, identified key attack points, re-wrote the programs such that all, most, or selected signals would decode, then installed EPROMs bearing their own modified programs back into the VC. These circuits came to be known generically as "magic chips."

Did they work? Yes.

Was G/I pissed off? Apparently so.

It triggered the predictable series of countermeasures and counter-countermeasures that mark the whole scheme as a human undertaking. First, G/I made it hard to get at key chips by encasing them in epoxy resin (see diagram of VC board). Hackers responded by removing the resin after melting it with heat guns or dissolving it with methylene chloride, aka paint remover. Both processes were tricky and potentially hazardous, both to other components of the VC and to the experimenter. "Professionals" would clean a board for $25 to $50. The instructional videotape, The Pirate II, demonstrated hands-on methods for removing epoxy.

Surely the most colorful word-grove now blooming in the American vocabulary has to come from satellite piratedom. They referred to chips and processes as "the Three Musketeers," later "Four Musketeers;" "the Wizard," "Doomsday," "Clone," "Chameleon," "Parasite," "Load Star," and "Zombie."

Companies dealing in hardware (chips) and software came and went almost like a different postman every day. Bad merch got distributed along with the good. True, some firms endured, but are now facing the kind of legal onslaught that only America's big and extremely well heeled corporations can mount. It seems that the cost of "experimenting" with the VC exceeds the cost of paying for services. That leaves the hacker mentality as the only motive, and tells us that these groups lack the resources to contest serious legal sanctions. Would the ACLU bite on this one in favor of the defense? Ralph Nader's group, maybe? Don't bet your VC on it....

Perhaps the most intriguing and ironic of all twists in this move/countermove scenario stems from allegations that booming VideoCipher sales arose from pirates' handy tricks that defeated the VC. Once word got out that the VC had been broken, sales took off so fast that G/I reportedly built up a nine-month backlog of orders for VideoCiphers. G/I might dispute the hackers' reasoning here. In any case, it cannot complain about a surge in sales of its product.

THE LITERATURE OF SATELLITE TV DESCRAMBLING—

—ranges in quality and utility from abysmal to superb. Books, newsletters, and videotapes, even a phone service which may or may not still be a going concern by the time this book makes it to market.

NEWSLETTERS

These run a gamut from mainly-satellite to mainly-cable, with one publication offering information on both systems. We'll introduce you to three.

Scrambling News

Available from Shojiki Electronics, 1327 Niagara St., Niagara Falls, NY, 14303, at $24.95 per year. Back issues (to October, 1987) available as of this writing, $3 to subscribers, $10 (!) to non-subscribers. Sample copy $5.

We had a chance to look over the March and April, 1988 issues, both dealing at length with the SSAVI (synchronization suppression and active video inversion) system of scrambling signals sent to cable customers,

along with the Zenith STV-1 descrambler. Material presented under an apparent pseudonym, "D. Scrambler," some printed on a low-resolution dot matrix printer, some on a higher-resolution printer, along with printed material and diagrams that appear to have been photocopied from manufacturer's manuals. Schematics abound, some quite clear, others so small and smeared as to be useless. With little to guide the novice, this series of articles looks as if it might be of interest to the experienced electronics enthusiast or hacker looking for that last bit of critical information to find out why his home-brew descrambler for SSAVI isn't working. Prior issues dealt with phone phreaking, turn-on techniques for specific decoders, tapping into cable TV lines.

The Decoder[tm]
"The technical newsletter of the satellite and cable descrambling industry." April, 1988 issue. Features screened photos of reasonable quality, typesetting is compressed-mode dot matrix printer using the WordStar[tm] method of right justification.

News stories (e.g., U.S. Customs' seizure of several thousand VideoCipher units which were allegedly going to be shipped to Mexico, something said to violate U.S. Law that forbids exporting DES technology; see report of "Mr. Chips'" tour of Mexico, described later under Scramble Facts).

Product review in this issue: the G/I 2600 series IRD (integrated receiver-decoder, a satellite receiver that has a VideoCipher built into it). Despite undertones of rancor against G/I felt in scanning much TVRO material, the reviewer put aside whatever bias he might have had and gave this unit top marks, but admitted it to be expensive.

Remainder of the issue contains large, detailed schematics of the Oak Orion PD 400C, though some component values, such as diode part numbers, are missing.

Tells of an extremely simple means to defeat the SSAVI system, at least on some units, that obsoletes outboard decoders. It involved shorting two pins on a readily identifiable IC chip, and removing a resistor if one is present at a special location. Contains mainly VideoCipher-oriented ads.

Published by Telecode, Box 6426, Yuma, AZ, 85364, $18 per year, single issues $3.

The Blank Box Newsletter
"Your source for the latest in Black Box devices and de-scrambling news." Vol. 3, No. 3.

Sporting the most professional look of the newsletters reviewed, hardly surprising since it appears to have been typeset with a laser printer and one of the better desktop publishing programs, Blank Box Newsletter comes from Resort Publishing, 100 Bridge St, #27, Hot Springs, AR, 71901. Yearly subscription $24.95, single issues $5, though the publisher seems eager to send single sample copies gratis upon written request or a call to 1-501-321-1845. Our sample was copyrighted 1987, though we requested it in the spring of 1988, so it isn't as if they are giving away the latest in this rapidly shifting field.

At forty pages (more in later issues, at least per their ads), easily the longest of the bunch, but only nine pages of news and technical articles. The remainder contained space ads, often full-page, from vendors of VC-defeating and repair gear, from software to chips to mechanical aids.

....which happens to be exactly what many subscribers seek. It has been alleged several times in material we reviewed that most of the VideoCiphers in use have been modified to receive scrambled services without the user necessarily paying the required fees.

This issue contained a report on the STTI/SBCA trade show in Las Vegas, as well as the most trenchant editorial material we have seen in descrambling letters. Technical articles range from beginner/explanatory—quite welcome if you have not mastered the lingo of the VC—to extremely technical, though apparently not beyond the grasp of the readership. Reviews products, offers notes from the "underground," and classified advertising free to subscribers.

Overall, the most incisive, contemplative, and professionally produced of the letters reviewed. Both BBN and The Decoder let the reader on to a free call-in information service known as....

Scramble Facts

Phone 1-718-343-0130. A new recorded message every Friday, except June, July, and August (every other Friday; message at end of August, 1988 stated at that Scramble Facts needed more callers to keep going), 24 hours a day, free, with some commercial slant, as seen from this partial transcript recorded 5/31/88:

> Get ready for another monthly code change on the first of June. The new 26-data is being transmitted now. Those with self-sustaining units such as Testron's PROTEC test devices are advised to park your VideoCipher on a non-pay-per-view service when not in use. Be sure to leave both the VideoCipher and receiver turned on all the time. This is necessary to capture the new monthly code data.
>
> Have you seen the new videotape from Blank Box Newsletter, A Pirate's View, Volume III? This 2-hour production divulges the newest information and products related to VideoCipher descrambling. Watch as they use the latest techniques and learn how easy it really is. See Testron's PROTEC test devices, the Wizard, Doomsday, and Parasite technology. You will probably come to the same conclusion we have after watching this outstanding tape: The only totally self-sustaining device is the one designed and manufactured by Testron. By the way, we noticed that the ribbon connector was damaged and repaired on this device. Blank Box should have asked Testron for a replacement. It did make this otherwise perfect device look sloppy. The tape selling (sic) for only $30. Mastercard, Visa, and COD orders are accepted. Call Blank Box Newsletter to order. Mention Scramble Facts and they will deduct $5. Also request a complimentary copy of Blank Box. They can be reached at: 501-321-1845. Call Testron at: 516-358-9414.
>
> Technical tips: Here are two problems associated with the power supply inside the VideoCipher. First, verify the VC board is working properly by testing it in a known working unit. A loud hum, and/or dark bar on the screen, is a common indicator of a power supply failure. Check the 12-volt regulator, IC904. It may be shortened (sic) or defective. Also suspect capacitor C931, a 25-volt 3300 microfarad cap. If the VC light flashes once and then refuses to stay on, then suspect the minus 5-volt regulator, IC906, or the minus 12-volt regulator, IC905. The capacitor C933 will most likely also be defective. C933 is rated at 25 volts, 3300 microfarads. If your board was working prior to the installation of a socket at U30, and is not working properly now, let's validate the reset line circuit associated with U29, an RCA 3406. Place a logic probe or scope on pin 13 of U30. A digital signal should be present. Now short pins 2 and 3 together on U29. This should stop the activity seen on pin 13 of U30. If this activity has not stopped, then U29 is probably defective.

This message, taped in a grim interlude of sheer boredom at 4:52 AM, was recited by an energetic-sounding woman who spoke fluent Brooklynese punctuated with bits of broken English.

Note that descrambling has its own jargon, much of it common to the electronics trade, that you must master to understand what Scramble Facts is talking about. "U," "IC," "microfarad," "picofarad," "cap," "pin," and so forth are common electronic terms. U20 is referred to most often when dealing with the VC, since that's where the action is.

Excerpt of Scramble Facts 3 June 1988:

> Scramble Facts, 3 June, 1988, updated every Friday at 5 PM eastern, updated every other week during June and July, your free service covering the latest news on the TVRO industry, each program devoted to: news and views, technical tips, and new product information. Please tell your friends about Scramble Facts, and call in every week. Each call counts. Thanks.
>
> The monthly code changes started on the first of June, and is 26A5 for 018 units; and 26C4 for 010 units. It is quite possible that a mid-month code-change will occur in June. This is part of G/I's ECM: electronic countermeasures program to disable Keyboard Wizard-type devices. A new 27 code is being transmitted now. Once again, we advise all VideoCipher owners to keep their VC and receiver on all the time. When you are not watching TV, park your dish on a scrambled service, but not a pay-per-view transponder. The same advice applies to IRD owners.
>
> G/I is designing a new scrambling system to be known as "Newcipher." The new system is expected to contain two scrambling systems. One would be compatible with existing VideoCiphers, and the other

would contain additional features, such as new security software, hard scrambling of video, high-definition TV capability, and anti-taping capability. The Newcipher is expected to supersede the existing VideoCipher in the next two years. Additional (sic) Newcipher will supersede the unreleased VideoCipher II Plus system. G/I is reassessing introduction of long-awaited Video II Plus, which has become known as the VSLI [VLSI?—ed.] unit. Rumors are that the VSLI unit is not working properly. The introduction date has been pushed back repeatedly for at least a year. If G/I's performance in introducing the Newcipher is similar to the introduction of other new VideoCipher products, then we can expect delays far beyond their target date of early 1990.

Technical tips: Does your VideoCipher lock up when inserting or removing the power cord? Then add a 10,000 ohm resistor between R86 and ground. Also add a 10 picofarad cap in parallel with the new resistor. This will allow a cleaner reset signal to be sent to U7. If you are experiencing flashing letters and/or numbers intermittently in the upper-left corner of your TV screen when using your VC, examine pins 11 and 12 on the U30. A bad connection or a cold solder joint will cause this problem.

In a number of letters we have received, we have been asked to explain the term, "trap." The VC II microprocessor, U19, has preassigned programs in the U30 called "traps." This term does not mean "ambush" or "pitfall." It does mean "snare" or "stratagem." Most microprocessors employ similar computer vocabularies. However, this CPU, U19, a Texas Instruments 7001-4, is the only one we know of using this term. A similar CPU, 8085, uses the term, "vector." The purpose of the command is to save on software space, thus allowing a greater economic condensation of data. A single byte of code is used to direct the CPU to the program. In the VC II, the op-code, F9, is trap 6, and is used in obtaining data and commands from U7. Next time, we will explain offsets and indirect addressing.

Send new products, news, and comments to: Scramble Facts, 71-34 Austin St, Forest Hills, NY, 11375. Don't forget, call Scramble Facts in two weeks for more up-to-date information.

Interesting that Scramble Facts and the pirate subculture have adopted a military designation for the struggle: ECM—electronic countermeasures—is an acronym bandied handily in the lingo of warfare....

Excerpt of Scramble Facts taped 1 July 1988:

[extremely sarcastic/histrionic tone]
Well, I just left our laughing room with G/I's form-letter to over 9000 satellite dealers. This curious document demands that the recipient cease and desist in the alteration, sale, or use of modified VideoCipher descrambling equipment. Many of the letters Scramble Facts has received are from dealers who do not engage in this illegal activity. Apparently, G/I has obtained the subscription mailing list of a leading satellite publication. This shotgun approach is about to backfire. Some of the letters to Scramble Facts stated that they will now start this illegal activity since G/I has already determined, without facts, that they are guilty. A few dealers have taken this silly letter to their lawyers and have started actions against G/I for harassment. The letter goes on to state that G/I's remedies include damages up to $25,000 and up to five years in the gray-bar motel for each violation. Now, we do know that G/I has sold approximately one million VCs, and we do know that only 350,000 are currently authorized. Therefore, if each dealer altered ten units, G/I will have to prosecute over 65,000 parties. Of course, the government will have to build a few new jails, as the total sentences will add up to 3,250,000 years. Of course, this action will help balance the national debt, as the fines will be as high as $16,250,000,000. The real fact is, up to this date, G/I has not collected enough from fines to cover the postage of this mass mailing. In a few cases the fine was only twenty-five bucks. Our jails are overcrowded with hard-core professional criminals, so let's release a few murderers, rapists, and drug-dealers to make room for those supreme enemies to society, the VideoCipher hackers. Carbon copies of this letter are addressed to: The FBI Headquarters, Fraud and Copyright Division, Washington, DC; the local office of the FBI; and to the Vice President and General Counsel of G/I. Informed sources have told Scramble Facts that, should this letter fail to stop this illegal activity, G/I is prepared to send the letter directly to your mommy, telling her what a baaaad boy you have been.

Excerpt of Scramble Facts taped 15 July 1988:

Informed sources have told Scramble Facts of visits by federal agents to the homes of satellite-dish

owners in upstate New York. The alleged feds flashed badges and demanded to investigate the owners' VideoCiphers. The feds confiscated the VideoCiphers, leaving only a handwritten receipt. Needless to say, this is a new scam—or, is this a new branch of Big Brother law enforcement, the video police? [theatrical sound effects: sharp rapping on door, followed by terse command: "Open up! Video Police! Open Up!"]

If you've been calling V. C. Hacker in Hot Springs, Arkansas, and the phone keeps ringing—good luck. He has been served a restraining order preventing him from conducting any and all business until a court appearance on the 28th of July. G/I will probably either delay the action or win a permanent injunction. In any event, it appears that V. C. Hacker is down for the count, and will not reopen.

The newest VC boards are numbered 0190, 0191, 0192. This is a normal continuation of the hexadecimal ID numbers. Some of these boards have 3.1 software. Most invoke 3.0 software. Our technical staff has also seen 018 and 018F boards with 3.1 software. There are no external differences and the epoxy is still the same. Our staff is comparing both softwares and will report any significant differences in the near future. Stay tuned.

Excerpt of Scramble Facts 29 July 1988:

Who will be the first person killed in the U.S. as a result of an alleged altered VC? With the FBI sending SWAT teams with automatic weapons to investigate some complaints by G/I, someone is bound to get hurt. G/I, this message is for you: We don't need Big Brother, the Video Police, in this country. [sound effects: sharp rap on door followed by voice: "Video Police! Come out with your altered VideoCipher or we'll shoot to kill!"]

Excerpt of Scramble Facts 5 August 1988:

A very reliable source of information recently told Scramble Facts about a business trip he had just completed throughout Mexico. You see, our friend—let's call him "Mr. Chips"—thought he could sell a ton of chips and VCs south of the border. Well, what a surprise Mr. Chips had. It seems that every TV store, every TVRO dealer, and just about every taco stand had VCs in stock. No shortage of VCs down there. Most of the dealers were offering chipped-out units. The others would modify the units while you waited for 'em. Our friend returned with his tail between his legs, unable to make a single sale in the whole country.

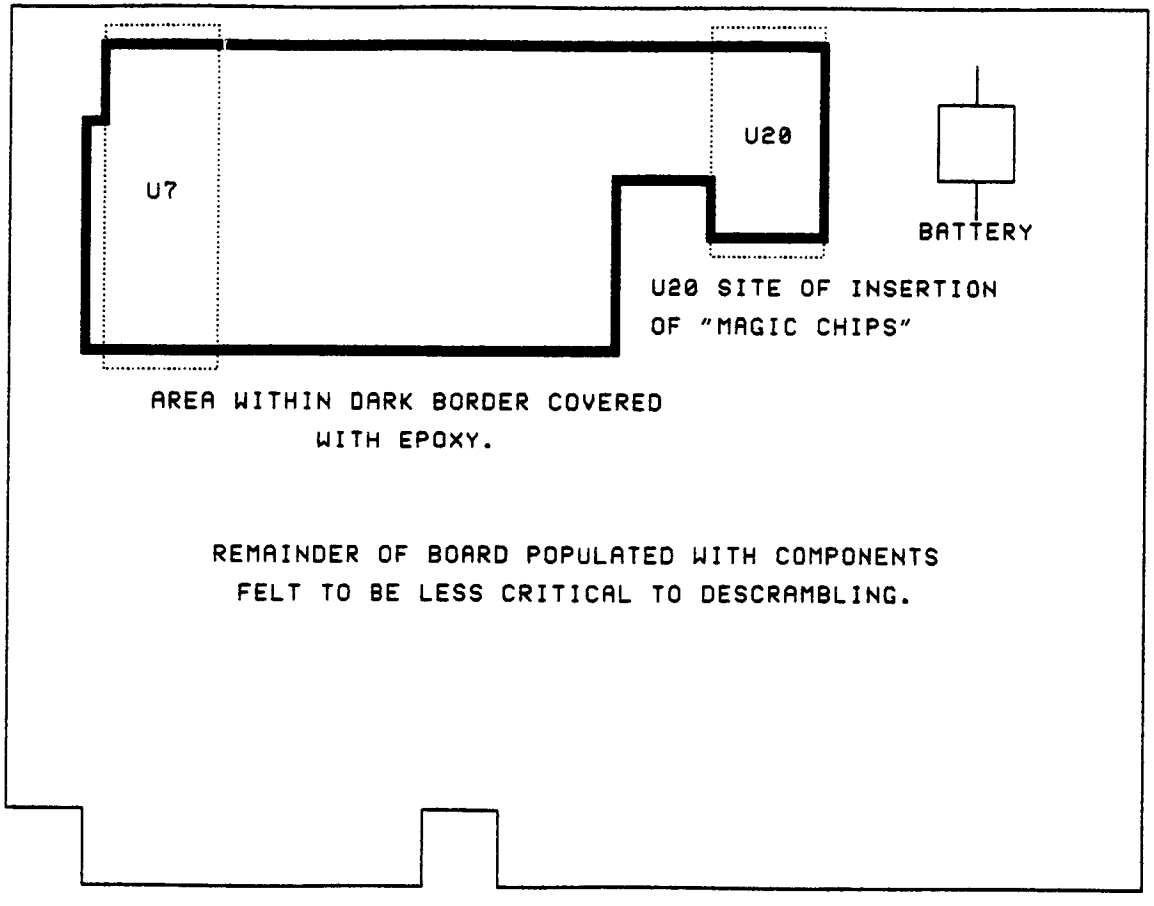
Scramble Facts has just celebrated its birthday.... In case you were wondering, we have received 158,576 calls during the past 12 months. That averages out to 440 calls per day.

Summary of The Pirate Video, Volume III:

[Tense music from Mission: Impossible. Opening graphics: "Warning! This video is presented for educational purposes only! Products shown may be illegal to use in the U.S." Cue ominous Dragnet theme. "Some modifications to the VC II may be illegal in the U.S. Have a nice day!"]

[narrator's voice:]
"The sole purpose of this video is to document the activity within the satellite underground as a news event. Certain products and activities shown on this video may be illegal in the United States. This video documentary is not intended to encourage, promote, or entice viewers into becoming involved with activities that may be illegal."

[Captain Kangaroo theme music; cut to shot of VideoCipher II]
[summary of narration:]
VC introduced 1986, supposedly unbreakable, broken quickly, approximately 750,000 VC2s, 80 percent of them modified. When news that the VC2 was broken the demand exploded. "Literally overnight," existing stocks of VC2s sold out and it took about nine months for supply to catch up with demand. At time of tape, VC2 selling "rapidly" at about $350. Points out that you would think that General Instruments, maker of the VC2, would have taken steps to prevent the VC from being broken, but apparently not (though G/I has begun electronic countermeasures not mentioned in this part of tape).



CRUDE OUTLINE OF VIDEOCIPHER II BOARD SHOWING EPOXY-PROTECTED REGION

Describes VC board. Blue-label board, the 018 series, supposedly unbreakable, covered key chips with epoxy resin, narrator claims that epoxy puts heat load on VC and hastens battery failure, which results in "brain death" of the board. U30 is location to plug in "magic chips" which tell other chips to do things they were not intended to do. If you remove the VC board from socket while unit is plugged in to AC outlet, you'll destroy it.

Looks at Testron's PROTEC test device, latest 018 model, plugs into U30 socket, allegedly used by dealers/repair techs to see if the rest of the VideoCipher is capable of descrambling all services. Says that Testron has incorporated circuits that prevent its own chip from being cloned (cloning was one method used to defeat the VideoCipher early on; G/I transmitted data that turned off many cloned units). Has socket that you can plug the original U30 into and a switch to toggle back and forth between the original and the test device. Tested on 3/29/88. Its set-up menu: installation, unit setting, rating ceiling, rating password. This device will work as long as the first two digits of the third byte are "FF" [in hex notation]. Narrator took it through all channels on Galaxy One, even and odd, and other satellites. It descrambled all but possibly one signal, sometimes took a second or two to "lock on" and begin descrambling.

[next segment: music from The Addams Family precedes...]
Lee Hadlock discussing "The Wizard Technology." Also refers to it as "Load Star Technology," an improved version of the original "Keys-R-Us." Load Star available in versions 2.4, 2.6, 3.0. Lee refers to the product as a "diagnostic repair tool." Setup screen considerably more complex than that for the Testron device. Displays inner workings of selected chips and registers, will show seed keys in 010 but not 018 series, allows user to modify and view what is in RAM, view data as it comes in over the signal, lets you look at "command data," Lee invites viewers to write him and he'll explain command data. User can look at register areas in U19, which makes for "a great diagnostic tool." User can write to U19, U20. Can clear U20 key area and reset U20. He says that G/I has installed a routine in U7 that zeros the working key if it detects any "slight enhancements." This makes a string of zeros a valid working key. Would not have worked had they chosen a random number. More complex, provides more information than the Testron device, more useful to hackers. At end, Hadlock advises viewers in the U.S. not to buy his product. Says other vendors are claiming to have Wizard Technology but hints that it's only a clone of the real thing. He sells a proprietary socket that solders via strip onto the back of the board and gives you a socket to plug in the Loadstar chip. Suggests that the 010 series had no epoxy, the 018 does. Offers repair services, will buy "dead" VC boards for parts for $150 each to repair other boards. Lee Hadlock, Inc., 528 First Ave, Bellmawr, NJ, 08031; 609 931 0655. Was taped in AR. He appears on Boresight News on satellite TV. Wizard requires that you enter codes every 60 days or so.

[next segment, new narrator]
The Doomsday chip is called the "Secure One," By United VC Technologies, Inc., 1-205-262-0480, again warning that it may be illegal in U.S. Refers to itself as the state of the art in a running key or working key system. Was developed as a cloning device first, "...and a running key or working key system as a backup feature. You may wish to use it differently." "Cloning is the least bothersome of any VC2-defeating system; however, recently G/I has defeated many clones with an ECM method whereby when a clone is watching an unauthorized program, bad information bits are sent to the box, rendering the box with no audio. The Secure One will not accept this bad information." Talks about the "Keyboard Wizard." Says it's a very safe method of turning on a VC2. It must be updated every 30 to 90 days. This means you must stay in contact with every VC [using this technology]. Uses some type of search. Takes several seconds up to a minute to find the right data to lock on and descramble. This also considerably more complex than the Testron device. $1250 complete. Needs a seed key. They will "archive" a seed key for $250.

[music from The Wild, Wild West precedes segment showing tools of the trade, hardware, replacement battery]

[brief segment discusses software/diskettes]
Average chip file 16K, use if you have an EPROM burner. Diskettes containing files for EPROMS sell from $89-$2000 depending on what files they contain and how modern they are. Outdated technology that once defeated the VC is often thrown in as a freebie (hardly surprising, since it is now obsolete).

[next segment: "V. C. Hacker" demonstrates EPROM-burning, narrator finds this boring.]

[next segment: plug for the Blank Box Newsletter.]
Says they provide a monthly list of services not to buy from, not seen in our sample from 1987. Describes Scramble Facts as "quite controversial," apparently has panned some products, angered their manufacturers. Boresight News, Thursday nights Westar 5, transponder 1, 8 o'clock central, Sunday night 9 PM. Will give $5 off next videotape if you buy one now.

[next segment: Steve Kline]
His creation, the Parasite Box, a stand-alone VideoCipher competitor. Kline was raided by FBI, he claims illegally so. Now in court battle, has given his technology to parties outside the U.S., trying to market it legally in the U.S. Claims his box is more secure than G/I's, but admits that "where there's a will there's a way" re: magic chips and his box. "Zombie," his firm's name, means that he is trying to bring the satellite industry back to life. Parasite Box has U.S. and Canadian flags on it. Kline also makes a "battery replacement tool" that can extract key from 018 units, archive the key, makes static dump from U20, put everything back into U7, put the box back into "original" condition. Could it be used as a cloning device? U7 upper left epoxy part of board. To extract key, put clip on U30; to put it back, put clip on U7. Numerous other single clips, message on screen says it's a battery replacement tool not intended for illegal use. Around $1200.

As this leaves for the printer, The Pirate Video IV has just been released, same price, same discount for mentioning Scramble Facts.

* * *

JAMMING POLICE RADAR

—is highly illegal. In fact, some states have outlawed receivers that detect police radar. Jamming the blessed units might obstruct justice, and since jamming requires transmission on police radar frequencies, something for which you probably lack an FCC license, you could pay a fine for broadcasting without said license. We do not recommend that the reader do anything illegal.

That said, note that it is possible to jam police radar. One source refers to this having been done, at least as far as anyone knows, in 1961. But in those fine days, on open highways with a sane legal speed limit and an unofficially legal one about 10 mph faster, along with cars that sported the correct amount of horsepower, who cared?

The 55 mph era changed that. We had just gotten used to cruising at 70, when the oil crisis forced us to downshift to second and lug along at 55. Radar remained the primary tool of enforcement.

In comically plain terms, radar works by bouncing microwave signals off radioreflective objects, such as cars or non-stealth aircraft, and processing the echo to read a speed relative to the radar unit. We can see intuitively that this presents less of an engineering headache for fixed units rather than those on the move, but even that feat has been done, as those who've been ticketed by roving state troopers will testify.

Radar-detector advertising has educated the public to the existence of formerly two, now three, distinct radar frequencies. The so-called X-band, the first to see service with police units, operates on a frequency of 10.525 Gigahertz (GHz; billions of cycles per second; called microwaves out of the fact that wavelength measures a few centimeters down to a few millimeters). Coincidentally, or maybe out of some sick, sadistic delight savored by nameless mutants deep within the FCC's RF-shielded underground bunkers, automatic door-openers and microwave burglar alarms function on the X-band, too. This subjects your dashboard radar detector to false alarms from those sources.

At 24.150 GHz we have the dread K-band, seen with "instant-on" radar, so-named since it emits no

electronic peep to betray itself until it has clocked you (at least if your reflexes weren't sharp enough to react instantly).

The latest round of move/countermove in the highway speed wars involves a setup that has, thus far, seen limited application but widespread publicity at the hands of least one radar-detector-maker looking to play on a cold and ugly Fear engendered by the new band. They hint that driving without a detector sensitive to this third Ka-band (around 34 GHz) is equal to driving blind. The new units don't clock your vehicle until it is so close that a photo, clearly showing driver, front-seat passengers, and front license tag, are visible. No pursuit-cops need pull you over. You receive a speeding ticket in the mail, with evidence irrefutable up to now that your vehicle was traveling X number of miles per hour above the speed limit on Y date at Z location, driven either by your own lovable puss shown in the photo, or...goddamnit, Wendy! What do you mean speeding in my pickup truck! And who's that hairy creep in the front seat with you!!

Yes, this little revenue-maker has been good for a few laughs and possibly a number of family spats, as well as an uneasy dread on the part of high-mileage drivers who depend on radar detectors. Those drivers traversing some parts of the country rightly feel that they will have to upgrade to Ka-sensitive gear.

While we're on the subject of frequencies, note that police so inclined can detune their speed guns so they'll still clock you, but won't trigger your radar detector. This is illegal, and if shown to be operating off-frequency, would negate any evidence from that particular speed gun: "Yes, officer; but when was the last time your supervisor documented that this unit was in fact transmitting dead-on-center of the K-band?"

SON OF SON OF FALSE ALARMS

If microwave sensors have proven themselves second only to ultrasonics as sources of false burglar alarms, it comes by no surprise that police speed radar is subject to false readings out of a horde of vile scenarios.

First, as extremely high-tech gear, radar speed units get out of whack easily. Most patrol units require their speed guns to be calibrated at the beginning and end of each tour, and on and ad-lib basis if the setup is in any way unusual or likely to subject the unit to more false readings than normal. In this document-everything era, a written record of valid calibration generally means you are guilty, while lack of same could let you beat a bad rap. Ask, politely, to see these records when you are charged with speeding, and to have the radar unit calibrated on the spot to see if it was within proper operating limits when it tagged you.

Second, radar speed guns work well only in trained hands. Those nationally publicized trees clocked at 85 mph in Florida had to pay the fine for speeding, not due to some evil jinn in the unit, but out of uninformed use of police radar.

Third, any number of poorly shielded electrical devices inside or outside a patrol cruiser can bollix a radar speed gun. Examples include rotating metal fan blades (e.g., the blower for the cruiser's air conditioner), radio transmitters, plasma-discharge lighting (streetlamps), and so on.

Fourth, accuracy of radar speed measurements falls off as the angle between unit and target vehicle departs from 0 degrees. The most accurate measurements come from units placed directly behind or in front of the target vehicle. A roving unit shooting you from across the median is likely to read a slower speed than your vehicle is actually doing—but look deeper into the false-reading trap. Your econobox presents a fairly small radar signature, nothing next to the semi half a mile behind you that's doing 85 mph. Some of the trooper's radar signal will strike your car, but some will miss it and hit the metal guard rail at the edge of the road. Under just the right conditions of angle and speed, the signal will ricochet off the guard rail, then bounce off the huge metallic front of the speeding semi, come back up off the guard rail and into the speed gun. Given a choice between signals, the speed gun will accept the stronger one bounced off the semi. Result: "you" were clocked at 85 mph. Now, since the gun is likely to err in your favor at that angle, buddy, you must have been doing 90. Time for a trip to the station....

Fifth, note a similar hazard when being clocked from behind by a moving unit, with a vehicle in the passing lane and far ahead, whose radar signature is much larger than your car's. Patrol car doing 55, your car doing 55, third big car doing 70. Result: "you" are clocked at 70. No trip to the station on this one, at least if you can post bond in cash on the spot.

There are others, less frequent, but they still happen. For instance, moving radar uses the radar to clock both the target vehicle and the trooper's car, so that an accurate reading of the target is obtained. Certain conditions give the unit false information about the trooper's speed that make it seem that your car is moving too fast.

JAMMING

Most laymen understand that military radar is subject to jamming. Many methods work, and new ones, countermeasures, and counter-countermeasures appear yearly. Laymen understand also that military hardware-costs begin at hundreds of thousands of tax dollars and ascend like a soul that just bought a Stairway to Heaven.... But few laymen gave serious thought to jamming police radar until it became a fait accompli, and one within the budgets of those who drive the kind of cars that feel at ease slashing the blacktop at a hundred and ten.

The first step in the jamming process has to be detection: You must be aware that your vehicle is being clocked before recklessly spraying microwaves into the atmosphere (and triggering every radar detector within a vast radius). Radar detectors of high quality have been available for years, and, without endorsing or panning any brand(s), Cincinnati Microwave's Escort[tm] and Passport[tm] led the pack in most magazine-sponsored tests.

Understand that Escort's existence eliminated most of the R&D cost of a serious police radar jammer. It handed jammers their front end on a plate.

Now, there existed also devices whose function was to calibrate police radar units by beaming signals that simulated microwaves reflected from cars traveling at selectable speeds, in the range of, say, 35 to 70 mph. Of necessity, these units transmitted on the X and K radar bands.

Question: What if a radar detector were wired to one of these test transmitters such that, when it sensed itself under attack, it would immediately activate a calibration transmitter to beam signals that misled the receiver by telling it that the vehicle was traveling at some speed selected by the user? Or, as an alternative, flood the area with microwaves so powerful as to blank out the police unit?

The answer, at least in sparsely reported tests, is that it would work, most of the time. The setup as currently marketed by Remote Systems[tm] (Burnsville, MN, 55337; 1-612-894-1309) consists of a Cincinnati Microwave Escort or Passport fitted with an output jack that interfaces with a control unit that Remote Systems sells as plans, kit, or fully assembled. Note that this configuration will do nothing further without X- and K-band transmitters (units known as Gunn oscillators) to beam out the false signals, but Remote Systems tells you were to get them and how to wire them together into a working jammer. (Gunn oscillators are available from: Advanced Receiver Research, Box 1242, Burlington, CT, 06013; phone 1-203-584-0776.)

When using any radar detector, typical behavior by the driver calls for quick deceleration when the unit signals police radar in the area. Depending on model and conditions, that can be miles from the source. Not so, of course, with instant-on radar; yet few drivers seem to know that it takes anywhere from 0.5 to 3 seconds for a radar unit to give the trooper a "reading" on them, or that a car can slow out of the danger zone in that time, due to the driver's cat-like reflexes and natural feel for the brake pedal; and that a vehicle whose speed is changing may give an unreliable reading. (Of course, you do not hit the skids with a semi thirty feet off your tail....)

Driving with a functional jammer should not change this response pattern, i.e., do not blast past the mountie at a hundred mph with the unit set to tell him you were doing 35. He will impound you and your car, then have the lab boys go over it and dig up that justice-obstructive jamming device....

....which ain't likely to be hard to find. The X- and K-band transmitters often look like black fog lamps mounted on the front bumper. To someone who knows what they're seeking, they are easily spotted. Genuinely slick setups hide the Gunn oscillators in cutouts in the front bumper, covered with radar-transparent black rubber.

Some drivers refrain from hitting the brakes even when that instant-on warning buzzer yelps, because they know their brake-lights will tell the world that they are slowing. But what if, instead of a jammer, the sensor unit connected to a relay that cut power to the brake-lights during a crisis? Wouldn't we all feel easier about a quick, sharp stomp on the skids? Remote Systems sells that little goodie, too, along with a circuit to mute your BlastMaster stereo system so you can hear the detector's meek beep over Lynyrd Skynyrd's "Free Bird," a merciless song conducive to savage spirit and a leaden foot....

STEALTH?

One source on police radar reported that older Corvettes, those with fiberglas bodies and a radiator angled back so as to deflect RF signals upward, are "invisible" to police radar at distances greater than about 450 feet. Hmmm. Strip off the chrome and clock it again....

Before leaving this rude topic let's be straight on one issue. Eclipsing the speed limit to the point of endangering innocents is culpable on its face, what Gordon Liddy would call "malum in se," a thing bad of itself. On the other hand, the American consensus has it that the 55 mph speed limit no longer serves a purpose, and we have it on some authority that many a grubby solon, from city hall to the state legislature, views police radar as a tool of revenue rather than the balm of public safety.

Not only does jamming spark us in a technological sense, but it appeals the bad boys in us all. A proper fix would reinstate the nationwide 70 mph interstate speed limit, which means that 75 and 80 are OK most of the time, seat belts and airbags a must. We could handle that.

* * *

FREE SOFTWARE?

In addition to securing your data from prying eyes, what a bummer that you must scan for software that intentionally destroys it. Computer users who own modems usually tap into one or more electronic bulletin boards where they can chat much like ham radio operators do, only via VDT. Bulletin boards let computer programs be copied to themselves, or "uploaded," as well as copied from the board to individual systems, or "downloaded." These programs are, by and large, the work of amateur but often talented programmers who wish to share handy if minor-league utilities with other users.

Many users found that programs they downloaded didn't perform as expected. In fact, some programs trashed hard disks or valuable floppies on a pure evil rampage. Since no one would knowingly use such programs, their true nature had to be hidden in machine or assembly language, and called something like "Computer Helper," a fictitious name used here only for illustration.

The unsuspecting victim would download the program, run it, see a screen-prompt that it was "installing" itself—only to be greeted by a message such as "YOUR HARD DRIVE HAS JUST BEEN REFORMATTED, DUMMY!" when the foul demon was done.

That dark breed of program came to be called Trojan Horse, since it hid mayhem in an appealing package. Often, the text message could be seen by examining the contents of the program with a utility designed for that purpose; or all but ASCII text characters could be stripped out, revealing the kicker before running the program.

VIRUSES

A Trojan Horse would trash or vex only a single disk or system unless manually copied and passed on. But a second form of destructo program took control of the computer to automatically create copies of itself on all hard or floppy disks it found free of its own code. Since an infectious organism that replicates by taking control of a cell is known as a virus, that tag seemed apropos of this new breed of electronic pestilence.

Viruses have emerged as the hot topic in computerdom as this goes to press. Though the concern contains

elements of hysteria and hype, the threat of viral programs has proven real. What can they do? For starters, they can mutilate or erase data.

Records that once lived only on paper have nearly completed their migration to electronic storage media. Most of these belong to the government and large private concerns that must process mountainous chunks of data. But with the spread of personal computers and minicomputers—bigger than a personal computer but smaller than a mainframe—with their natural affinity for data storage, the impact of unanticipated and willful destruction of all data accessible to the virus cannot be downplayed. The sloppy novelist who fails to back up his files after each writing session could find more than a year's work banished to the Phantom Zone. Time magazine told of one writer who had several months' worth of notes erased by the Pakistani virus, "Brain." An insurance company or bank could see its financial records scrambled into useless characters. The ability to destroy data is quite enough.... (The lesson Time all but ignored teaches to keep multiple copies of important data, updated each time the data changes.)

A second uneasy property of viruses lies in their latency. They do not attack immediately; rather, they key on input of a certain word, arrival of a certain date, a specific instruction, or some other condition set by the viral programmer. (And here the analogy to infectious agents holds up. Cold sores are caused by Herpesviruses. The infection usually takes place during childhood, but the virus remains in the individual's cells for life, dormant until triggered by fever.)

The self-replicating property of viruses has led to "infection" of hundreds of thousands of diskettes. Most computer-users, from corporate research labs to video game buffs, exchange information by physical transfer of diskettes and by electronic hookup via modem. An infected diskette will copy its virus to whatever media the hidden program finds accessible in a new computer. Those who download software from bulletin boards have no way to know whether it's infected. They may not know until their data is dust. Hackers who deal with potentially infected code often use a separate, floppies-only computer to handle suspect software.

These bugs may prove to be the final solution to software piracy, out of dangers inherent in accepting or buying diskettes from unsecured sources. You don't know where they've been, whether they might harbor a virus along with the pirate copy of Paradox[tm], or whatever. It just isn't worth the risk anymore, getting copies of expensive software on the sly. (And at least one major software vendor unkowingly sold copies of its program infected with a benign virus that erased itself after flashing its stuff.)

Money is being made selling anti-viral programs, whose names match the metaphor: Viralarm, Virus RX, Disk Defender, Vaccinate, Data Physician, etc. (All registered trademarks are hereby recognized.)

Who creates viruses, and why? Both professional and amateur programmers. Disgruntled employees of computer firms are suspected in several cases of virus attacks; and the Pakistani "Brain" virus featured in Time was the work of self-taught programmers driven, they said, by a desire to punish software pirates. Their work drew praise for its elegance and curses for its plunder. Viruses smack of the hacker mentality, an offshoot of human nature, a force that motivates us to do what hasn't been done, or is claimed to be impossible.

Some viruses have been directed at specific targets: IRS, FBI, and CIA computers reportedly came under attack, as did those of the large computer consulting firm, EDS. Many university computers have suffered viral assaults, hardly surprising, given the campus nerd population.

John Williams' firm, Consumertronics, is now selling what they advertise as the unaltered Pakistani "Brain" virus, along with programming analysis and an "antidote," for $50. Literature insists that buyers give Consumertronics a signed statement that they will not use the virus destructively, will make no copies other than backups, will not transfer the virus to another system, and will not modify the program so as to make it more virulent.

Big-leaguers have taken steps to safeguard their computers and products, but the average user must now be alert. Sound advice says not to use software obtained from iffy sources, particularly pirated copies of programs, and never let anyone have access to your computer (that keyboard-locking switch which everyone leaves "on" may have found a use). As always, keep multiple backups of all data and repeat the backups regularly—like after every filing session.

* * *

BE CAREFUL WHOM YOU CALL

—because date, time, duration, and both numbers become immortal data that remains on-line forever. The phone company had the ability to record this information as early as the fifties. It installed the equipment in the sixties, according to one source, but denied its existence to the government, which wanted to tap into the resource to gather evidence on organized-crime bosses. Any company that says No to Uncle has got to have the flush to back it up against Uncle's favorite means of harassment, a permanent state of IRS auditure.

Look over your telephone bill, the one that lists all numbers with dates and times. Machines make child's play out of matching names with those numbers. Is one company a purveyor of information about jamming police radar detectors? Is one an, ah, escort service? What will the opposing counsel insinuate from your having called them? (The opposing counsel keeps on a leash a private investigator who has "contacts" in the phone company. If the opposing counsel is the DA, his investigators are the police, and the likelihood of a mole in the phone company quadruples.)

Dialing some numbers may trigger automatic monitoring, place your name on a mail-intercept list, say, if you accidentally dial the NORAD mainframe, or if your computer committed the same blunder.

If James Bamford's estimate of the design and prowess of the NSA is to be believed, they have the ability to monitor all telephone communications in this country. Furthermore, they can detect a certain voiceprint and have it taped automatically, even screened for words and phrases, and very soon, automatically transcribed and edited, and translated into English or some other tongue.

Remember that the phone company, in whatever now-disbanded guise, has the power to monitor all calls, even local ones, as to time, number calling, number called, time spent on the line. They do not have to list this on your monthly statement, but in a civil or criminal action they can pull it and show that somebody called these numbers. It goes for pay phones, too. The old axiom that you cannot be too careful was never more apropos now that universal surveillance has become interwoven with the cloth of our society.

A NON-DIGITAL VOICE-SCRAMBLER

Both completed commercial units and schematics for do-it-yourselfers exist. This details a device featured in the January, 1988 issue of Radio-Electronics magazine, which kindly granted permission to reprint the schematic and PC board template. The advanced hobbyist can decipher component layout from the schematic. Others would do well to order the quoted issue from Gernsback Publications (see Chapter 9). The photo shows the author's nearly completed model. He bought the board from WaveLink Laboratories (Box 199, Trumbull, CT, 06611; $11), highly recommended, but better write to see whether it's still available.

The 555 timer chip here is the new MOS version which drinks far less power than its bipolar predecessor. The other chips are standard logic devices and a dual op amp, along with the common LM386 audio amp IC, all available at Radio Shack. Use proper care in handling static-sensitive chips.

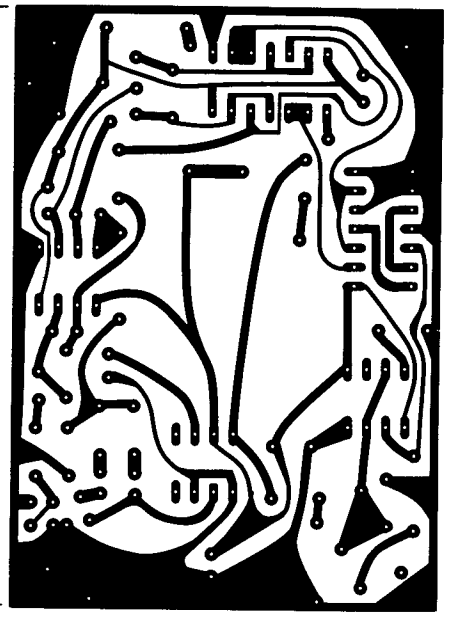
This device chops, splits, and folds the audio input; reverses those functions when descrambling. You must build a pair for simultaneous operations. The 50K pot is a 20-turn device that tunes it, and allows variation in signal over a wide range.

Determined foes will descramble this breed of signal with ease. If you plan to face no determined foes, the device offers acceptable security.

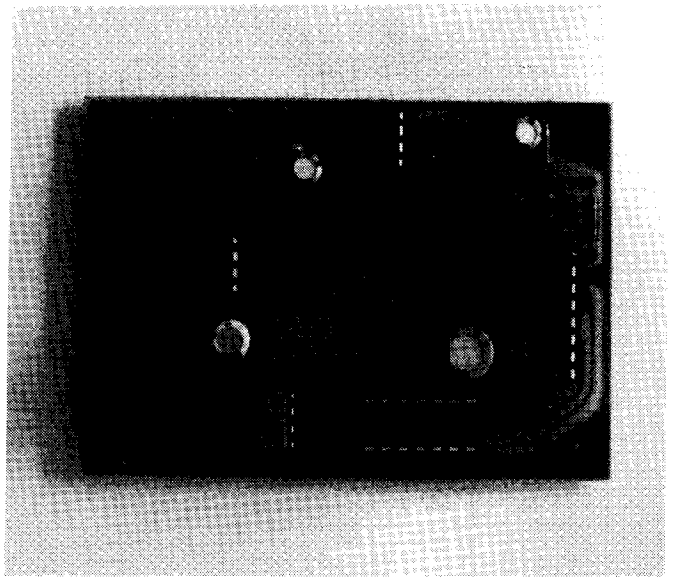
MAILING LISTS

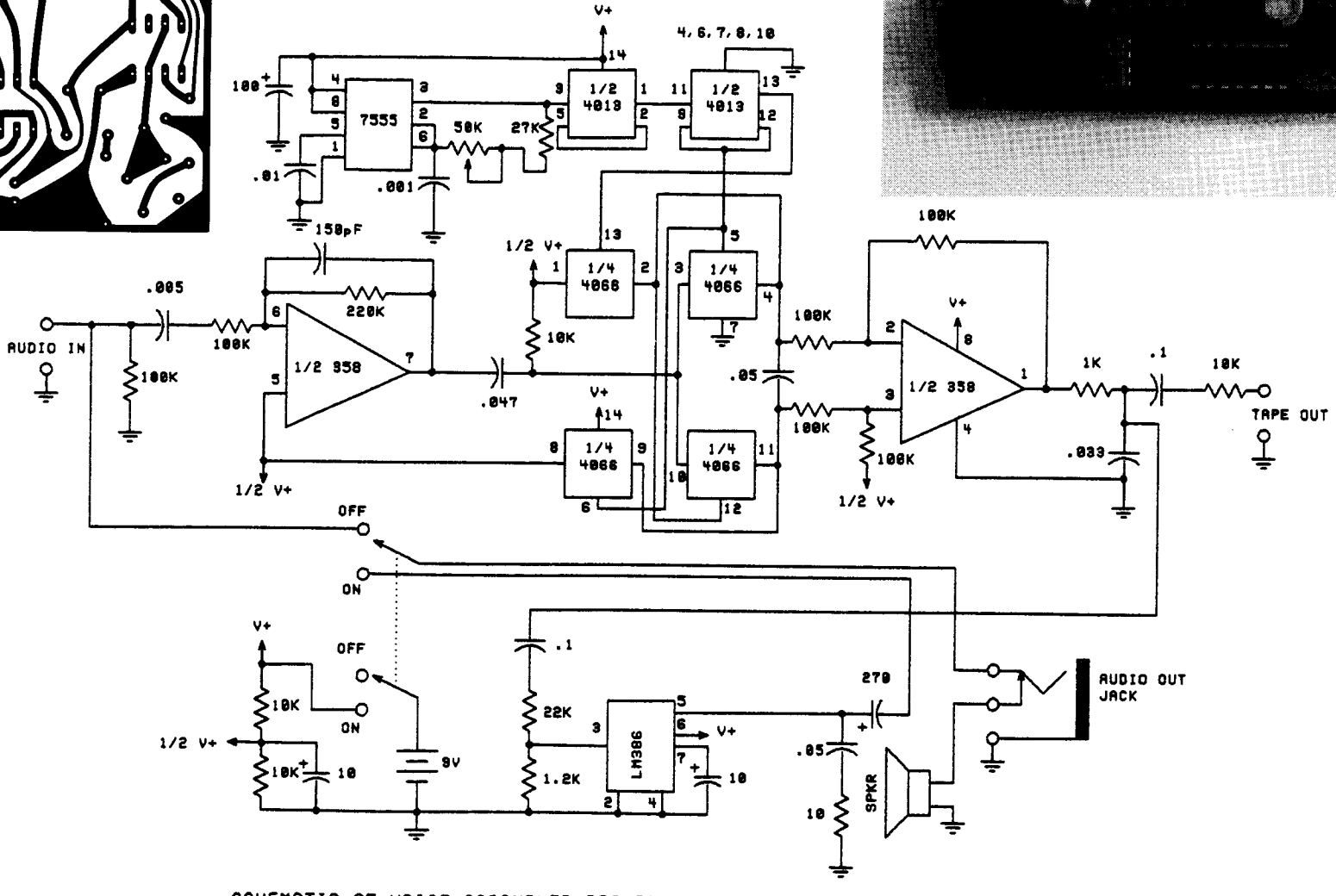
What are these mailing lists everyone talks about? Who keeps them, sells them, uses them?

Many companies. Consult Literary Marketplace to find them. Most public libraries keep a copy in the reference room. Get names and addresses, write for their listing. Some companies specialize in subpopulations, such as lawyers, doctors, or accountants. Others boast that all the customer need do is supply the



LEFT: life-size PC board template for voice scrambler; Copyright (c) 1988 Gernsback Publications, Inc. Reprinted with permission. RIGHT: underexposed photo of author's nearly completed project.





SCHEMATIC OF VOICE SCRAMBLER PRINTED IN THE JANUARY, 1988 ISSUE OF "RADIO-ELECTRONICS" MAGAZINE. COPYRIGHT (C) 1988 GERNSBACK PUBLICATIONS, INC. REPRINTED WITH PERMISSION. ALL CAPS IN uF EXCEPT 150 PICO CAP AT 358.

criteria and they will compile the list: age, magazine subscriptions, income, zip code, credit cards, and so forth.

Lists derive from pooled, organized information known as databases. Many contain tens of millions of names and addresses. As a key point, people can be selected or sorted according to age, type of credit card, type of hobby gear they have purchased, whether they have bought smut by mail; marital status, religious affiliation, political registration, criminal history, and so on. (The government's database includes also the subject's IRS files, fingerprints, voiceprint, retinal scan, and very soon, personal DNA code....)

It takes no imagination to see that a party serious about tracking down a missing person could easily give your name, along with specified variations or aliases, income, occupation, magazine subscriptions, hobbies, political bent, and so on to a mailing-list vendor, and have a fair chance of coming up with your new address. More, the programmer could specify near-meeting the standards within a set range, to catch you if you were to modify only some of your traits.

How to combat this? You must alter EVERYTHING about yourself. Stop all prior magazine subscriptions, drop credit cards, give up uncommon hobbies, and so on. You might even throw in red herrings, such as subscriptions to Good Housekeeping mailed to a female name at your address. This way you avoid creating a telltale profile.

SECURING PERSONAL COMPUTER DATA

That same paper-to-electronic storage migration that took place within government and business is picking up steam in the private sector. A 60 megabyte hard disk impresses no one these days—and there is no point to having all that storage if you don't use it. Go ahead and use it—but anticipate: What could the authorities or a private enemy learn by confiscating your computer with the megabytes of data it hides?

Plenty. Growing numbers of Americans keep bank, tax, business and other sensitive records on these disks, along with dandy programs for handling it. The IRS, for instance, loves to pore over these files.

What about poison pen letters you used your word processor to create? Erasure makes no difference. The files still exist. Only the file allocation table, or FAT, changes with an erasure. The sectors of data remain until other data overwrites them. At least a dozen commercial and public domain programs will examine disks sector by sector. Some will automatically recover erased files. Great for you in the case of an accidental erasure, bad if your hard disk gets impounded.

Reasonable level of security can be had by encoding your files, then copying them onto a diskette that you first bulk-erased then formatted anew (formatting does not destroy data in the sectors, only rewrites the FAT). A trick beyond that would go into the touchy file with DEBUG.COM or one of the countless utilities having similar powers, then modify the first three or four bytes so that the decode program does not recognize them (encryption programs often tag the files with part of the manufacturer's name, so the decode program can recognize it; remove this information). Of course, you must remember what changes you made, or the file becomes useless.

One method of added security for files subject to casual attack by duffers converts them to "hidden" files. Several utilities on the market, some of them public domain, let you make this simple change. DOS will not display hidden files to a DIR command, though CHKDSK will list the number of hidden files. The computer-savvy snooper would pick up instantly on the fact there are too many hidden files—the operating system usually creates two; copy-protected software may add others—and go after them first.

The agencies who would get at your files are aware of most encryption software. That software usually alters the output file in a way that makes it recognizable to the decoding program. All the codebreaker has to do is look into the file for the proper tipoff as to what program was used, then set up his Cray to try all possible combinations of keys to decode. To take one example, a utility called LOCK.EXE, included by Softlogic Solutions with its excellent Disk Optimizer program, has a keyspace of 8 characters. Knowing what program it was dealing with, it would take the Cray a few minutes to go through all possible combinations of 8 ASCII characters and open your files.

Patterns lead to uneasy inferences of the lore of encryption. Taken back to the 1960s, we read authoritative material boasting that the current algorithm is uncrackable in any "practical" sense. Trouble is, the exponential rise in computer power and intelligence redefines "practical" every three years. One merchandiser of encryption equipment for business boasts that the output of its program withstood attack by a Cray supercomputer for 22 days. And the private sector does not have access to whatever goodies the NSA has cooked up in its avowed intent to stay at least 5 years ahead of the state of the art.

As this goes to press at least three private-sector encryption programs hold themselves out as secure. Their vendors feel strongly enough about it that they have posted dollar rewards ($1000 is the largest sum we have seen) for those who crack their codes. This may convey a false sense of security. First, rewards offered to date would not of themselves provoke a serious attack by our top cryptographers, or even by the third string, nor would they satisfy the cost of using genuinely powerful computers for the attack. Second, as commercially available software, anyone looking to crack the ciphertext would use the huge lever of seeing how the program encrypted it. We must assume that the cryptographer would get his hands on coded text also, as well as a sample of plaintext. Those three elements simplify decoding enormously. Finally, we, the potential users, will never know what degree of security we have entrusted potentially vital secrets to. NSA isn't apt to advertise those encryption schemes it has defeated.

DES AND THE NSA

The National Security Agency might or might not exist, depending upon whom you ask. The Presidential memorandum that created it cannot be accessed, even under the Freedom of Information Act, to this day.

The NSA has so far insisted upon maintaining the ability to reach any information about anyone, anywhere. In fact, one of many problems that face those who make decisions at the NSA has been what to do with serendipitously detained data that proves criminal conduct on the part of elected officials and enforcement agents. NSA's information-gathering power has grown so fearsome that they literally do not know what to do with much of the news. They do not discard it. It sleeps entombed on magnetic tape hidden deep in climate-controlled caverns, patiently awaiting an opportune time to rise like the Phoenix. Census data is supposedly secure for something like 72 years; but don't let that claim fool you. The NSA knows a few tricks about accessing verboten data.

Our National Bureau of Standards promulgated a now-widely-used encryption system known as the Digital Encryption Standard, or DES. Tacit in the fact that this supposedly sophisticated system was disgorged is that NSA had satisfied itself that it could crack codes based on DES. In fact, sources indicate that DES encryption is considered secure only for unclassified data. The NSA takes executive action whenever it senses that genuinely secure technology is about to be marketed.

Let's admit to a bit of ambivalence about this all-powerful (second only to the IRS) agency. We do not mind seeing its incredible power turned against our enemies. Case in point: the fatal odyssey of Flight 007. We played back transmissions of Russian fighter pilots with chilling clarity for the United Nations and the world. The NSA had done the listening. It has pretty good ears, out there north of Japan.

CRYPT

One example of privately written and distributed encryption algorithms is called Crypt, by M. J. Maniscalco (PO Box 11235, Cleveland, OH, 44111). As this goes to press, one version of Crypt is available on public computer bulletin boards, while a more sophisticated version will soon be available on diskette from Mr. Maniscalco for $20. Write him for current information. The story of Crypt illustrates important aspects of the encryption/decryption game.

First, a few terms:

plaintext—message prior to encryption
ciphertext—message after encryption
algorithm—mathematical process that accomplishes encryption and decryption
key—character string used by algorithm to encrypt plaintext and decrypt ciphertext
keyspace—the number of characters the algorithm actually uses; generally, the larger the keyspace, the more secure the algorithm

apparent & functional keyspace—the algorithm may modify a key of, say, 32 characters prior to use such that it becomes effectively a key of only 8 spaces; 32 is the apparent keyspace, 8 is the functional keyspace; smaller keyspace detracts from security of the algorithm
substitution cipher—algorithm that substitutes one character for another as determined by the key
transposition cipher—algorithm that changes the sequence of the characters in the plaintext, again, according to the key
product cipher—algorithm that invokes both transposition and substitution; many times more secure than either transposition or substitution alone

Substitution ciphers are notoriously weak, since the serious foe will eventually get his hands on plaintext, as well as a wealth of intercepted ciphertext. Plaintext allows working backward in a mathematical sense to get the key and the algorithm. Pathetically insecure.

Transposition ciphers jumble the message, but since all characters remain, piecing them together through ultrafast computer trial and error poses no hitch.

Seriously secure codes begin to arise when we use the product cipher, a combination of transposition and substitution. But even the product cipher falls to mechanized attack due to weaknesses inherent in some schemes. For instance, a small effective keyspace lets the old Cray try all possible keys in a brief time. Demands on computer time rise exponentially with increasing effective keyspace, though statistical methods reduce the number of avenues to pursue, simply because both easily remembered keys and decrypted messages tend to consist of limited numbers of words arranged to make sense. The DES keyspace gives 10 to the 17th power possible combinations. This doesn't faze the NSA, one reason it let the algorithm become "standard."

An algorithm that repeatedly uses even a large key tends to betray itself in a mathematical sense, and for that reason offers less security.

Taking these factors into account, note how Crypt works. First, it employs a product cipher, one of the hardest to crack. Second, it uses a large functional key: up to 64 ASCII characters in any combination. Alteration of even one character will change the ciphertext completely, i.e., the algorithm takes no shortcuts to speed calculations. Sixty-four characters translates into an effective keyspace of 10 to the 127th power, 110 orders of magnitude greater than DES. This would give the NSA computers a headache, even with shortcuts allowed by artificial intelligence programs and statistical analysis. Furthermore, the margin of safety appears so great that even a 10,000-fold gain in computer speed would not materially affect the security of the algorithm to a brute-force attack.

Crypt uses its 64-character key only once, but even then, does not use the key in native form. It first alters it by combination with two independent pseudorandom numbers, each of which repeats only once in 30,000,000 runs. The program uses each new incarnation of its key to process only 32 characters of plaintext, then shifts the key again—but the shift does not depend upon pseudorandom number generators. That would weaken it, since pseudorandom patterns eventually betray themselves. Rather, Crypt bases the new key for the next 32 characters, known as "autokey," on the content of the plaintext. Thus, it uses a key constantly changed by variables which the codebreaker cannot divine through backtracking to a pseudorandom number generator.

Plaintext helps in cracking the code, but even taking that into account, a conservative estimate based upon all assumed advantages to the codebreaker, including computers so fast they do not, as far as anyone knows, yet exist, it would take approximately 10 to the 25th power years to run an exhaustive search of keys.

Crypt as supplied on diskette comes as an executable file, as well as source code written in C language. Those with a serious grasp of programming can shorten or lengthen the keyspace and alter the random number generators, leading to a unique algorithm. Calculation time rises exponentially with growing keyspace. Execution times for Crypt on the author's "clone" running an 8088 at 8 MHz were barely tolerable. Doubtless, these times would shrink on 80286- or 80386-based machines, especially if Crypt could invoke a math coprocessor.

The version of Crypt current as this goes to press will handle only ASCII text files. Utilities and improvements in version 3.0 to be released soon may remedy this.

Shortly before press time, Mr. Maniscalco informed us that U.S. Law forbade shipment of data encryption software to countries outside the U.S. except Canada, and that he could not fill orders received from any other country. Presumably, this restriction holds for all encryption software unless Uncle has approved it for export.

Safe rules to live by hold that ordinary data—material in which no one has a particular interest—can be secured using off-the-shelf encryption software, transmitted via coded phones, and so forth. Do not assume anything to be safe from big-leaguers, private or governmental. If they cannot break your algorithm and its 128-bit key, they have the resources to bug your apartment, learn the distinctive audio/RF signature of every key on your board, and get the key that way; steal the program; have you "accidentally" meet the love of your life, who will gain your confidence and feed them information, and so on.

PREDICTIVES...AND OTHER ORDERS

Is the NSA, or some sinister private corporation, running a predictive on you? And what in God's name is a predictive?

To explain it, use chess computers, the dedicated board games, as a point of comparison. These feisty machines have evolved to a state of prowess that commercial units selling for less than $200 can beat 98 percent of the world's chessplayers at tournament level, i.e., both computer and player have 2.5 hours to make their first 40 moves—and, like a human player, the computer "thinks" on its opponent's time.

The machine chooses moves by analyzing the position, an ability now crude but improving, and by evaluating all possible moves, something known as a full-width search. In that way it first examines all moves open to itself, then assigns a desirability rating to the position reached by each move. Then it proceeds to analyze all replies to its best move, followed by all possible counter-replies, and so forth. Each full-width move-search is known as a ply, and two plys constitute one move (i.e., move and reply).

Special positions may send the program branching into algorithms that examine selected moves to a greater depth, or achieve specifically defined goals, such as mate in three, or doubled pawns on a file.

Machines based on the 6502 chip—as most are, out of economics and efficiency, though the 68000 series looks to be taking over—running at 4 MHz perform the first ply search in a second or less. The second ply takes a bit longer, the third may require 5 to 15 seconds, depending on complexity of the position. Fourth ply can take a minute or more, and the fifth may take several minutes. Tests on two of the author's machines —by no means state of the art—show that a 7-ply search takes well over an hour in the average midgame position. Eight plys generally take overnight in all but the simplest positions, or in cases where forced mate becomes evident.

Time-demands rise exponentially the deeper the search looks, since the number of potential variations rises sharply the deeper we peer into the game. Solid units running under tournament time rules typically search at least 5 and up to 7 ply per move. Mainframes, such as the Cray series and Bell Labs' computers, look even deeper. An 8-ply search is generally regarded as endowing the computer with candidate-master-level skill. The human chessplayer would have to look at four possible moves, in all variations, to achieve the same, though human grandmasters usually beat even the best chess computers handily because they can "see" far more than 4 moves ahead. Analysis of Bobby Fischer's games, for example, showed that he typically made moves that indicated an appreciation of the position 10 moves hence, sometimes far deeper than that. This shows the gift of genius and the ability to recall outcomes of similar positions from past games, as well as the capacity to perceive the gestalt of the position, something computers yet lack.

Board machines in the $200-$400 price range were used in the Kasparov-Karpov World Chess Championship match completed late in 1987. In seconds to minutes, the computer found moves regarded as minor tactical brilliances, actually played by the grandmasters. This does not mean the computer possesses anything near grandmaster-level skill, but that there is much to say for the full-width search, a process that overlooks no legal moves, even ones that first appear lifeless or suicidal, but which on deeper inspection prove decisive winning strokes.

Chess pieces are limited in what they can do: Knights make L-shaped moves, bishops move and capture diagonally, and so forth; and it all follows a simple set of rules.

What a shock that human behavior, though indubitably more complex than a chess game, lends itself to exactly this mode of analysis, one demanding greater sophistication, consideration of more variables, yet still one that has been reduced to a program.

This explains Big Brother's insatiable appetite for information about you. The more it knows, the more it can predict and control your behavior. And control is the ultimate goal.

The only computers capable of handling this software at more than a slug's pace belong to the National Security Agency, hidden in its secret underground silos, a curious name for computer storage sites, but one with a certain ironic aptness, since the ability to predict human behavior carries power on par with that of nuclear warheads.

This process of analyzing an individual's behavior, with an eye on foretelling his future moves, is known as running a predictive on him.

Predictives are further designated by their orders, corresponding to the chess computer's plys. A first-order predictive might eat up 12 hours on a Cray XMP, with a 70 percent likelihood that the subject will take the predicted path. After two days of thinking, the computer will give us its second-order predictive, one that ups the surety to 78 percent. Note the pattern: exponentially rising computer time, exponentially decaying incremental accuracy. That extra 8 percent cost 300 percent more time than the first 70 percent surety.

If valuable computer time rises with increasing order of predictives, so does accuracy. A fifth-order predictive, corresponding to an analysis involving uncountable variables and calculations, is rumored to show 90 percent accuracy. In human terms, that's enough to gamble for big stakes, such as the fate of the world. If the Soviets had had this capability during the Carter administration, it is likely that they would have started and won WW III. Why? Because Carter's milquetoast profile suggested that he would have "ridden out" the first strike by the Reds, then negotiated. Back then the Walker spy case had not broken, so we were at bliss thinking our nuclear subs invulnerable.

The Afghanistan affair was a simple exercise based on shrewd estimation to show that the U.S. response would amount to nothing (Reagan, not Carter, sent in the Stinger missiles that ultimately drove the Reds out). The Soviets probably considered Afghanistan an drill to sharpen up the troops for...what? Western Europe? With a fifth order predictive available to it, the Soviets could have known, rather than surmised.

To help it even more to tell what a person will do, the Agency may interview him, with or without his knowledge, and subject his physiognomy, physiologic variables, and microtremors in his voice to what is in essence a digital polygraph probe. It helps eliminate avenues of computer concern, thereby cutting down on the time spent analyzing them.

Few if any people have learned that they were the subject of predictives. The topic remains under wraps, and what sparse information has leaked has filtered through private consultants who previously worked on the project. That means the information is at least five years old....

The persons are classified, but must include top-level policy-makers, unruly members of the private sector, terrorists, and so on.

Predictives' accuracy is enhanced immeasurably by knowledge of an individual's resources, education, IQ, modus operandi, allies, family, and so forth. All this eliminates so many variables.

FUTILITY

With encryption software of Crypt's caliber available to us, we must feel that encrypted data is secure. Naturally, we will decrypt it before displaying it on our VDTs....

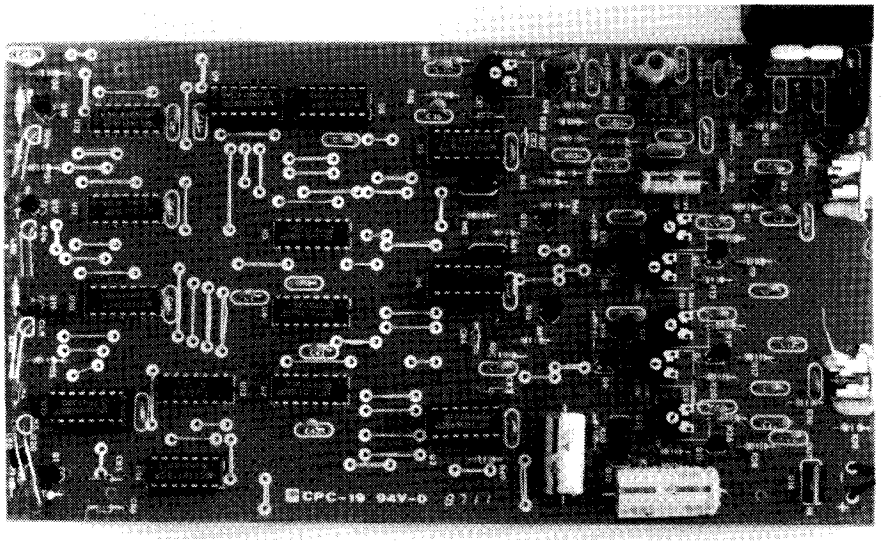
....at which time determined parties may intercept it and view it on their own monitors and store it for future review.

Television sets and computer monitors emit small amounts of RF. Confirm this with a bug sniffer. Calibrate your unit and move the probe slowly toward the screen. It will register as if you were closing on a low-power bug.

It is possible to use this low-power RF energy to reconstruct the screen image. The name which has come to be tied most closely with the practice is that of Wim van Eck, a Dutch computer expert. In keeping with the hacker vernacular, this feat is known as "Van Eck Phreaking."

If this stunt lies within reach of hackers (we tend to doubt on intuitive grounds that it lies beyond the power of the NSA), what good serves your uncrackable codes? They'll protect a stolen disk, but you must decode to deal with sensitive data on-screen.

Potential solutions involve shielding the entire computer setup, including monitor, cables, and processor, as our government has done in its secure "TEMPEST" installations; encrypting the video signal; making passwords and other sensitive data not display on screen at all; and use of monitors that emit no RF.



ABOVE: Tri-mode sync suppression descrambler, detailed in Radio-Electronics and built from kit of parts. Unit did not work on scrambled signals in author's tests, but he cannot verify that they used tri-mode sync suppression. This unit no longer exists.

6
WEAPONS

Are you talking to me?
—Travis Bickle, Taxi Driver

* * *

What use have you for slingshots, blowguns, spears, bows, boomerangs, and so forth? Well, they can be fun to play with, and with determined practice can develop into formidable weapons, at least in a relative sense. In a showdown between foes armed respectively with a slingshot and a .45 one must give the edge to the firearm: rate of fire, accuracy, raw power and general ugliness....

In this age that demands greatest economy of resources, it makes sense to analyze these questions:

1) What goals will keeping weapons meet?
2) Within reason, what weapons meet those goals most efficiently?

The law-abiding citizen finds self-defense his main objective. Hunting, target-shooting, and plinking all have legitimate places; but these have become luxuries for many. One horribly brain-damaged journalist has bragged about the rush he gets from sitting naked on his porch, blasting the countryside with hot lead from his pet .44 Magnum. As for you, best keep those stray rounds at least into the backstop at the target range....

The times force us to give urgent matters top priority. Physical security for oneself and one's family grows more imperative by the day, and thus commands more attention and resources.

Limiting it to physical means, analysis concludes that small arms give greatest return on dollars spent on hardware and effort spent in training. The guns and ammunition available to most Americans have proven the decisive if undistinguished answer to a host of problems not solved by tear gas, hand-held shockers, high-powered ultrasonic devices and all manner of exotic weapons. Those unusual tools find a place in proper context, and we will review them in turn. But let's start at the top with life and death, and work our way down into that lively but sublethal realm.

That said, we cannot escape a need few consider: study available arms and ammunition, and learn to apply them. If the opportunity presents, obtain bonded permission to carry concealed arms.

GUNS

What is there to say about guns and shooting them not already apparent from the once-trendy Miami Vice, or perhaps All My Children?

Plenty. For all the high-tech emphasis on these shows, consider this: Compared with exotic, silenced, or automatic weapons, common firearms serve equally well as to effectiveness, speed, lethality, and destructive power, when properly applied. Yet few genuinely understand their workings, the correct way to employ them, or know the laws that govern use of deadly force. Most lay assumptions about arms arise from folklore. Spooks learn the basics before they resort to spook stuff.

Small arms fall into two main categories: handguns and rifles.

HANDGUNS

Handguns may be the best known but least understood of all firearms. Their invention and evolution contain elements of utility, even dignity, as a replacement for the cavalry sword, according to some; as well as overtones of perversion, as the late-favored tool of felons.

Experts consider the pistol a defensive piece. Those anticipating trouble have time to arm themselves with whatever they choose. Most choose rifles, out of their superior power, accuracy, and range. The pistol's small size and—yes—concealability in special cases make it practical to carry an effective defense, though not a weapon that will replace the rifle.

No one can deny the pistol its repugnant if earned role as close-in assassination tool or weapon of crime. Here we speak of arms on the assumption that their use carries legitimate urgency at the time. Use of firearms does not belong to the realm of the casual.

REVOLVERS VERSUS AUTOLOADING PISTOLS

As difficult as it is to review arms without involving controversy, let's stick to functional basics before sinking into quagmires of dispute. Two types of handguns predominate: revolvers and autoloading pistols.

The revolver is a pistol whose cartridges rest in a cylinder containing usually six chambers. All who have seen a "Dirty Harry" movie know a revolver by sight. (Interestingly, until the debut of "Dirty Harry," which instantly popularized the Smith and Wesson M29 .44 Magnum, those pistols sold at no premium. After the movie series began, every macho man within hollering distance had to have one. Smith and Wesson built up a backlog of orders while gun dealers raked in cash by upping the markup on these otherwise reasonably priced arms.)

With each pull of the trigger, a revolver rotates the cylinder to center a new round behind the barrel, simultaneously cocks the hammer, and lets it fall at the end of the cycle. This is known as double-action shooting. It is possible also to cock the hammer manually, which does everything just described but fire the round, and is known as single-action shooting. It is far easier to shoot accurately using single-action than double-action shooting, though single-action is far too slow for combat in the hands of all but a rare breed that has devoted years to perfect the technique.

If one shot were all we needed, and if we had time to set ourselves before firing, the revolver might suit our use admirably. But situations often demand that we fire and reload rapidly. Here the revolver cedes many advantages to the autoloading pistol, known simply as an "automatic."

Automatics store their cartridges in a vertical column, single or double, inside the grip. A spring keeps them under upward pressure. Though diverse mechanisms or "actions" exist for autos, the basics call for the recoil produced by each shot to spit out the spent casing and load a fresh round into the chamber from the magazine. All this takes a fraction of the time to fire a revolver double-action. Assuming we can control an auto in rapid fire, it beats the revolver there.

Autos enjoy superiority in capacity, too: six rounds for service revolvers, eight and up for service autos. It takes less than a second for an expert to release the empty magazine and insert a fresh one into an

automatic. The wheelgunner must open the cylinder, eject cases, fit new rounds in, held in an ungainly contraption known as a speed-loader, then close the cylinder (loading one-at-a-time from ammo spilled from a pouch went out shortly before Jim Morrison died in a Paris bathtub). Here a revolver loses precious seconds in a complex maneuver whose mastery eats up practice time with less return than we get from an automatic.

RELIABILITY

It can be extremely dangerous to trust your life to an autoloading pistol as it comes out of the box. Many, and the .45 auto tops the list, jam frequently when new and need to be broken in by firing a few hundred rounds. Revolvers enjoy a better reputation in that regard, but lose to the big auto in other spheres.

Those who elect to use the auto should satisfy themselves that it will not jam in the crunch. Generally, if it will shoot two hundred rounds in a row without a jam, it is considered reliable enough to carry. There is also something to be said for learning to clear various types of jams....

STOPPING POWER

What is it that we ask of the service pistol? In two words, stopping power. The ability of a pistol bullet to incapacitate a determined aggressor with a single, centrally placed hit defines its stopping power. It is almost painful to broach this topic, beaten to death as it was in the 1970s, for fear of boring the reader or stirring controversy on a subject long closed by silent assent. The point still surfaces in gun magazines, like a weighted corpse all would rather see hug the bottom. Those who read gun mags for more than a year understand that it bats stale air, fills space on the page.

Two equally ardent schools vie for primacy. The first believe in the superior stopping power of large-caliber bullets (.40 or greater). Their advocates use heavy-caliber weapons. Those who believe the .36 caliber series adequate (9 mm, .38 Special, .357 Magnum, and even the meek .380 auto) carry those weapons. Mute testament, perhaps, that some Latin American countries have outlawed civilian possession of the .45....

Handguns illustrate the laws of physics. One law says that for every action there must be an equal and opposite reaction. This explains the phenomenon of recoil: Guns "kick" when fired. The heavier the bullet and the faster it travels—the product of speed and mass is known as momentum—the heavier the recoil. This demands consideration, since the degree to which we can control a pistol depends upon the amount of recoil it generates. Without control, "the most powerful handgun in the world" becomes a noisy, dangerous, useless piece of machinery.

It turns out that the power-window where recoil is manageable, yet the bullet's momentum meets its task, is a small one. This puts power at a premium in pistols, compared with the surplus of it the rifle disposes.

To summarize—and this paraphrases Jeff Cooper's party line, Cooper being widely regarded as the father of modern pistolcraft—sidearms are deemed defensive units. Their purpose is to halt an aggressor with one center torso hit. Observation from actual shootouts suggests that the standard military .45 caliber load will do this close to 90 percent of the time. Numbers for the .38s make it to the 50-percent mark. (Newer, less imposing data argues against such a decisive advantage for the .45 and, coincidentally, keeps the controversy alive. It will be interesting to see if this heresy withstands the test of time.)

Despite evidence favoring the .45, which, at the moment, is the only duty-ready heavy-caliber sidearm available, it does not enjoy universal acceptance. (Colt's new 10 mm auto shoots .40 caliber ammo. It yet lacks a track record to define its role among sidearms.) Thirty-eight special and 9 mm weapons each rule droves of advocates. Part of this devotion in the face of compelling evidence lies with tradition. Cops have always carried .38s of one sort or another; tradition is reluctant to cede its center to reason. Our military has begun a sulking surrender to the notion that we should drop the .45 in favor of the 9 mm as our standard pistol cartridge simply because the rest of the world and our NATO allies use it.

Another factor, a rather fanciful idea, has it that use of "expanding bullets," i.e., bullets intended to deform or upset or blow up on impact, will compensate for smaller caliber. That logic has proven faulty because

these bullets recovered from felons often show no upset at all, unlike their behavior when fired into inert targets. (Gun-nuts get an orgasm of sorts from shooting hollow-point bullets into gallon milk jugs filled with water, basking in the explosive spray that erupts. Shoot the same container with a .45 jacketed bullet and it leaks water like tears of woe. The intuitive favor for the small-caliber hollow-point that results from this non-demonstration is understandable, but sways only those who cannot reason from real-world events.)

If the big .45 leaves 10 percent standing, and the .38s don't faze half our foes, we have to consider the shock delivered by pistol bullets to be marginal at best. This led naturally to attempts to improve their efficacy by alteration of design and materials. Those who would use pistols, and presumably purchase ammunition for them, should grasp the fundamentals of pistol bullets.

BULLET BASICS

Stop the average citizen in the street and ask him, or her, about bullets. Typical quips include, "They're made out of lead." "I wouldn't want to get hit with a dum-dum." And so on. This gut-level ignorance of the purpose, design, and function of pistol bullets led to perverted ideas and distorted notions that make for racy viewing, lurid reading; but they mislead us, sometimes with deadly results, in choosing our own personal arms. In truth, we understand bullets and their function straightforwardly, if incompletely and empirically.

All bullets possess three attributes: material, shape, and, once fired, velocity. Interaction among them determines their effect on a target, live or inanimate.

TYPE AND FUNCTION OF PISTOL BULLETS

Pistol bullets suffer in comparison with rifle ammunition in that they must get by with less punch. Alterations in shape, material, weight and speed of pistol bullets compensate partially for their marginal power. We will ignore the true Magna, such as the fabled .44, which offer an abundance of power, since that and similar loads defy control in the hands of all but a few master pistoleros, who choose tamer pieces for defense work in any case.

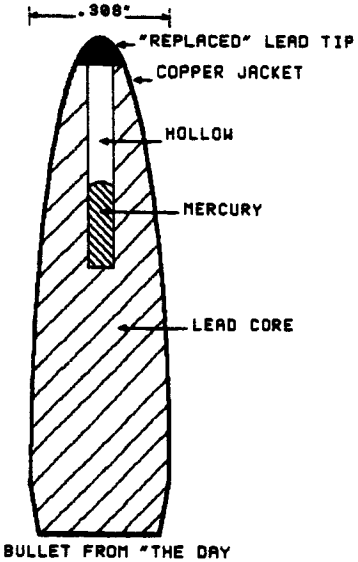
The average handgunner can narrow his or her choices, both of weapon and breed of bullet, through basic grasp of design and function of bullets.

WADCUTTER (WC)

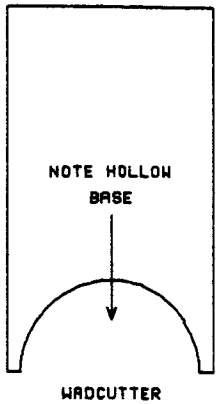
As its name suggests, the wadcutter punches a circle in a target, hardly a surprise, since it is a bore-diameter cylinder of soft or hard-cast lead. The full circle proves important when the judges brood over whether a given shot actually cut the X-ring. Most commercial loads are mild, since their intended use is target-shooting, rather than people- or material-shooting. Not that the design cannot be effective for defense, loaded to proper velocity; but we find few police or combat-oriented handgunners toting pieces chambered with wadcutters.

The bottom of many wadcutters holds a gaping, hemispherical hollow. It is supposed to flare under pressure and thereby seal the rear of the bullet upon firing. This prevents blow-by of propellant gasses. A few devilish handloaders (people who load their own ammunition, discussed below) seat the bullet base-forward, converting it into some gross, fearsome hollow-point. Shoot a plastic milk carton full of water with a frontward wadcutter and it sneers at you with a new eye. Shoot the same jug with a backwards wadcutter and it explodes in a spray of water and plastic that is flat impressive. Trouble is, there is no correlation between this eternally popular pastime of splashing milk jugs and stopping felons. The full metal jacket .45 slug, for example, has proven notoriously unimpressive against milk jugs, yet an exemplary stopper in gunfights.

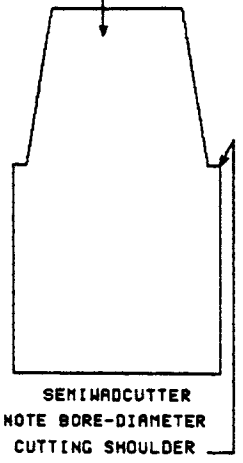
Avoid the wadcutter unless you are punching holes in paper and prefer light recoil. These bullets have been known to tumble in flight ("keyhole"), such that they strike the target sideways, with too little momentum spread over too great a front to let them penetrate articles of clothing, such as a leather belt.



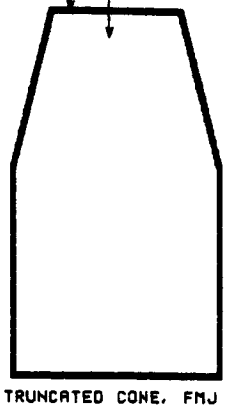
BULLET FROM "THE DAY OF THE JACKAL;" SEE TEXT



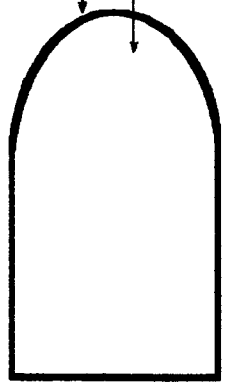
WADCUTTER



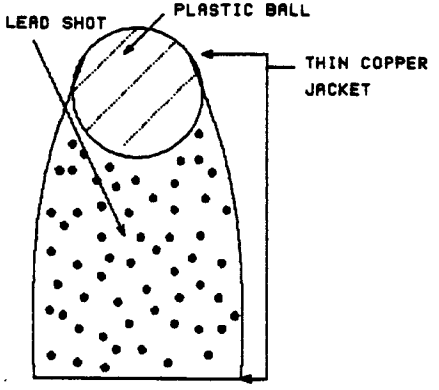
SEMIWADCUTTER
NOTE BORE-DIAMETER CUTTING SHOULDER



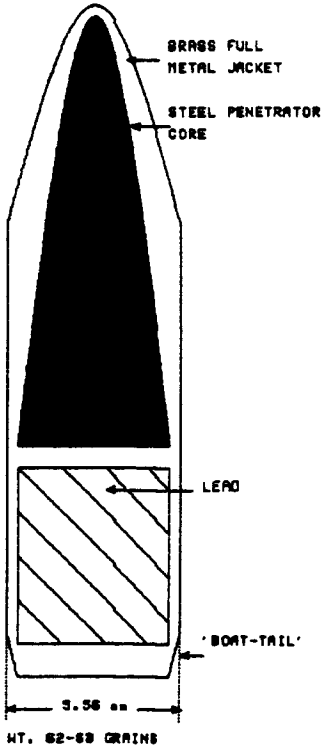
TRUNCATED CONE, FMJ



ROUND NOSE, FMJ
(THIS DESIGN ALSO COMMON W/PURE LEAD)

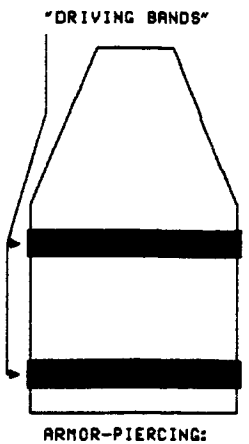


GLASER SAFETY SLUG

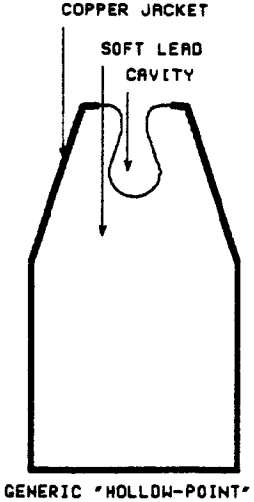


WT. 62-69 GRAINS

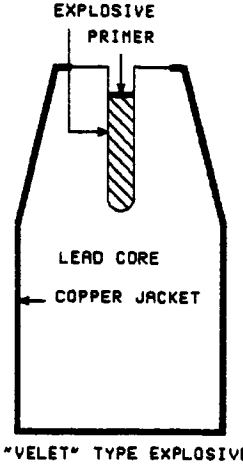
DIAGRAM OF NEW STANDARD 5.56 MM ROUND



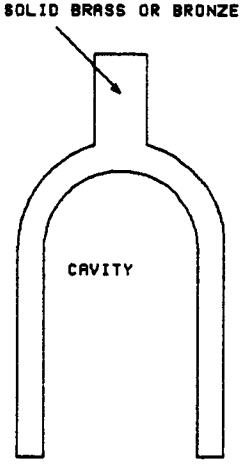
ARMOR-PIERCING: SOLID STEEL, BRONZE, OR TUNGSTEN ALLOY, W/ OR W/O PLASTIC COAT



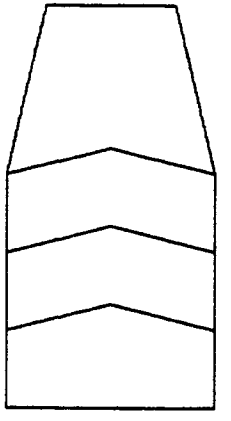
GENERIC "HOLLOW-POINT"



"VELET" TYPE EXPLOSIVE BULLET, NO LONGER SOLD



SHORT-RANGE ARMOR-PIERCING; SEE TEXT



PRE-FRAGMENTED SLUG

SEMIWADCUTTER (SWC)

Glance at the two designs to note a family resemblance that gives rise to the name, yet only hints at the vast difference in roles of the two shapes. The semiwadcutter is known also as the "Keith-type," after the late and eminent Elmer Keith, whose colorful career as marksman, cowpoke, and hunter has the stuff of legend. Keith is given credit for this basic design.

The SWC features a cylindrical base on top of which sits a truncated cone, with the specific feature of a sharp, bore-diameter shoulder at their junction. Consider the benefits of this design compared both to the wadcutter and to the common round-nose bullet. First, the SWC has proven extremely accurate. Properly executed designs do not keyhole. Second, it has shown itself to be a more effective bullet than most. We measure a hunting or defense bullet—and let us not avoid the grisly point—by its ability to wreck tissue. Passage of a round-nose bullet through tissue at pistol-bullet velocities must cleave a path; but we could not choose a more gentle probe than the round nose. It pushes structures aside to let itself through a path of least resistance.

But look at the semiwadcutter. Its broad, flat tip cuts whatever tries to slip around; the sharp, bore-diameter edge at the junction of base and cone is far more likely to cut whatever it grazes: arteries, nerves, other vital structures. Some have opined that the SWC, other factors being equal, gains 25 percent effectiveness over a round nose bullet.

SWCs are available as dead-soft lead (which is more likely to deform on impact, perhaps gaining as a result of that, but losing its SWC shape) and also as hard-cast lead, the choice of most who shoot this design.

The SWC shown in the photo is a 185-grain full metal jacket design atypical of the breed, since it is intended to feed in automatic pistols. The diagram shows the most common SWC shape. The slug in the photo lacks the mean cutting shoulder of designs found on bullets used in revolvers. This one is fit to the .45 automatic. Sacrifices had to be made to facilitate feeding. When found in commercially loaded cartridges, its velocity is usually mild, since many consider it to be a light target load. In guns modified to feed it reliably, and loaded such that its momentum matches that of the standard round, it can be effective. (The standard .45 load we have referred to, the one with such a splendid record in defense situations, is known as military ball-type ammo, or "hardball." It is a 230-grain round-nose, full metal jacketed bullet traveling about 830 feet per second. For the 185 grain bullet to match hardball's momentum, we must load it to a velocity of 1030 fps, though experienced handloaders [the reader is warned not to attempt this] push the round up to far higher speeds, at their risk....)

Given a choice between a "hollow point" and a hard-cast SWC, take the SWC if anything important rests on the shot.

JACKETED HOLLOW-POINT (JHP)

Prior to 1960, mere mention of dum-dum bullets sent cold chills shuddering through a simple-hearted populace. Tale was told that drilling a hole in the tip of a lead bullet, or carving an "X" on it, guaranteed that, when it struck its pathetic victim, it would mushroom into a horrible glob of death, ripping a wound that killed all hope of survival. Gangland types were reputed to give their ammo this type of treatment before a rub-out. (They were whispered, also, to smear the noses of copper-jacket bullets with garlic, since this would induce gangrene.)

Even Mad magazine swallowed this malarkey. In a hysterical parody of gun-ownership it ran in the early sixties—a better time, and one of Mad's cuter pieces, by the way—it promoted the sale of an X-ray machine to let kill-crazed hunters watch their dum-dums expand inside the game. We had a fine chuckle at that. Gun-nuts would have less of an attitude if they could laugh more at themselves.

But back to the point. The dum-dum concept served as forerunner of the modern JHP, or jacketed hollow point, now offered in an array of catchy designs. The prototype shares a core of soft lead wrapped in a copper jacket, with a tip that may or may not expose some of the lead, and which holds a hollow cavity whose placement and design are specifically made to cause the bullet to upset (mushroom; blow up) on impact with semi-soft material.

But what does that, in turn, accomplish? The larger the diameter of a projectile traversing flesh, the greater damage it leaves. But the diameters of bullets we would prefer to shoot—say, three quarters of an inch—are not practically attained in hand-held firearms. Many refuse to carry even the .45, whose bullets need no further expansion. The JHP is supposed to let us shoot skinny bullets that act like a fat ones once they strike home.

And tests of these deadly missiles with inert, supposedly flesh-like material would lead us to expect the best (or worst) of them. A .45 caliber 185 grain Sierra JHP whizzing along at 1200 feet per second (fps) hitting duxseal, or a string of gallon milk jugs filled with water, or soft sand, produces a beautifully pancaked slug, a shape reminiscent of the first 300 milliseconds of a nuclear groundburst—and does it quite consistently. (The same can be said of most other brands and designs. We use Sierra here out of personal experience.) The withering thought of this explosion taking place inside one's flesh is enough to make it feel as if it were already jelly.

But JHPs have had problems, chief among them an uneasy reluctance to expand, even change shape at all, when fired into felons. Some bullets collapse, actually shrinking their frontal diameter. Autopsies are a routine part of processing felons terminated in the course of gun battles with cops. They tell us what happened to the bullets. Evidently, flesh and bone lack something found in inanimate media.

Some of the projectiles fragment, as soft lead bullets are wont to do. Flesh is not a homogeneous medium, and that may explain it in part.

Consider velocity. This seems critical to proper performance of the JHP. The likelihood that the JHP will live up to its hype grows in proportion to its velocity at the target. Bullet makers and gun writers test these products under conditions most conducive to expansion: We do not shoot milk jugs at 80 yards with JHP pistol bullets. We shoot them at close range, before they shed velocity. Expansion, after all, is the name of the game. There would be no photos, no ad, no article, without it.

Test-bullets get fired from long-barreled guns to maximize their speed. But in the real world, police often shoot these bullets from snubby revolvers with two-inch barrels—bullets that had been tested in guns with eight-inch barrels. (The longer the barrel, the higher the velocity, especially with pistol ammunition. When fired from 18-inch rifle barrels, otherwise marginal bullets move up into the magnificent class. Shot from a rifle, they actually do what we expect of them fired from the pistol. Perhaps Wyatt Earp's Buntline Special would have proved a proper match for the JHP had they been contemporaries.)

Cartridge designers have not been blind to this need for speed to get the product to perform; but the only practical means of pushing a bullet faster out of a given sidearm is to lighten it. (Load a heavy bullet to higher velocities and its recoil renders the weapon uncontrollable, useless in hitting the target. And these hotter loads mean higher chamber pressures. At some point, the gun will explode. For these and other reasons, bullet makers have gone to lighter bullets to reach needed higher speeds.)

But with a light, high-speed bullet fit with a soft, hollow tip, we run into the same penetration difficulty that plagues heavy wadcutters moving at low speed: The light JHP can pancake on a wallet or belt and fail to penetrate.

The diagram illustrates a generic JHP design; the photo shows two examples, one a .45, the other a 100-grain .355 caliber designed for the .380 auto. The .45 bullet weighs 200 grains; but we have already noted that likelihood of expansion depends largely on velocity. Twelve hundred fps is a comfortable minimum when talking JHPs. The 200 grain JHP will match hardball recoil at 954 fps, hardly enough to promote confidence in its expansion. Moving up in speed to 1200 fps would take recoil out of the controllable range for many shooters. Fortunately, the round is quite acceptable at 954 fps because it is big-bore: it leaves the barrel already "expanded."

JHPs offer a theoretical advantage that their properties reduce the chances of passing through a felon and injuring bystanders. (The lawsuit would name the officer, his Department, the gun-maker, and most of all the bullet- and cartridge-maker, along with every known insured party within a twelve block radius of the shooting....)

ROUND NOSE LEAD; ROUND NOSE FULL METAL JACKET (RNL; RN FMJ)

Round nose bullets probably appeared shortly after the musket ball. The evolution was natural: The shape retained the frontal curvature of the original, but added a cylinder to the tail, which gave it greater sectional density and stability. This made it carry further and penetrate deeper, and improved accuracy. There are too many documented instances of pinpoint-accuracy at thousand-yard ranges, with simple round nose bullets fired from the Sharps carbine back in the buffalo-slaughter days of the old west, to deny the accuracy of which this plain design is capable.

The form comes in dead-soft lead, hard-cast lead, and lead fully covered with a metal jacket, usually copper or copper alloy. Aside from general popularity—this shape appears in the lay mind's eye at mention of the word "bullet"—the breed finds greatest application in automatics. The rounded nose slides easily up the feed ramp, making for fewer jams. Now, even SWCs will feed reliably in carefully modified autos. But it is wise to regard the automatic as a finicky eater. It was designed to feed round-nose, full metal jacket bullets. That design remains the odds-on choice for reliability.

The photograph shows two 230 grain .45 RN FMJs; but note subtle differences in shaping. The leftmost two bullets are different brands, one slightly less pointed than the other. Both are 230 grain RN FMJs. (Incidentally, a 230-grain pistol bullet is considered heavy. The .357 Magnum commonly handles 158 grains as its heaviest load.)

As to effectiveness, the RN FMJ is considered least efficient. Where other shapes offer several means to disrupt tissue by their passage, the round-nose slug, particularly jacketed designs and hard-cast lead, present the least. One authority feels that we should deduct 10 percent from a bullet's expected performance if burdened by this shape, with the exception of dead soft lead, which will probably deform or fragment on impact.

FLAT-POINT FULL METAL JACKET (FP FMJ)

This design has done well in the 1980s. It offers theoretically better performance (i.e., carnage) over the RN FMJ by virtue of its flat tip, yet has shown itself to feed reliably in automatics. And those who have owned automatics will testify that feeding can be iffy, particularly in new, unmodified weapons. Third, the bullet has shown itself accurate. Author's choice for the .45 auto.

HYBRIDS

What if we took a base of dead-soft lead, wrapped it in a copper jacket, then mounted a truncated lead cone atop it, giving us the bore-diameter cutting shoulder of the SWC—and then threw in a hollow tip just for good measure and a bit of spite? That would designate the SWC/SJHP (semiwadcutter/semijacketed hollow point).

This isn't so much of a Rube Goldberg design as it seems. It offers, or tries to, the most desirable features of all bullets—and it has succeeded. Some highly qualified people have investigated the performance of this design in gunfights, and have come up with figures supporting its efficacy.

SPECIAL-PURPOSE AMMUNITION

GLASER SAFETY SLUG

Take a thin, hollow copper jacket, round-nose shape, closed on the bottom and open at the tip. Fill it with as much tiny lead shot (#12 or so) as it will hold, along with a buffer to keep the shot suspended, then close the tip with a plastic sphere. On impact, the jacket peals away, leaving loose lead shot to do its grisly work.

The notion of "safety" in this slug comes from the fact that A) it is unlikely to exit anyone it strikes, and B) it is unlikely to ricochet as an intact mass, preferring rather to fragment into semi-harmless micropellets.

How does it stack up in stopping power compared with ammo that stays in one piece? Ads tout it as 3.5 times as effective as hollow-point bullets of equal caliber. Frankly, it has racked up too little gunfight data to judge it at this point. It has drawn "Ooohs" and "Aaahs" from some sectors, but the combat mainstream has

not jumped on the wagon. In theory, there is something to say for the design, available in both pistol and major rifle calibers. Cost runs several dollars a round. It's on the shelf at your local gunshop, or you may order it from Phoenix Systems (Box 3339, Evergreen, CO, 80439; 303-674-2653).

PRE-FRAGMENTED BULLETS

Remember the Duncan Top craze of the early 1960s? One model split into two separate spinning tops upon release. The two mated snugly in a way similar to certain pistol ammunition that splits into two to four separate slugs once it leaves the barrel. Some have dubbed it, like the Glaser, a "safety" slug, since its chances of coming out the other side of a felon are just about nil. An interesting if unproven concept.

ARMOR-PIERCING PISTOL BULLETS

An army needs to punch through inches, sometimes foot-thicknesses, of alloy plate specifically designed to resist attack. This notion is second nature to the military. Fortifications and armored vehicles instantly call up the need to defeat their protection.

Armed forces can tap a vast set of projectiles and explosive weapons to penetrate armor. At the infantry level, armor-piercing ammunition is nothing more than the standard rifle round that substitutes a steel core for the lead one. It will penetrate light armor, as in the metal flanks of jeeps and such.

But when talking serious armor, as found on tanks, with a foot or more of solid or composite armor to tackle, a host of devious weapons are at the infantryman's disposal.

Probably the best known is the shaped charge. Refer to the diagram of a generic antitank rocket. Note the warhead. The charge consists of a cylinder of plastic explosive, flat on its rear, where detonation triggers. The forward end is hollowed into a cone lined with copper about 3 mm thick. The cavity subtends an angle of 42 to 44 degrees. Further, note the distance between the charge and the projectile's tip, necessary to achieve "stand-off," a space that attains optimum penetration.

When the projectile strikes its target, it initiates detonation at the base of the charge. The shock wave moves forward in a millisecond or so, where something known as the Munroe effect focuses the energy of the blast to a point. The copper forms a jet moving at incredible speed, under incalculable pressure. Some refer to it as a high-density vapor, while one authoritative-sounding source indicated that the copper does not melt in this process. In any case, the warhead carries enough punch to breach armor plate five times the diameter of the charge. For a 3" warhead, that's well over a foot thickness of armor.

The charge must detonate about 1.5 times its own diameter off the armor for maximum effect, and this explains the stand-off space at the front of the projectile. Indeed, recent designs sport a long snout protruding from the tip of the charge, which serves to initiate detonation so as to maintain optimum stand-off.

For decades, the power of a big enough shaped-charge warhead to defeat tank armor remained unquestioned. Heavier warheads countered thicker armor. The Chobham composite armor used on our latest M1 main battle tank contains layers of ceramic sandwiched between metal and plastic, its exact makeup and configuration still classified, but since the design originated with the British, whose intelligence system has more moles than your garden, the Soviets are assumed to be well up on its particulars, and to have incorporated it into their own tanks.

On impact, the ceramic fragments, distributing force over such a wide area that penetration fails. Our best armor is said to be able to survive several hits from various types of armor piercing rounds without compromising the tank.

The latest on our passive armor tells of a composite of steel and spent uranium that achieves twice the density of steel, yet retains its toughness. One source maintained that it would take the Reds "a decade" to develop weapons that would defeat this armor. Uh-huh. (And there is some irony to using spent uranium in armor, since it has long found a use in armor-piercing bullets, discussed below.)

There are other ways to "get" a tank. One requires no penetration of the thickly armored hull, but wreaks havoc inside. The weapon is a cylinder of soft plastic explosive arranged such that the front half of it flattens into a pancake on impact. Known as the squash head, this mushroom shape detonates to render a shock to the hull like a blow from God's own hammer. This throws off material lining the inside of the turret with devastating force, a phenomenon known as spalling.

Finally, we have pure kinetic energy weapons—devices that punch through on momentum alone. Students of armor-piercing have found that power of a missile to penetrate correlates with its velocity, hardness, absolute density and sectional density. That means a hard, high-velocity projectile that concentrates its momentum on a point. Successful designs look like mean, slim, ten-pound tungsten darts, which is what they happen to be. Tanks fire them at muzzle velocities in excess of 5000 fps. The projectile, which measures only a fraction of the diameter of the tank's main gun, traverses the barrel held centered by plastic material, known as a sabot, that sheds once the projectile exits the barrel. The idea is to get this comparatively lightweight piece of ordnance moving at extremely high speed. The concept has found application all the way down to .22 caliber weapons that fire saboted projectiles the diameter of BBs (.177 caliber).

There are defenses, at least against the shaped charge. In addition to composite armor, one late development (1982 to 1985, depending upon which source you believe) is known as active armor. It consists of flat slabs of high explosive sandwiched between metal plates, mounted on standoffs from the main armor and surrounding the most vulnerable yet toughly protected part of the tank. When struck by a shaped charge warhead, it triggers detonation of the plastic slab. The outward force of its detonation counters the incoming jet of copper to prevent penetration. (Predictably, counter-weapons placed a miniature shaped charge on a stalk several warhead-diameters in front of the main anti-tank round. It triggers the active armor prematurely, paving the way for the big jet.) There is talk of of even more aggressive armor: It senses the incoming projectile and explodes like a mine, spraying shrapnel to deflect or disable the warhead.

This lewd digression into military armor and its solutions will serve as points of comparison as we confront the similar if small-scale problems of personal body armor and its devils, and also lays a base from which to discuss armor-piercing pistol bullets. The need to defeat armor arises with less clarity in the civilian sector, even among law-enforcement, though that grim scene has changed with the ugly spread of terrorism.

Until 1968, the answer to reaching felons barricaded or protected by armor of sorts—automobile bodies or other thin metal—was to move up to rifles. Standard military FMJ bullets penetrated easily. Either that, or lob in a canister of gas.

But in '68 a company which called itself KTW, an acronym based on the company principals' names, began to market handgun ammunition possessed of genuinely startling ability to penetrate. No longer was there a wait for the squad to bring up its riflemen. The officer at the scene could spill a few KTW rounds out of his ammo pouch and have his bullets penetrate car-bodies—several thicknesses of metal sheet—with enough punch left to dispatch the felon. There was even talk of stopping getaway cars by shooting the engine block with these unique rounds.

KTW ammunition remained an obscure if dramatically effective piece of merchandise, a very special product with extremely limited application. In recognition of hazards the ammo would pose in casual hands, the company refused to sell to any but police, military, or State Department agencies, or to foreign governments approved by Uncle. In fact, sources report the bulk of the company's product earmarked for overseas shipment.

KTW ammunition evolved. Early on, the bullets were made of tungsten alloy of a type in military use for some time. But tungsten is both expensive and difficult to work. Producing uniform projectiles, a must for accuracy, could be simplified if a cheaper, easily worked metal were used; but that would rob the bullet of its terrible penetrating power.

The sixties happened to be the era of polytetrafluoroethylene (PTFE), discovered, incredibly, thirty years prior, about the same time as Nylon, and sold by DuPont under the trade name "Teflon," which became as much a household word as "Alpo" or "Maidenform." PTFE gained renown for its non-stick qualities and its ability to cut friction between sliding surfaces. One source states that PTFE holds a place in The Guinness

Book of World Records as the slipperiest man-made substance. PTFE might have found earlier commercial application had it not proved vital to one phase of the Manhattan Project, a quirk that kept it under wraps.

What, asked the inventors of KTW, would happen to a hard, solid bullet coated with PTFE? Would its penetration power change?

A determined series of experiments produced the answer. It would multiply the piercing power of the bullet enough to let the company discard expensive tungsten in favor of a more workable alloy coated with PTFE—and there it rested, quietly and efficiently filling needs, often covert and involving terrorists, met by no other product. And there it would have remained, were it not for the slaver of our own savage media and its insatiable lust for cheap thrills.

KTW AND THE "KILLER BULLET" FIASCO

The years following debut of KTW saw in addition the arrival of another miracle from the DuPont laboratories. Its trade name: "Kevlar." This aramid fiber proved incredibly strong for its weight. What's more, it could be woven into fabric as easily as orlon or rayon.

Kevlar possessed a property besides tensile strength. When ruptured, it split on a microscopic level into many smaller fibers, thus distributing the force over a great surface area (compare this with the behavior of ceramic composite tank armor). This endowed it with amazing resistance to penetration, and gave birth to the first generation of genuinely effective body armor: truly bulletproof vests.

Flak jackets made of so-called ballistic nylon had existed prior to this time, as had a ceramic armor used to shield helicopter pilots in Vietnam. But in Kevlar we had a product that let us fabricate a "vest"—front and back panels—weighing about 2.5 pounds, capable of stopping a 12 ga shotgun slug and most common pistol ammunition at point blank range.

Availability came first to those at greatest risk: law-enforcement and security personnel. It filtered quickly down to righteous citizens, then further down to the sinister underworld of criminal types and terrorists.

The question which had not pressed itself up to that point was, Would any pistol bullets defeat the unreinforced Kevlar vest? When trials got around to testing KTW, the answer was yes, and rather handily. This proved the proverbial double-edge sword. KTW put in the hands of police and proper authority the ability to dispatch armored gunsels. But tacit in this ability was the notion that, should gunsels get their hands on KTW, nobody was safe, even behind Kevlar.

This prompted some few but vocal members of the law enforcement community to call for a ban on KTW and other bullets capable of penetrating their soft body armor. If the debate had taken place behind closed doors, as well it should have, no problem might have arisen. Instead, the television media decided to deal with the issue on its own inimitable terms.

America's vile customs dictate that the way to get one's way is either to buy it or have the media promote it as good for the common weal. In 1982, a major television network aired a piece that showed just how effective KTW ammunition could be against soft body armor. The demo placed three vests in a stack, and set the bundle against a backstop. A henchman fired one KTW round at the armor. It whizzed through all armor panels, coming to rest finally in a thick backstop. Impressive performance, to say the least. But what lacked class, in the opinion of some, was the way the show handled it. It went along with those who had dubbed KTW "killer" or "cop-killer" bullets because they could defeat the armor worn by many police. While this made for lively viewing, some called it irresponsible.

A reporter involved in bringing us this fated story did not try to hide his glee as he announced that DuPont would, reportedly, refuse further sales of Teflon to make "killer bullets." Literature published some years after the TV event showed that PTFE-coated bullets were still available. The publisher wrote DuPont's public relations department to ask for a statement of policy in this regard. We have printed a photocopy of their courteous and informative reply.

Tacit in the notion of the "cop-killer" bullet has to be the knowledge that police wear body armor. Since

KTW had gone to some trouble to keep its product out of the wrong hands, most criminals would have a hard time procuring it. The solution is obvious to any sixth-grader contemplating a shootout with the law: Shoot for the head or, just as bad, south of the border.

Some have charged that several deaths, both of peace officers and diplomats shot in the head in the wake of the program, traced to their assassins' having been wise to the fact that the targets were probably wearing soft body armor—and the assassins did not use KTW bullets.

The TV program maintained that its subject was armor-piercing bullets, not body armor. But no one can deny that the program effectively educated thousands, perhaps millions, of potential criminals as to how to handle a shootout with the cops without armor-piercing ammunition.

That observation calls up such grim irony because, in the wake of the broadcast, AP pistol bullets have been restricted or banned at the state level in many areas. According to ATF P 5300.5 (12-86) State Laws and Published Ordinances - Firearms, 17th Edition, the following states have nixed armor-piercing, metal-piercing, plastic-coated, or PTFE-coated pistol bullets: AL, CA, DC, FL, IL, IN, IA, KS, LA, ME, MN, MO, NV, NH, NJ, NY, OK, OR, PA, RI, SC, TN, TX, and VA. Wording of some laws infers an element of raw hysteria. For example, one law bans KTW bullets by name, despite the fact that at least one other firm produces PTFE-coated bullets, and another makes non-coated armor-piercing bullets. Presumably, one could buy identical bullets by any other name and stay within the folly of that law. Other states ban only PTFE-coated bullets, or specify the composition of pistol bullets as to percentage of lead and so forth. Many states exempt police and the military from these bans.

BATF's publication offers a wealth of additional information concerning weaponry laws, neatly summarized, though necessarily not up to date. Some states have banned electrical weapons, firearm sound suppressors, or destructive devices, such as the reactivated hand grenade discussed below, including the components needed to construct them. There seems to be little doubt that millions of Americans break these laws every year, perhaps every month, simply because they don't know what's on the books. Indiana, for instance, prohibits civilian use of bullet-resistant materials to harden private vehicles. This booklet is available at nominal cost (BATF sent our copy gratis, since they believed our query had invoked the Freedom of Information Act) and should be considered a starting point in screening sites for engaging legally in some activities discussed herein. What you cannot do legally, do not do....

Before so many states outlawed PTFE-coated bullets, how many cops died after being shot with KTW bullets that defeated their body armor, as compared to the number killed by felons hip to the fact that the cop was armored, and shot for the head? The media has yet to force the answers on a dumb populace the way it shoved the idea of "killer bullets" down their throats. In fact, the author's research has failed to uncover a single instance of a police officer shot through his body armor by a felon using KTW ammunition. Readers with proof to the contrary, please write the publisher.

So laws have been passed banning a product which, from the outset, its makers kept out of the wrong hands.

The possibilities inherent in armor-piercing bullets have not been lost on terrorists. The Eastern Bloc has responded by producing a round with similar ability to defeat body armor, and it has seen use in terrorist attacks. Some terrorists have eschewed the suicide credo, and for that reason wear body armor themselves. Depriving our own operatives of KTW would make splendid sense in that context....

FRENCH ARMOR-PIERCING

KTW is hardly the last word in ways to defeat body armor. Unreinforced Kevlar doesn't stand a chance against common military ordnance such as the 5.56 mm or 7.62 mm FMJ bullets, the smaller caliber now standard of our army's own M16-A1 and the latest NATO family of assault rifles. These projectiles have sharp points by pistol-bullet standards, and carry far greater velocity. They whiz through soft body armor. That observation and the presumption that velocity is a key factor in penetration led one group to design a pistol slug that would defeat a Kevlar vest at short range, and yet not present nearly so much danger as a stray KTW round or rifle round at longer ranges.

The design is a solid metal with a semi-pointed tip, weighing only a fraction of the 158 grains or so for the typical .357 magnum round. The slug reaches velocities in the vicinity of 2000 fps from a handgun barrel. At that speed, it burns through the front thickness of armor.

But lightweight projectiles shed their speed quickly. This design clearly presents less of a threat than ordinary rounds at longer ranges.

The round, like others specifically designed to defeat armor, is highly specialized, with restricted access.

SPENT-URANIUM HANDGUN AMMO?

We have found uses for uranium which has sacrificed its radioactivity on the alter of nuclear power. Known as spent or depleted uranium, it loses none of its incredible density, greater than lead, and adds the property of pyrophoria. This refers to the fact that, like plutonium, it will burst into flame on exposure to air. The heat released lends spark to its penetration power.

This material found a home in saboted 30 mm and 20 mm cannon rounds used as antitank/antimissile weapons. The 30 mm projectile, traveling at several thousand feet per second, could defeat all known tank armor, at least until recently. (And when it makes it to the boiler room, it sprays burning, highly toxic molten metal around the interior with explosive and incendiary effect. Amazing how insecure one can feel behind a foot-thickness of armor....) An otherwise identical projectile of lead would splatter on the armor like high-velocity Haagen-Dazs.

The Phalanx antimissile defense system fires 20 mm rounds. This same fearsome setup was not activated in the USS Stark tragedy in the Persian Gulf. The weapon tracks sea-skimming missiles inbound to ships and sprays its 20 mm spent uranium bullets at an incredibly fast rate. A single strike from such a round could destroy the missile, render it inexplosive through damage to the detonator, or splash it in the ocean.

This makes for compelling speculation as to what kind of performance we might expect from a .45 or .357 Magnum bullet made of spent uranium. Sadly, speculate is all we can do. The determined experimenter may get his hands on tungsten or less exotic alloys nearly as hard, but will not come by spent uranium or the inert-atmosphere chamber necessary to keep it from igniting out of spite.

EXPLOSIVE BULLETS

Ads appeared in Soldier of Fortune in 1978 for Velet exploding bullets. Those ads have faded, and so, presumably, has the product. Some states have banned explosive bullets along with AP rounds. The diagram follows one that appeared in a Velet ad.

Its purpose is obscure, since the whole rationale of exploding projectiles is to deliver the explosive to the target and let the explosion, more than the kinetic energy of the projectile, do the damage; or, with anti-aircraft rounds, let the explosive blast the projectile into shards of flak, to be sucked into a jet intake and devastate the turbine. We do not reach the point at which the power of the explosive exceeds that of the the bullet's kinetic energy until projectile diameter passes an inch.

The design is reminiscent of exploding pellets 13-year-olds used to make back in '65. Scrape the coating off match-heads—the strike-anywhere variety gave best results—and pack it into a pellet for a Benjamin pellet rifle (or any brand that will fire hollow-based pellets). Load the pellet open-end forward and fire at a hard surface, such as brick. It lets go with a satisfying report, like a loud cap pistol. The thrill wears off after about three shots. Hard to believe that deranged experimenter would go on to get his bachelor's degree with honors. Our world has shown little use for star students but will pay to read about mindless trivia, such as exploding pellets....

RUSSIAN AFGHANISTAN-TYPE

Now, what manner of bullet might we expect the Soviet Army, the same force fond of leaving explosive dolls and other crippling toys around to maim Afghan children, to shoot from its rifles? Strictly Geneva Convention ammo, right?

Soldier of Fortune reported on rounds it obtained on a field trip to Afghanistan. One examined by X-ray showed what appeared to be FMJ—standard military ball type ammo—but the tip was hollow without an exposed hole. According to reports, the round produces wounds which are difficult to treat and heal poorly. For lack of a better name, why not call them "Detente" rounds, since they see so little mainstream press....?

STRANGE BULLETS: JAWS II

Credit the cinematographer for Jaws II. He shot a splendid close-up sequence in which beleaguered peacekeeper Roy Scheider drips a deadly blue solution of "cyanide" into the hollow points of his pistol bullets, then seals the tips with melted wax, grimly awaiting the next attack of a mechanical-looking shark.

Do poison bullets exist in life? They have, though not on a wide scale. We have darts which inject immobilizing drugs into animals, and one supposes that a fatal potion could be substituted easily. But as for use in firearms, on a one-off basis only.

JACKAL-TYPE

—so-named for lack of a better designation, since the design seems to have seen life only in the pages of Frederick Forsythe's first-rate thriller, The Day Of The Jackal. He had his assassin use special "explosive" bullets in the attempt to dust DeGaulle. His clandestine armorer cut the tips off a brace of rifle bullets, drilled holes down the center of their lead cores, put a drop of mercury in each hole, then re-sealed the tips with molten lead, restoring their pointed shape. The added destruction was fancied to arise from some demented no-seat-belt mechanism: When the bullet struck, the body of the bullet would slow, while the extremely dense mercury (13.6 times as dense as water) would keep going, splatter out the end of the bullet and do untold ruination.

If it served some purpose, all the fuss might be worth it. But the fact is, it's tough to improve on the destructive performance of readily available projectiles. Worse, to keep accuracy from falling off into the unusable range, the hole would have to be drilled exactly on center, a tough feat, as those who have tried will attest. (And what of the mercury as the projectile spun in flight? Would it be thrown outward onto the walls of the hole, altering center of gravity constantly?)

Applaud Forsythe for a superb imagination on this one, but do not bother to worry about foes using this round on you, or of ways to make your own. As a bullet it's a belly-flop.

HANDLOADING

There is much to say for factory-loaded ammo. American-made product almost invariably rates high quality, passes numerous inspections, has proven reliable, and, due to sealants applied to bullet and primer, lives longer on the shelf than handloaded ammo. And in most cases it is reloadable, i.e., we save the spent case and a great deal of money.

Its cost can be reasonable, particularly for those willing to go in for a thousand rounds at a time, or those willing to settle for aluminum-case ammo, specifically designed not to be reloaded but to be inexpensive (about $.26 a round for .45 ACP).

On the other hand, the occasional shooter will find factory ammo extremely expensive: up to fifty cents a round for large pistol ammo. Now, it is possible to reload cartridges spent cases, sometimes more than twenty times, before the case gives out. Reloading requires removal of the primer and replacement with a new one. Cost: roughly one cent per round. Second, the powder charge must be replenished, again, at a cost near a penny a round, though this varies widely among propellants. Third, a new bullet must be seated in the case. New, factory-made, FMJ or HP bullets go for 6 to 8 cents a round in quantities of 500; less in larger quantities, more for boxes of a hundred. A cheap alternative involves use of cast lead bullets. An artificer can make these for less than a penny apiece, exclusive of cost of machinery needed to melt scrap lead and cast it.

It boils down to about $.25 a round for the least expensive factory ammo, versus less than ten cents a round for handloaded ammo.

In addition, handloading offers incredible flexibility. The loader may choose reduced powder charges for light loads pleasant to shoot and easy on the gun; or may push his luck by gradually upping the charge until signs of excessive pressure appear, or the gun explodes. Not recommended.

We mention handloading primarily as it relates to cost, since the one factor essential to maintenance of proficiency with the pistol is practice, and we have seen over and again that the urge to practice rises as the cost of practice falls. Only handloading offers such a huge price break over factory ammunition.

The handloader will have to lay out about $150 initially for a basic setup: reloading press, a set of dies (one for each caliber), a scale with which to weigh powder charges accurately; and, most important, a good reloading manual, to be memorized before ever attempting a reload.

Pistol cartridges are extremely easy to reload; rifle cartridges a hassle. Best start with pistol ammunition and work outward into this fascinating hobby. Those who find it necessary to fabricate truly effective armor-piercing rounds discussed below must master the basics of handloading before attempting that grim feat.

Recent relaxation of the firearms laws made it possible to purchase bullets and cases by mail. No records of your name, address, and so forth, if you use an alias and have the merch shipped to a secure drop. Powders, primers must be purchased at your local gunshop, but, again, there is usually no longer a need to flash your driver's license and fill out a form (though some states and municipalities have been more tight-assed about this). The last time the author purchased pistol ammunition, he walked in, pointed out what he wanted, had it rung up to "cash," and walked out of the shop, a total stranger, the way it should be....

* * *

FABRICATE GENUINELY EFFECTIVE ARMOR-PIERCING PISTOL BULLETS

The author sleeps more correctly knowing that laws in his current state of residence restrict KTW-type ammunition. In theory, the wrong crowd can't get their feverish hands on it.

Having said that, let's take a serious look at fabrication of armor-piercing pistol ammunition by the non-professional sporting a legitimate need for it.

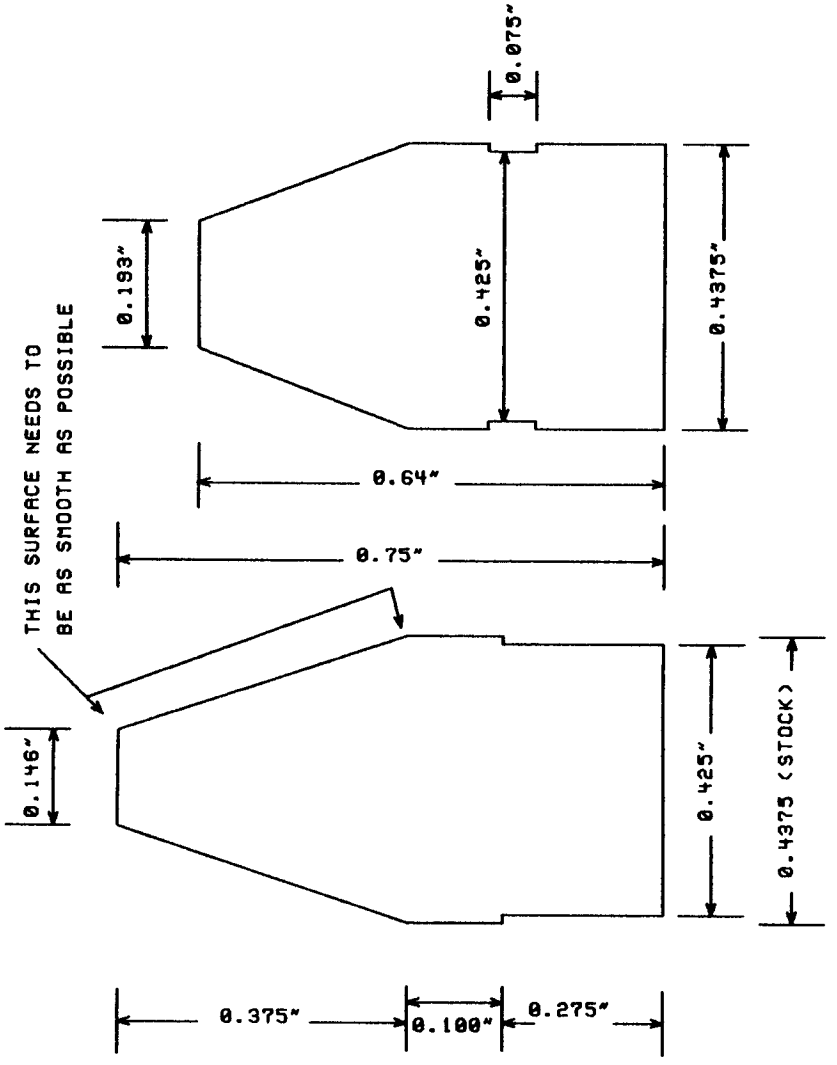
Ugly scenes around us hint at such a proper need. Urban and suburban residents today face constant peril from drug dealers in previously crime-free neighborhoods. Crack houses have sprung up in what were once model suburbs. It takes no frisk to tell that these hoods are wearing standard body armor. Either take them with head shots, something best left to skilled shooters, or defeat their armor, taking advantage of the false sense of security it offers, and giving the advantage of surprise.

Do not spray a PTFE-containing lubricant on the tips of common FMJ RN bullets and expect them to penetrate armor. Much of this sad lack of zap has to do with the fact that the bullet itself is too soft, and the spray coating is mostly oil that doesn't stick. (In fact, if the lubricant wets the chamber of the gun, it could lead to an extremely dangerous malfunction.) So, as a first step, fabricate bullets as close to KTW in shape, weight, and material as possible.

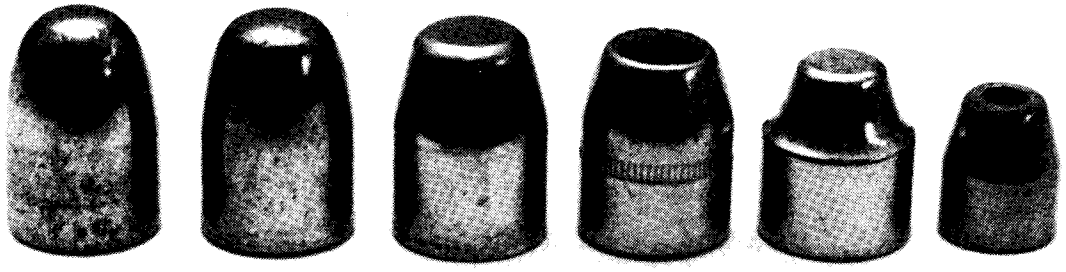
Principles of piercing armor, both formal and intuitive, provide for the following:

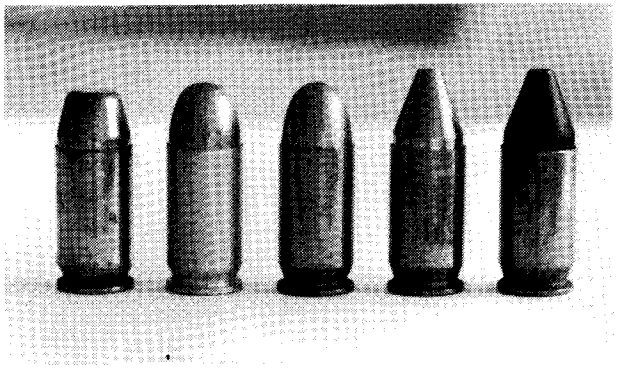
First, the bullet must be hard relative to the target. We cannot expect lead bullets to defeat steel; they splatter like rotten fruit when they impact a hard surface. (Recent experiments with magnetically propelled projectiles showed that this hardness factor fades as velocities reach several miles per second.)

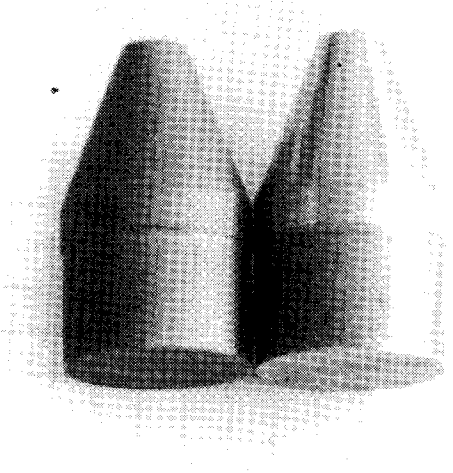
Second, the faster the bullet travels, the better. When talking pistol bullets of reasonable weight, a practical range spans 1000 to 1500 fps.



LEFT DESIGN IS ACTUAL PRODUCTION DRAWING SUPPLIED TO MACHINE SHOP FOR FABRICATION OF TEST A-P BULLETS FROM DRILL ROD.
TESTS OF FIRST DESIGN INDICATED THAT DESIGN ON RIGHT WOULD PROBABLY BE EASIER TO JACKET WITH COPPER AND WOULD FEED RELIABLY.







TOP LEFT: From L to R: 230 gr RN FMJ; another of the same type, different maker; 230 gr FP FMJ; 200 gr JHP; 185 gr SWC; 100 gr JHP. All .45 except far right, .355 for .380 auto.
TOP RIGHT: From L to R: Handloaded 230 FP FMJ; commercial 230 RN FMJ; handloaded 230 gr RN hard-cast lead; handloaded 170 gr steel armor-piercing; finally, same type of bullet that has been..."coated"...with a certain substance. That round no longer exists....
BOTTOM LEFT: Raw steel bullets, fresh from the machine shop, caught in a pose of quiet deadly menace.
BOTTOM RIGHT: Left bullet has been acid-etched w/ferric chloride, producing just the right finish for PTFE coating. Adjacent bullet identical but for etching.

Third, a sharp point helps, up to a...er...point. It need not be needle-like, or commercial products would have points. Instead, they sport elongated cones more sharply angulated than those tipping SWCs. We will use that shape, arbitrarily selecting a tip one-third the diameter of the body of the bullet.

Finally, there must be something to this business of coating the bullet with PTFE, or KTW would not have done it. As we shall see momentarily, the process is complex and demands great attention to detail to turn out consistent product. It may be overkill for civilian needs.

The goal does not embrace piercing the toughest armor possible. A practical endpoint is the ability to penetrate reliably at least one and preferably two thicknesses of "level II" soft body armor. We assume that the felon's body will offer enough resistance after the first pad has been pierced to let the rear pad stop the projectile. We wish to avoid overpenetration. Too effective a unit could prohibit its use. If one's armed and armored assailant were standing in front of, say, a day-care center, and we had ammunition equal to KTW in efficacy, the round would probably penetrate armor and felon, then continue into the center, through most types of walls except brick, injuring or killing innocents. That must be avoided at all costs, even our own safety.

In 1982, before PTFE-coated bullets were nixed where the author lived, he split the project into two steps: Fabricate armor-piercing bullets, but don't coat them, at least until he tested uncoated rounds against soft body armor. Only if the coating proved essential would he proceed to that grim, costly, complex process and coat an entire batch of bullets.

As bullet material we used what is known in the machine trade as drill rod, a hard, tough, tool steel that comes in a variety of uniform diameters, in lengths commonly 12 and 36 inches. It is cheap; tough, yet easily worked with carbide-tipped tools. Machine shops often stock it in several sizes.

Scanning a table of drill rod sizes, we chose the diameter closest to, but skinnier than, the bore of our weapon. We experimented with the venerable .45 auto, whose bullets measure to a true .45 caliber. The range typical of commercially sold FMJ bullets is .450 to .452 inches.

We wanted the fattest stock we could use, but still leave room to put a soft driving band on it. Drill rod is as hard as, if not harder than, the barrel of the gun. To fabricate and load bullets as if they were as soft as copper jacket or lead invites disaster. The breech might explode, since the hard bullet will not deform to traverse the lands and grooves. Here 7/16" drill rod was just about perfect at .4375". This meant we did not have to turn the stock to a smaller diameter, and we had plenty of room for the copper jacket which fit the base only, leaving the steel tip exposed. Photos of the resultant bullets date from 1982.

Here digress a moment to learn about bullet swaging (pronounced SWAY-jing). The process is a proper hobby only of advanced handloaders. It forms bullets by combining lead cores with copper or alloy jackets in unformed states and passing them repetitively through a press that squeezes their diameter and molds their shape into what can be a highly professional bullet. In this case, we sought only to swage a copper cup onto the base and lower half of a steel core. This copper, rather than the steel, would behave properly when it met lands and grooves in the barrel.

It would be dandy if the cup we sought came out of the box in the exact dimensions for our needs. No such luck. We had to trim the length of the cup, or do with a slightly shorter cup than we would prefer. We want the cup to end at the notch on the bullet (see photos & diagrams).

Assume we have cup stock of suitable length and thickness. Insert the steel core into the cup, then pass it through the press with a die that just begins squeezing it against the core. Copper is malleable and ductile, but do not expect to swage it down to .450" in one pass. The press may not take it, or the die may crack. Use progressively smaller dies.

Note that this bullet is too long; that is to say, it protrudes so far from the mouth of the case that it would not load in the magazine nor would it feed. In this experimental work we loaded each round individually. Since the tip of the bullet does not contact the bore, its length was of no concern.

We could, conceivably, have seated the bullet deeply enough to let it fit the magazine, but that would cramp the powder charge, something that might lead to dangerous pressure within the cartridge.

Our finished bullets weighed an average of 170 grains, with jacket. Extrapolating from data available for 185 grain bullets, we found velocities in the 1200-1400 fps range practical; but matching type and weight of powder to bullet and gun through trial and error, a process known as "working up a load," always begins with the lightest practical load. Here we traveled new and potentially dangerous ground, with no comparable bullets to guide us. In many but not all cases, we can apply the same powder charges to commercially produced bullets of the same weight and diameter with little fear of overpressure, assuming we are not working with maximum loads at the start. But this was certainly not a commercially produced bullet.

We were limited in that we had only nine bullets. (At $11 apiece from the machine shop, not to mention the cost of swaging equipment, and that godawful PTFE, realize that the experimenter with greater ambition would invest in a small metal lathe. It would save money in the long run.) Without getting into brands of powder and so forth—it makes all this read too much like an article you'd catch in one of the gun mags—we started with a powder we had used many times with the big .45, with both heavy and light bullets, with consistent performance and no problems with overpressure. We underestimated the charge and loaded each successive bullet 0.5 grains more than the last. During testing, we insisted that we would not fire the next hotter load if the last showed any sign of overpressure. Stone-sober and a bit paranoid, we left for the range.

We had to be careful about this from many angles. First, we would be shooting two Kevlar pads extracted from a Second Chance[tm] "Y" vest purchased in 1978, not exactly a common practice. An off-duty cop would probably freak out at the sight. We chose not to fire if others were present. Second, there was always the chance that the gun could explode, damaging the author. We wore gloves, a polycarbonate face-shield, and hearing protectors. In addition, we kept most of the body behind a barricade. Finally, recall that these were uncoated bullets, perfectly legal in the state where the experiment took place. We did not yet know whether a coating would be needed, and, in 1982, no law banning coated bullets had been passed in the state where this terrible experiment took place.

GRIM RESULTS

With the first shot, approximating grossly from recoil since we had no chronograph, the bullet came out at about 900 fps. It cut most of the first Kevlar pad, but did not penetrate. Predictably, succeeding shots powered by heavier charges penetrated deeper. The experiment proved beyond doubt that these uncoated steel bullets, propelled by a charge of "more than" 8.5 grains of Unique[tm] smokeless powder, would defeat two thicknesses of Kevlar armor. Recoil noticeably exceeded that of hardball. We estimate from recoil that the final bullet made it to 1200 fps at the least.

Do not attempt to duplicate this frightful experiment. Tell an experienced handloader that you fired a .45 round loaded with 8.5 grains of Unique. He might ask whether the gun exploded.

A most instructive assay, perfectly legal, though we would have to have tested coated bullets had penetration failed. And what a relief that we did not. But some might....

PTFE: THE DUPONT METHOD FOR APPLICATION TO STEEL OR ALUMINUM

So what if it seems you do need PTFE coating? You will have to get hold of a fresh batch of genuine PTFE and coat the bullets. This is no simple feat. The author coated bullets prior to passage of a law banning such bullets in his state of residence in 1982. Note the bullet on the end of a line of .45s. This old photo shows one coated bullet at the far right. We disassembled the round and discarded the bullet long ago before state law banned it. We did learn a bit about coating PTFE in the course of the experiment. We pass along these observations purely for informational purposes.

Teflon comes in a variety of drab colors. The maker supplies it as a resin which the user may spray onto the surface, or dip the bullet tip in it. Then you must bake it at a controlled temperature of at least 600 degrees F. Our resin came with details for coating aluminum and steel. You may have to experiment if you have chosen other materials.

Name [redacted]

1. License No. [redacted]	2. Expiration Date 6/6/74
3. Employer Identification No. or Social Security No. [redacted]	4. County [redacted]

5. Class of License and Explosives

- ☐ Manufacturer
- ☐ Importer
- ☐ Dealer
- ☒ Manufacturer—Limited
- ☐ High Explosives
- ☒ Low Explosives
- ☐ Blasting Agents

6. Issued by Assistant Regional Commissioner, ATF, at

Atlanta, Ga.

Copy of License (18 U.S.C. Chapter 40, Explosives)

I certify that this is a true copy of a permit issued to me to engage in the business specified in item 5.

(Signature of Licensee)

PURCHASING COPY

The licensee named herein may use this form, a reproduction thereof, or a reproduction of his license, to assist a distributor of explosive materials to verify the identity and the licensed status of the licensee as provided in 26 CFR Part 181.

[redacted]

Department of the Treasury—Internal Revenue Service
Form 4706 (2-17) Part 2

E. I. DU PONT DE NEMOURS & CO. (INC.)
FABRICS & FINISHES DEPT.
ORDER ACKNOWLEDGMENT

PAGE 1

SHIP TO:
MEDICAL UNIV[redacted] DEPT.OF
ATN;
[redacted] AVENUE

BILL TO:
MEDICAL UNIV[redacted] DEPT.OF
ATN;
[redacted] AVENUE

CUSTOMER ORDER NUMBER
LETTER 5/21/82

DUPONT ORD #	REQ DATE	SHP PT	ORD DATE
[redacted]	820607	001	820601

TERMS
CASH IN ADVANCE

IND	OFFICE	TAX	CUSTOMER CODE	
14	6 6	N	000000000059	481

FOB SP
PRPD & CHRG FRT

LINE#	PRODUCT CODE	PRODUCT DESCRIPTION	SIZE	QUAN	UNIT PRICE
1	958-208	GRAY	01	1	67.00 *
2	T-8595	THINNER	01	1	11.50 *

PLEASE SHIP VIA UPS PREPAID AND CHARGED.
CUSTOMER'S CHECK #343148 DEPOSITED WITH WYNNEWOOD
CASHIER 6/1/82 IN THE AMOUNT OF $82.28.

Copy of DuPont's Teflon[tm] order acknowledgment to author, 1982. RIGHT: "Purchasing Copy" of Federal Explosives License author held in 1974, but which was never used due to prior commitments....

END OF ACKNOWLEDGMENT

* PER GALLON

This gig gets into some right specialized doin's that fairly beg for a graduate degree in chemistry and an isolated workplace where a boo-boo will splash no one but you. Act responsibly. Place your own safety second to others'.

We face multiple unknowns here: What thickness gives optimum penetration? What application method is most uniform? What prep method is best? The answers to these questions are probably proprietary and closely held by makers of coated bullets. (A pause to remind the reader that all this is pure speculation. In addition to being illegal in many venues, be aware that coating bullets with PTFE might infringe on patents. Don't do it.) The KTW people have doubtless studied all that, but, aside from the information unavoidably revealed in patents, have no interest in sharing their stock-in-trade with irresponsible amateurs.

The following data comes from technical sheets supplied with Teflon resin obtained from DuPont in 1982, on application procedures for the 958-200 Teflon-S[tm] and 959-200 Teflon One-Coat[tm] finishes.

First, these instructions apply to aluminum or steel. They may work quite well with other materials, such as bronze or brass, but require changes in procedures. The manufacturer would probably be only too glad to offer help to what it perceived as legitimate research.

Prep the surface of the metal by "grit blasting" in what DuPont calls a "40-50 micro inch profile." An alternative is a phosphate coating.

Note the importance of this step. Coated to a smooth surface, PTFE would peal away under mild friction like paint. The forces generated by impact of a bullet would surely strip the coating and thereby neutralize its value. The coating must adhere viciously to the bullet if it is to cut friction and enhance penetration. To accomplish that, we must give the resin a vast surface of microscopic holes into which it can flow and take hold before curing.

There are several means to produce tiny pits in the metal surface. Grit blasting (sandblasting) is readily available, but care must be taken to ensure uniformity of the process. After seeing what ferric chloride etchant did to a "stainless" steel sink, we decided to try it on one of our eleven-dollar bullets. We soaked one in warm ferric chloride for about 30 minutes. It produced excellent results: a dull, evenly etched surface that, at least to unmagnified inspection and feel, was rough on a fine level, just right to soak up the resin and give it a good bite. The photo shows an etched bullet on the left, an untreated one on the right. DuPont refers to "phosphate coating," which may be the same as "Parkerizing," the name of the process that produces a flat, dull coat on the .45s issued to our armed forces; or another term for acid etching with phosphoric acid. Many gunshops are equipped to perform Parkerizing, though you might get an odd reaction if you asked to have your bullets treated....

If you must coat bullets with PTFE, do not skip this crucial prep. That would probably nullify the benefits of coating.

The machining process leaves oil on the work. Remove it and other foreign material adherent to the surface. Usually, a pre-bake of the material to be coated at 650 degrees F for about 15 minutes will do this, but ensure that the projectiles are physically clean first by washing them with a degreasing agent.

Next, shake the resin mixture thoroughly (the shaker at the local paint store will do), and filter through a cheesecloth or 150-200 mesh wire filter to remove lumps. To apply, the material may be sprayed or coated with and electrostatic applicator (quite expensive just to whip up a few rounds for testing....). Dipping the tip of each round individually may be more practical. DuPont states that the maximum thickness that should be applied per coat is 1.0 mil. The 958-200 series may be applied up to a total thickness of 3.0 mils, in 3 successive coats. To recoat a PTFE surface, it first has to be grit-blasted with 350 grit material to give microscopic holes into which the resin can flow and take hold. You might try manual sanding with carborundum paper if you do not own a grit-blaster.

Once the bullets are coated, let them air-dry 1-5 minutes, something DuPont calls "flashing." Then pop then into an oven preheated to 300 degrees F, for 15 minutes, then transfer them immediately to a second oven preheated to 650 degrees F, for 15 minutes. Literature indicates that you can get by with less time at a higher temp, up to 700 degrees F.

This can be dangerous business from many perspectives. The solvent is highly flammable. That brings up the ugly specter of a fire or explosion. No one has to repeat that the fumes are toxic. Properly ventilate the work area.

The experimenter on a budget might try to get by with a conventional oven and hope for the best. Some kitchen ovens can hit temperatures of 600 degrees F, though that might strain their design limits; or use a lower temperature, say, 500 degrees F, for a longer period.

How can you tell whether your coating process succeeded? Coat a flat piece of steel, preferably of exactly the same composition and preparation you gave the bullets, along with the batch. When the job is done, drip water onto it. If it beads easily and will not wet the surface, you have probably achieved a successful coat.

The proof, of course, lies in performance. You would have to return to the range and try out the deadly fruit of your labor against genuinely formidable armor, say, four pads of Kevlar, minimum, with an appropriate backstop (a foot thickness of tightly packed magazines will do). Only in areas where the practice is legal....

DEALING WITH DUPONT

Fashionable as it is to bash big business, particularly high-profile concerns whose products and inventive genius we enjoy—indeed, cannot do without—nothing said here should be taken as a swipe at the DuPont company....

....but we do have to recognize the idiosyncrasies of large corporations. They have a public image, pay a great deal to maintain a sunny one. And they have all become increasingly conscious of product liability. For example, the February 22, 1982 issue of Chemical Engineering News reported that the company that marketed Tufoil[tm], an engine oil additive, had some problems initially with PTFE micropowder contained in early versions of its product—powder it bought from DuPont. The powder tended to clump. That rendered it less effective than desired for reducing engine wear. DuPont cut them off when it found that what was in essence a DuPont derivative product did not live up to expectations. It did an about-face with the emergence of PTFE surfactants and dispersants, chemicals that kept the PTFE micropowder suspended and prevented clumping. These let the product perform "as advertised" and thereby avoided any tarnish of the fine DuPont name.

We saw the same reaction with "cop-killer" bullets. Apparently wary of bad press, or of product liability, should a cop shoot a felon with KTW ammo, only to have the round overpenetrate and zip through a few bystanders in its deadly path. DuPont cut KTW off its buyer list.

Thus, if you wish to purchase Teflon resin for experimentation with armor-piercing ammo, it will be necessary to appear in your letters or over the phone to be an entity, preferably a firm rather than an individual, with legitimate reason to handle the stuff. Now, the number of legitimate and profitable and patentable uses for Teflon would fill this book. The number of uses for which it has been tried would fill an encyclopedia. Yet DuPont understands that there are still inventors out there seeking new uses for it that will earn them—and DuPont—still another fortune, and for that reason remains accustomed to requests to supply it in small, "experimental" quantities.

In 1982, prior to passage of that grisly spate of laws banning PTFE coated bullets, the author obtained a gallon of Teflon resin and a quart of thinner (use no substitute!) for less than $90, including postage. He represented himself as a medical researcher loath to discuss exactly what type of devices he intended to coat out of concern over patentable ideas, a legitimate and probably recurrent theme. It helped that he had the resin shipped to a large medical research facility, one unquestionably equipped with the fiery ovens necessary to apply the coating, and heavily staffed with chemistry types. He had the presence of mind to use an alias, and had the stuff mailed to this alter ego in care of a secretary employed at the facility.

All told, it was no sweat. Note however that Teflon resin, at least in 1982, had a shelf-life of only 6 months. Heed the manufacturer's expiration warnings.

DuPont's letter to us notes other potential sources of PTFE resin....

DU PONT
ESTABLISHED 1802
E. I. DU PONT DE NEMOURS AND COMPANY
INCORPORATED
WILMINGTON, DELAWARE 19898

EXTERNAL AFFAIRS DEPARTMENT

October 21, 1988

Suzanne [redacted]
Research Assistant
Trentland Press
[redacted]

Dear Suzanne:

I am sorry it has taken us so long to respond to your inquiry on PTFE coated bullets; your letter was sent to several departments before it reached me. In a place of this size, it's sometimes difficult to know who is the appropriate person to handle a given situation.

In response to your question, our policy is still the same: we do not knowingly sell "Teflon" PTFE to makers of armor-piercing bullets. We have made it a practice to strongly reject orders for our product that will be used in such bullets.

Your letter indicated that there are still PTFE-coated bullets around, and I can suggest a few reasons for that. Du Pont discovered PTFE and markets it under the trade name "Teflon". Hoechst, ICI, Daikin and Ausimont also make the material, and while I don't believe they supply the makers of armor-piercing bullets, I can't answer for them on the issue. At any rate, there's often no way for any of us to control where our products go. Our customers don't always tell us what they use the product for, and information they give us may not always be true.

We believe our products contribute significantly to our society's quality of life, and we are highly opposed to our product being used in a way that detracts from that contribution. I'd be happy to answer any more questions you have, and would appreciate knowing about what you publish. Please keep my card for future reference.

Best Wishes,

Janet E. Smith

Janet E. Smith

We do not wish to disseminate information dangerous in the wrong hands. We weighed many factors before deciding upon this discourse, presented as no more than a sordid if intriguing fantasy, and came up with a number of reasons to justify it.

First, it is undeniably exciting. Even those who lambaste television for airing the tape of a KTW round penetrating several Kevlar pads could not help but be fascinated with the pure technology involved. (The same brand of intrigue underlies production and sale, with some success, of a videotape that plays out every gun-nut's most lurid fantasies: machine-gunning a car, shooting a gas tank to see if it will ignite; and, yes, shooting an engine block with KTW ammunition.) To say it bluntly, this species of discussion sells books.

Second, in these changing times, it is wise to be informed of threats to your own security, along with possible countermeasures. (Metal and ceramic inserts for Kevlar vests that will defeat KTW, along with at least one hit from military assault rifle AP ammo, are available to guard limited areas, such as the chest.)

Third, relativity, and not the Einsteinian sort, steps in to justify what was unthinkable 20 years ago, because the world and the people in it have changed. Lt. Colonel North testified that Americans need to wake up to the fact that we live on an extremely dangerous planet. The land of Love Boat has seen and felt less immediate threat than any nation in history. That has led to a softness exploited by a tougher breed of foe. Drug lords from South America and subversives grown at home and abroad play rough. It makes sense to respond to escalating threats with appropriate measures.

* * *

COMBAT PISTOLCRAFT

Owning a pistol and handling it effectively—even competently—are different things. Jeff Cooper's doctrine led to a proliferation of academies to teach the new ways. If you are willing to travel, buy/rent the guns and pay the fees, and do not sport a corrupt background, you can learn to handle the pistol, rifle, or shotgun to whatever level of expertise your desire and pocketbook will stand. Even so staid a figure as Cooper has not been above salting his ads with panache, telling prospective students that they could "join the ranks of the adept." Quite a draw for the snob in us all. Then again, Mr. Cooper is not known to exaggerate....

In addition to pure mechanics of gunhandling learned over a generation of Darwinian selection, one truth to emerge from study was the singular edge only competition gives. Students compete against one another. It just isn't the same, racing the clock. Ego comes into play to motivate us where the clock fails, especially when the other shooter is someone of the opposite sex.

With the rise of skill and personnel to teach it, what a drag that you may not be able legally to carry the heat that will become an extension of your hand, as it were. With cops gunning down kids carrying eerily realistic submachine gun/water pistols, the fat bulge of a heavy service pistol at your side is likely to spook an already nervous herd.

Which is not to say you will travel unarmed, only that getting caught without the right papers could mean a vacation in dreamland. If papers can be had, get them. If they cannot, be damned prudent about when and how you carry heat, and what you use it to accomplish. It is not for wowing dates or settling "Oh yeahs?" in the parking lot. Shooters trained at a proper academy understand that the time between drawing the weapon and firing it reduces to a fraction of a second. There is no point to brandishing the thing unless you have already decided to pull the trigger, and to live with the ominous consequences.

These points make themselves evident to casual students of the scene. We cannot go further with technique of the draw, aiming, firing, reloading, and so on, since only hands-on practice conveys useful expertise.

* * *

RIFLES AND RIFLE AMMO

BIG BULLETS AND LITTLE BULLETS

From sometime in the 1950s until the Vietnam era the standard battle rifle of our armed forces was the M14, firing the 7.62 mm NATO round, known to the civilian sector as the .308. Ballistically the functional equivalent of its predecessor, the .30-'06, but packaged more compactly, it fired a 150 grain FMJ bullet at about 2700 fps.

No one disputes the intrinsic accuracy or power of the round, or the reliability and accuracy of the weapon. Both cartridge and weapon were and remain top-notch. Problems had to do mainly with inability of flocks of recruits to master the heavy recoil, and with the size and weight of weapon and ammo.

Those factors, coupled with a growing sentiment in some quarters that it was unnecessary to devastate a human foe with one hit in order for the assault rifle to accomplish its mission, led to adoption of the present standard 5.56 mm round.

The 5.56 is in essence a .22. In its first 20 years of service, the bullet weighed a mere 55 grains, this compared with 40 grains for the .22 rimfire ammunition you buy at the local hardware store. But it left Colt's 20-inch M16 barrel at a nominal 3200 fps (3000 fps is perhaps more realistic), which gave it adequate stopping power within those ranges where it retained high speed...which weren't too far. The light bullet shed speed quickly, making it less impressive at 150 yards than at 25 yards.

But stories circulated about terrible devastation this round produced on human flesh. While hydrostatic shock probably had much to do with its ballistic effect, the short, slowly spinning bullet proved unstable, prone to tumble once it struck flesh.

Then there was the weapon that fired it: Colt's M16 in military trim, known as the AR-15 in semiautomatic versions sold in the civilian market. To avoid a stink it is perhaps best to say that the weapon drew mixed reviews; yet no one denies that it remedied several drawbacks of the M14. It weighed about 7 pounds, kicked only a third as much as the 7.62 mm, and its smaller ammo meant that each soldier could carry twice as many rounds, disposing of greater firepower and/or cutting resupply problems. Troops forced to carry and shoot the weapon appreciated those qualities, particularly those who came through in the transition, and had genuine problems with the big and powerful M14.

Standard military small arms ammo almost exclusively carries the moniker, "ball." For this we have no explanation other than tradition. Ball ammo for rifles usually means a lead core covered with a copper or brass jacket, with rifle bullets configured to end in a fairly sharp point.

As noted, 55 grains is light for the .22 caliber. Fast out of the gate, the round lagged in the stretch. In plain talk it wasn't worth much, either in accuracy or penetrating power, at long range. ("Long range" is a nebulous concept dependent on many variables. Here we mean longer than 250 yards.)

Though some quarters called for the adoption of a round intermediate between the unwieldy 7.62 and the unsatisfactory 5.56, that latter round has become the United States and NATO standard, so attention turned to fixing its perceived flaws.

The new standard 5.56 mm bullet weighs 62 grains (at least the U.S. version; NATO has adopted the Belgian-designed SS109 at 63 grains; both embody the same basic design changes); is longer than its predecessor and sports a tapered "boat tail," a feature that improves stability in flight; and incorporates a steel insert tip as standard to help ensure penetration. It sacrifices muzzle velocity in the trade, but this has not been cause for concern of military planners. A cutaway diagram, modeled after one printed in Advanced Technology Warfare, shows the internal design. If you plan to use this ammo, note that it requires a barrel with a 1-in-7 twist, this compared to the slower 1-in-12 twist of older 5.56 mm weapons.

Believe it or not, there is a trend toward smaller bullets still. The Soviets have used a 5.45 mm round in Afghanistan, and a 5.56 mm sabot round fires a bullet only 4.5 mm in diameter.

HYDROSTATIC SHOCK AND PRECESSION

FMJ rifle bullets fired from military weapons produce fearsome tissue damage through what has come to be known as hydrostatic shock. A bullet traversing flesh at speeds in excess of, say, 2200 feet per second sets up an extremely violent fluid wave, sufficient to disrupt structure and function in tissue far distant from the path of the projectile. We see little need in military rifle ammunition for the varied shapes and materials found in pistol bullets simply because a pointed, FMJ design has proven optimum to the task.

But there may be more to this than velocity alone would explain. Students of this phenomenon (would you believe that the Government report that discussed this back in the early fifties bore the name of future cardiac surgeon Michael DeBakey?) have commented that such a bullet may leave tiny entry and exit holes, yet puree' the tissue between them.

In addition to hydrostatic shock, precession has been proposed as one mechanism to explain this. Rifle bullets spin with the axis at right angles to the direction of travel. This stabilizes them, like tiny gyroscopes, but subjects them to a second type of spin, known as precession. The bullet "wobbles" about some point, usually its center of gravity. As a point of comparison, note that the Earth turns one revolution every 24 hours. This corresponds to passage of day and night and to spin of a bullet induced by the lands in the barrel. But our planet also undergoes change of seasons due to the fact that it precesses, or wobbles.

If the rifle bullet wobbled much its accuracy would drop quickly; but it spends most of its flight in the low-density medium of air. Flesh possesses far greater density than air, a key fact, since precession is proportional to the density of the medium the projectile traverses. Thus, a bullet with no visible precession in air may gyrate wildly in transit through the body, rending and tearing what it would otherwise spare if it held true. Pistol bullets rarely reach velocities required to bring hydrostatic shock and precessive effects into play.

As a rule, modifying factory loaded ammunition creates some risk of malfunction that could harm the experimenter. Off-the-shelf stuff is mean enough. Those who would experiment with altered ammunition or design their own should go in heavily with professional machinery. And run a patent search. It's probably been done.

AUTOMATIC WEAPONS?

Sound arguments have been made for eliminating the automatic firing mode from the M16 because, in the heat of battle, troops have shown a tendency to spray areas thought to harbor enemy, rather than waiting until they have spotted targets and taken aim.

If the military has considered taking machine guns out of the hands of most ground troops—a need will remain for automatic weapons in the hands of those specifically trained to apply them effectively—what earthly use have you for a machine gun? Apply a practicality analysis to the breed in light of your objectives:

First, these weapons are verboten in some states. BATF will let you buy them, but if you reside in The Wrong State, you're out of luck.

Second, add a fat tax to the cost of the weapon.

Third, what tactical situations do you plan to engage that controlled fire would not better serve, as opposed to hosing areas—which is about all that untrained persons can do with automatic weapons?

Let's admit that machine guns are good for a fine rush and plenty of envious looks down at the range when you cut loose with a 30-round magazine in one long burst that shreds the target and throws up a cloud of dirt and debris. Whooeee! Load up and do it again!

But how many thugs have assaulted you at the range? Where is your automatic weapon likely to be when an

attack comes? (As a "safety" measure, many owners keep the bolt or sear, the parts that make the weapon automatic, in a safe deposit box until they plan actually to take out the weapon and fire it.)

Finally, with all the files that B.B. has on you already, do you need another, one with a red flag on it, that says you own a NFA weapon?

So, OK. You must have one. How do you get one legally?

First, check state and local laws. If you doubt your ability to do so competently, hire a lawyer to find out and report to you in writing (this makes him liable for the consequences of his advice; you might tape pertinent conversations with him). Do not ask the cops. The author phoned police departments in three large cities in his state of residence, asking about permits to carry concealed firearms. All told him there was no such thing. State law says different. If the police do not know about concealed weapons, chances are they don't know about machine guns, or would try to jerk you around by flatly denying your right to own one.

Assuming you clear local hurdles, review the questions on the BATF form. You cannot buy automatic weapons if you're an ex-con, use dope and drugs, suffer psychosis, abuse chocolate, etc.

Third, choose your weapon and your dealer. If he is not in your state of residence, you will have to have him ship the NFA weapon to a local dealer in conventional firearms.

Fourth, file the necessary forms with BATF, and wait. Assuming approval comes through, send your papers to the dealer and collect your weapon. And may God have mercy on your soul....

* * *

SILENCERS

A catchy term, silencer, but one reserved for amateurs. The operative word is "suppresser" or "moderator," since these engines mute and alter the blast of a gun, but do not silence it.

Firearms generate noise containing multiple elements: mechanical noise of hammerfall and primer ignition, "pre-blast"—the sound made by air pushed ahead of the projectile before it leaves the barrel; the blast of propellant gas as it discharges from the muzzle; and, in the case of supersonic projectiles, a sonic crack. In semi-automatic and automatic weapons we must contend also with sound of the mechanism cycling.

In any practical sense, sound suppressors help mute only the blast of expanding propellant gas as it is discharged into the air around the muzzle. Fortunately, this is the loudest and most objectionable noise.

How loud? Military assault rifles can generate speak sound levels of 168 dB at the muzzle. Anyone who has fired an M14 or sporting rifle of comparable caliber understands the frightful intensity of the report. Recall that a decibel is a unit of measuring sound and electrical power. It is an exponential function in which power doubles or halves with slight steps in dB.

Good suppressors typically achieve sound reductions on the order of 20-30 dB, which means that they reduce the peak acoustic power by a factor of roughly 10 to 30. Now, that still leaves us with a peak of well over 100 decibels. Music that loud would break your lease, easy. But a report lasts a fraction of a second, and there is a difference between the way the brain processes impulse noise compared to its handling of continuous sound. As a vital point about suppressors, realize that they muffle sound enough to alter the tactical role of the weapon by making it extremely difficult to locate or even detect by its sound.

A BIT OF THEORY

Humans perceive brief or impulse noise in a different mode from continuous noise. Take the sound of rainfall. We hear it, yet we don't, not due to some change in hearing sensitivity, but by the way our auditory processors operate. And those same processors, through some devious subterfuge yet unraveled, let us slumber through the most violent thunderstorm, a symphony of heavy impulse noise. Yet they awaken us from

sound sleep to the barest creak of the stairs, instantly alert, certain that Jason has returned for his hockey mask.

So there appears to be some threshold at which any type of noise, impulse or continuous, prompts us to attend it. In firearm reports we deal with an impulse that overwhelms all but the loudest background noise, and by its identifiable nature, with the danger implicit, turns us to seek the source immediately.

To illustrate the point, let us say an unsilenced firearm generates a peak muzzle blast that measures 135 dB 15 feet from the muzzle. It lasts only milliseconds, yet overwhelms ambient sound. Its intensity and signature tell us: gun report.

Now attach a suppressor that mutes the report to about 110 dB—and alters its signature. That, as much as the reduced intensity, may explain the sonic camouflage effect of silencers. Even on television, the sound of machine gun fire at, say, 80 decibels instantly identifies the source.

Mental exercise: Record the sound of a pistol blast. Assuming extremely sophisticated and unbelievably powerful equipment, we could play back the sound at the same intensity it was recorded. Now turn down the volume 30 decibels. You will still hear a seemingly loud gunshot, instantly recognized and calling forth that automatic alerting response gunfire evokes. The same does not happen when a suppressed firearm shoots because suppressed firearms do not sound like firearms with the volume cranked down.

Fourth factor: Eardrums are equipped with muscles to soften the sounds of low and high frequencies. Many people can activate them voluntarily (in anticipation of a loud sound; it makes a rumbling sound in your ears). Loud noise activates them automatically through pathways still obscure, but it's a safe bet that sounds that do not activate them stand less chance of drawing attention than those that do. The multiple actions of suppression probably prevent that complex but obscure combination of events.

Intensity aside, the sound configuration or signature of suppressed weapons is foreign to the hearing experience of all save experienced spooks (and cagey ones at that, to have survived silenced assassination attempts). For that reason, it fails to alert us to danger, despite a peak impulse of well over 100 dB. That same awful sound level of raucous music would prompt a hassle for disturbing the peace.

Silencers, genuinely effective ones, date back to Hiram Maxim (the machine gun family). In the 1960s, the Frankford Arsenal tested the Maxim silencer marketed in the early 1900s and found it to be among the more effective of all devices studied, despite its ancient vintage. As seen from a diagram of its internal construction, it not only places a series of baffles in the path of the expanding propellant gas, but the baffles are angled back so as to cause an outward vortex that draws the gas to the edge of the suppressor (i.e., lowers pressure in the center of the tube; pressure determines loudness of the exit sound). The principle was not proven, only theoretical.

Since pressure determines loudness of the blast, lowering pressure should soften the report. The universal gas law (PV=nRT) tells us that pressure varies directly with temperature: lower the temp, and the pressure falls. Reasoning from that equation, suppressor-designers packed the spaces between the baffles with metal screens having high heat conductivity, designed to soak up heat from the propellant gas. This cools the gas and lowers its pressure.

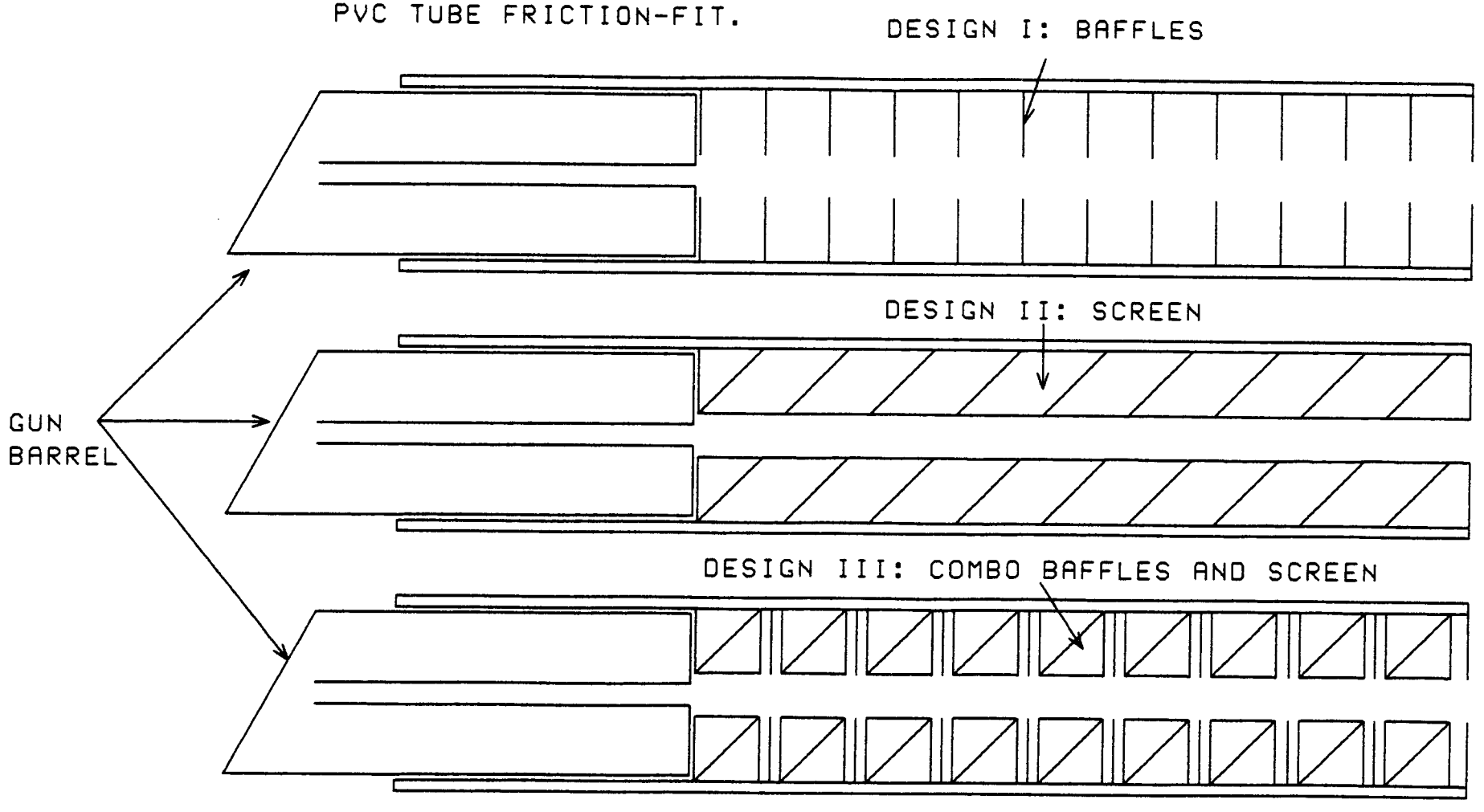
Many designs use both principles, i.e., contain a series of baffles, and pack the spaced between them with metal screens (a copper scrubbing pad in some cases, or steel wool).

Older designs used rubber diaphragms that closed or nearly closed the silencer to gas but passed the bullet. Tests indicate that these dams are not needed and cause more problems than they solve.

DESIGN

Sound suppressors vary in their design, but all share the property of forcing the muzzle blast to undergo a relatively slow and confined expansion within the suppressor, as opposed to an instantaneous release. Most successful suppressors present an expansion chamber on the end of the muzzle. The inside of the chamber

FOR PISTOLS, MOST
EXPEDIENT CHOICE IS RUGER
5" BULL-BARREL .22
W/FRONT SIGHT REMOVED.
PVC TUBE FRICTION-FIT.



SILENCER DESIGN: HOW EASY CAN IT GET?

contains three types of filling: 1) A series of baffles through which the hot propellant gas passes before exiting the silencer. 2) A wire mesh screen. 3) Some combination of the two, i.e., baffles and screen.

Proponents of each design have carved niches for themselves in the suppressor market, and tests have shown their handiwork to be effective. This suggests that punctilious execution of any basically sound design will succeed. The patent literature is filled with designs that claim to achieve swirling and counter-swirling of gasses; use complex venting stratagems; and shape expansion chambers into futuristic outlines that look like they must be effective. Yet, when we buy suppressors from the pros, men whose livelihoods and reputations depend on performance, we find the simple baffle, screen, or combo....

....which means that those with a mind to roll their own should not be surprised that dramatically effective units await at the local hardware store, in unfinished form, as PVC pipe, screen or copper scrubbing pads, metal washers, along with an expanding array of miracle adhesives. Scanning a few proven suppressor designs shows that it would be ridiculously simple to duplicate them without resorting to a machine shop. The diagram shows the 3 basic designs. Common sense and knowledge of physics fills in the details for a particular accessory.

KITS

Those who peruse Soldier of Fortune and its clones noticed that kits of replacement parts for suppressors were offered for sale. Reports have it that some were scams and customers lost their money, while others were the real thing: suppressors that were fully effective when assembled and attached to a firearm. Usually, the only part missing was a threaded tube, or the suppressor for which the parts were designed. This subterfuge brought the ruthless attention of BATF, and kits were not long on the market.

Who made them? Several small companies, some of which began with lone, dedicated craftsmen.

The silencer is nothing more than a barometer of the times. When humans lived in a more violent but paradoxically more civilized climate, the silencer's legitimate use put it on the end of sporting arms and target pistols to be shot in semi-populated areas without disturbing everyone within miles or having to wear earplugs. Today, the idea of inner-city mutants wielding lethal weapons with less noise to them than cap pistols is unnerving. It says much about what we have come to expect of human nature, rather than some innate evil of the device.

Can a private citizen make or buy silencers legally?

Yes, in some states, but there is a catch. A silencer is subject to the same restrictions applied to machine guns and destructive devices (hand grenades; yes, you can own those, too, but it costs $200 apiece since each must be registered; and, of course, you cannot keep the device in the dresser drawer....). Violation brings a fine of ten grand and up to ten years in the joint. BATF has prosecuted a man for taking an inert hand grenade, and rigging it to make a report with about 5 grams of black powder—in effect, a practice grenade. The grenade did not fragment; BATF won. The guy became a felon for that. The bravura of the IRS seems to have rubbed off on its sinister sister service, BATF.

The literature of amateur spookdom is filled with advice on how to make suppressors. Frankly, these devices can be damned effective, but the risk of making a suppressor is prohibitive, unless you notify BATF of your intent in advance, submit to their background check, pay a tax of $200 per unit, and fit every silencer with a serial number, keep records, and subject yourself to the risk of a 3 AM surprise visit from the jackboots. Remember that you have the right to remain silent, cold comfort in a jail cell which is probably bugged anyway....

Lo those many years ago, better days it now seems, one experimenter found himself with time on his hands during a holiday visit home. The rest of the family had taken off for the weekend, and the young and naive hobbyist noticed that he had a 12" length of 5/8" inside diameter cardboard tubing (in fact, it was a Class B roman candle casing). He had a selection of paper endcaps left over from manufacture of aerial report devices, and couldn't help wondering whether this combination might fit together as a makeshift suppressor.

He removed the front blade sight from the barrel of a .22 rifle and slipped the tube over the muzzle. It friction-fit snug and tight. Next, he took 7 endcaps and punched quarter-inch holes in them centered as well as he could, then positioned them at roughly even intervals through the length of the tube.

After remounting this jiffy-popped paper silencer, there wasn't much left but to test it. Instead of going with full power ammunition, which would have meant a trip to the range, with the likelihood of shocked stares and furtive calls to the Authorities, he chose the wiser course of "caps"—partial power .22 loads made by CCI.

Well, the loudest sound was the hammerfall and the sound of the bullet penetrating a stack of old paperback books set up as a backstop in the garage. The report was literally inaudible amidst the other sounds which, alone, would have drawn no more notice across the room than thumbing an old Zippo lighter. Accuracy was as good as he could hold. It was eerily effective, just the sort of thing for serious control work on barking dogs in the wee hours of the morning....

After firing about twenty rounds the thrill wore off, and the tube and its internal baffles found a safe and final haven in the fireplace.

If one found oneself in need of an effective suppressor that could be put together in a flash, less than five minutes, that paper-tube model would take the prize, and it could be made into a non-silencer in the time it takes to run a wooden dowel through the tube and trash the paper baffles (which could be chewed and swallowed in a pinch, when that awful knock came at 3 AM....). Needless to say, we recommend that no one actually attempt to duplicate this youthful and irresponsible experiment that, according to the publisher's attorney, took place so long ago that the statute of limitations has expired and the individual involved needn't fear legal reprisal....

Who uses silencers—and why? Professionals in and out of the government: assassins, police counter-sniper squads, counter-terrorist squads, criminals, and dilettantes. Government personnel are presumed to use silencers to help avoid detection when carrying out assassinations—and let us be frank in saying that assassination serves as much a tool of foreign policy as the sham-negotiations that occupy page one of the Times. Due to layers of hypocrisy in which information has become wrapped in this country, it is necessary to insist that we do not kill people covertly in the national interest, while our enemies kill them openly, invade neutral countries, spread terror, etc.

CBS television figure Dan Rather opined that the Afghanistan atrocity had not caught the minds and hearts of Americans the way Vietnam had. On the other hand, Danno, it saw maybe 0.000001 percent the TV coverage 'Nam got....

Army and Marine sniper teams achieved spooky results in Vietnam using silenced M14 rifles modified for extreme accuracy. Kills at ranges of 600 meters or more were recorded, with a rounds-per-kill ratio reported around 1.3 (i.e., it took 4 shots to kill 3 enemy soldiers, compared to about 50,000 rounds, some said, for regular ground soldiers to wax one enemy soldier). Enemy personnel would march in a line, and one after another they would fall dead without apparent reason. At 200 meters or more, no sound was heard. This unnerved the enemy and made it difficult to spot the sniper. It came to be called "whispering death."

Feats of trained riflemen using finely tuned and suppressed weapons cannot help but astound us, but silenced pistols are strictly close-range weapons, usually arm's length, primarily assassination devices meant for point blank head shots. This is needed because the most common (and quietest) round is the .22 rimfire, a round with poor ability to stop a target unless it strikes the brain.

A sonic crack follows bullets traveling faster than 1100 fps—a miniature sonic boom. Those who grew up after about 1965, except people who live near fighter jet staging areas, may never have heard a sonic boom. This single "boom" or thunder-like sound follows aircraft traveling faster than 1100 fps, the approximate speed of sound at sea level. Any object that breaks the sound barrier in air makes this sound. The very quietest combination of suppressed firearm and projectile are made with .22 ammunition traveling at subsonic velocities. Upscale gunshops stock subsonic .22 ammo for use in target rifles, since it proves just a hair more accurate than supersonic ammo. Beware that it leads barrels of some pistols, though.

What do those who own suppressors legally use them for? And why do they pay a tax per item that may double the price of ownership?

Those who understand the gun-nut mentality, and a bit of that must curse us all, see that the lure of a gadget rises in proportion to its rarity. Some men simply must have them, even though they never use the device. Perhaps some do shoot targets in large basements, and some poach game with suppressed weapons.

Then there are those who make or buy suppressors illegally: organized crime, street gangs, motorcycle packs, and other colorful strata.

Does the average law-abiding citizen have need of a suppressor? In most cases, no. But situations have come and will arise again when a suppressor provides essential advantage for self-defense or just vengeance the law will not offer.

Take the example of a dog that mauled you daughter. You sued the owner and won, but a paltry token sum. And the bum got to keep his pit bull. Fine. A 3 AM trip by his house with a suppressed .22 should settle the question decisively (as to the dog, not the owner).

Occasionally, targets further up the evolutionary scale—yet more savage than any animal—come in for special regard. But those are rare: grave matters of honor, principle, or personal safety. A grasp of suppressors gives comfort that extremes can be resorted to in competent fashion, responsibly, if that grim need arises.

We've seen countless instances of spoiled justice—obvious convictions thrown out on technicalities. Fiction gave us the undertaker whose daughter suffered at the hands of vicious youths. The court suspended their sentences. So the undertaker went to the local mafia Don for justice.

But those with no, ah, Family connections have no Don, and the police have more important things to do. Plaintiff's attorney's yawn over won cases for which there will be no payoff. Wronged parties with no recourse at law find the rage unbearable and take justice into their own hands, sometimes melodramatically in the latest fashion, mass-murder followed by suicide.

One cannot help but speculate that a more prudent approach would be to bide one's time until the stink dies and the perp's guard drops. Then dispatch the felon in a quieter mode.

Societies that tolerate too great a divergence from conformity do not survive as societies very long, and most would deem that rapist who chopped off his victim's arms a bit too deviant; yet he has been released from prison, though no community thus far will take him in. If someone were to use a suppressed weapon to put that rapist out of his remorse, you can bet the police would mobilize all resources to track down the killer....

ARMOR CARS AND WALLS

The material that forms the basis of most bullet-resistant windows is known as polycarbonate plastic, marketed by General Electric under the trade name, Lexan[tm], and by other firms under their own trademarks. This material can be had commonly in sheets of four by six, or larger if you want to custom order, and in thicknesses of a half-inch, more than adequate for stopping most handgun ammunition.

For vandal-prone windows it is the material of choice, and can be had in a version that is about as scratch-resistant as glass (we now have plastic-polishing kits to take away those unsightly scratches). It may deteriorate through prolonged exposure to ultraviolet rays in the sun, even now rising ominously as the ozone layer wilts.

Despite its amazing impact resistance, polycarbonate shares the drawbacks of other plastics. It burns, meaning that a torch will make quick work of it. It can be drilled quite easily, and one hole big enough to admit the blade of a saber saw means that a man-size opening is about five minutes away. Polycarbonate has been put forward as a means to harden house walls to bullet impact.

One of the better places would be the front door, if you anticipate shots fired through it.

It can be plastered over, drilled, painted, and wallpapered. Dealers for the stuff in large sheets are usually found in cities of more than 200,000 population, and you may have to order custom sizes or thicknesses.

What about sheets of Kevlar? They will serve; but make a cost comparison, and ask, if a vest of about two sq ft costs $200, what will a 32 sq ft panel cost? And what about handling? Limp Kevlar would have to be supported at key points, unlike a sheet of polycarbonate, which could simply be propped up, or secreted in slots prudently made during construction of the house or mobile home.

* * *

TEAR GAS

Any decade ushered in by Klute cannot help but consider itself chic. The seventies were a trendy time for personal tear-gas weapons. The rise of feminism brought with it the need for a portable weapon women could use to thwart muggers and rapists; or, just on a whim, teach cheeky and self-satisfied chauvinists a lesson. Due to the leftist pull of feminism, guns and other fascist (i.e., effective) weapons did not qualify. So hand-held gassers filled the need by fashion and default. What an irony that the police types who gave Mace[tm] its first surge saw it go on to become the darling of liberals. Political extremes oppose possession of all weapons by anyone but Big Brother...and themselves, of course, since they aim to step up to the top spot....

Two compounds are commonly available as "tear gas." The first is called CN, which stands for chloracetophenone. One brand of spray dissolves it in the propellant that squirts it out of the canister. Its maker maintains that the propellant dissolves fat on the skin of the assailant, and through that means exposes nerve endings to the CN, which makes it more likely to hurt.

The second type, the varsity of tear gasses, is known as CS (or orthochlorobenzal-malononitrile). When riot-control cops get serious they turn to CS.

Both types cause intense burning of exposed skin, ten times worse on mucous membranes and a thousand times worse in the eyes. If inhaled they induce coughing and a sense of constricted breathing. The literature indicates CS to be more pitiless than CN.

One gun mag reported a test of CN tear gas. An experienced combat handgunner let himself be maced straight in the face, then drew his weapon and fired controlled burst, hitting a standard combat target. A surprise splash of CN might give you time to flee a casual mauler in an open space, but this non-lethal defense will not stop the determined adversary. And think if he had tried to duck the burst, wore glasses.

Streetwise punks can duck or cover their eyes in a flash. Most of them laugh when the imminent victim brandishes a gas canister, since they recognize it as a non-threat that gives the user a deadly false sense of security.

Other types of gasses are available to highly placed powers. One is known as sternutator gas. It induces such severe nausea and vomiting that victims feel as if they want to die. Mean stuff. Better stock up now to gas your brokerage after the next crash. One rumor making the rounds in Frisco in the wake of Watergate had it that the security team at Democratic National Headquarters planned to plant sternutator gas in quick-release canisters to catch, and presumably punish on the spot, the second wave of buggers that would take Liddy's place. We put no stock in rumor....

* * *

PERSONAL LASER WEAPONS?

You can buy kits to make lasers in the shape of ray-pistols right off the set of Forbidden Planet. What end they serve is not clear. Their laser light might conceivably cause momentary blurred vision if it accidentally shown straight in the eye of a felon, but not much else.

For the present, genuinely effective laser weapons remain experimental and bazooka-size, exclusive of their power packs. One-shot chemical lasers might do without the power pack, but one shot is not much....

And yet, there can be little doubt that this will change. Science fiction writers saw the laser light long before it shown in Charles Townes' lab. The rise in laser efficiency and strides in density of energy-storage devices claimed for magnetic projectile weapons will lead to ever smaller laser weapons.

Visible lasers have found greater application as add-on aiming devices for conventional firearms. With a properly aligned laser—the bullet drops in flight but the light does not—it's a matter of putting the light on the target and pulling the trigger. That ruby-red glow is something of a giveaway, though, and those who know its significance would probably seek to neutralize it without further provocation....

* * *

ELECTRICAL WEAPONS

High voltage has seen its share of press lately. First the hand-held shockers, followed by the cry for their banishment. Then, in France of all places, where cabbies wired their back seats with 50,000-volt jolters designed to thwart robbery or murder (several cabbies had been killed by passengers prior to the shocker move). Some vehicle anti-theft systems make the driver's seat a true hot seat unless the right code is entered quickly.

How do these devices work, mechanically and physiologically?

Physiologically, note that the human nervous system is composed of two main parts, the central nervous system consisting of brain and spinal cord; and the peripheral nervous system, consisting of nerve after it leaves the spinal cord. It all runs on minute amounts of electricity.

Ever see someone have a seizure (epileptic fit)? What you witnessed resulted from most of the neurons (nerve cells) in the brain firing their electrical impulses at once, in disorganized fashion. Electricity can indeed induce one of these seizures if applied to the brain. This is done intentionally in electroconvulsive therapy given for severe depression. (TV People shudder and call it "shock treatment," but it remains the treatment of choice for severe depression unresponsive to drugs.)

The human heart is mostly muscle, but it, too, has a nerve system that runs electrically. Executions carried out with the Chair do two things: 1) Immediately render the victim unconscious with a huge jolt through the brain, just as if he were having a seizure. 2) The charge gets to the electrical system of the heart and leads to fibrillation, which amounts to stoppage. The condemned man dies of cardiac arrest.

The peripheral nervous system carries impulses to muscles and tells them what to do. Also, it carries impulses back to the brain, to keep it informed of temperature, position, vibration, touch, and pain.

Electricity whose direct effects do not reach the brain generally lead only to disrupted feeling at the point where the juice is applied. This can be beneficial: witness the Tonic Electrical Nerve Stimulator, or TENS, which fools the brain by drowning out pain impulses the way the sound of rain on the roof masks that party next door. Or it can be damned irritating, like that sudden jolt on a cold, dry day after scuffing your feet on the carpet then grabbing the doorknob.

Deadly electricity, the kind that electrocutes, delivers substantial power. The juice out of the wall socket is plenty to stop your heart. But that's only about 110 volts. They key lies in the amperage, or current. The wall socket will pull 15-20 amps before the circuit breaker kicks in.

Compare that to the spark you get from the doorknob. Though harmless, it can measure tens of thousands of volts. The current measures bare millionths of an amp. It's enough to jangle your peripheral nervous system, and thereby cause pain, but its high voltage/low current properties keep it out of the boiler room.

Electrical weapons, at least those designed to incapacitate and not kill, employ high voltage, infinitesimal

average current; peak current is quite high for some weapons, but it lasts only microseconds. Fifty thousand volts pulsed 20 times a second overrides the normal sensory input and motor output of the peripheral nervous system. The victim, if standing, will usually flop instantly to the ground because his brain can no longer tell his legs to hold him up, and his sense organs no longer tell the brain what it needs to know to give the right signals. It is an unpleasant experience, but permanent damage never occurs from the shock itself. Bones can break in the fall, and a man with a weak heart could have a heart attack from the sudden, ugly adrenalin rush the jolt triggers.

We've had cattle prods for decades. They got the doggies to move along but didn't hurt them, all with about 7000 volts. The riot years of the sixties saw cattle prod circuitry incorporated into police batons in several modes, some designed to keep the baton from being taken away from the officer. Still, cattle-league voltage.

TASER

The early seventies gave us Taser[tm]. This weapon is still around, and seems to have been the spawn of the early skyjack era as one potential solution to stopping 'jackers without shooting innocents or blowing out a window of the jet a la Goldfinger.

Taser looks like a flashlight designed by Salvador Dali. It indeed contains a flashlight, but beneath that it holds two replaceable cartridges that shoot a pair of wires, each with a tiny barb on the end to make it stick to clothing. It does not need to penetrate flesh, since its 50,000-volt charge will easily leap to the victim's skin. And when that happens, the victim flops helplessly to the pavement. Descriptions of tests stated that this put a martial arts expert instantly on the floor, and did the same to a baby bull (did the ASPCA approve that test?).

Taser is right conspicuous, a known sight to street slime who would casually step out of its 15-foot range at the sight of someone brandishing it, call in reinforcements before taking you down. Taser makes the typical liberal assumptions that things happen honorably and predictably, as if you were obliged to give an attacker the option to depart. Maybe Bernard Goetz was right.

Literature BATF sent us detailed past controversy over whether early versions of Taser were firearms. Some were deemed so, and some states restrict the sale of Taser as if it were a gun.

HAND-HELD SHOCKERS

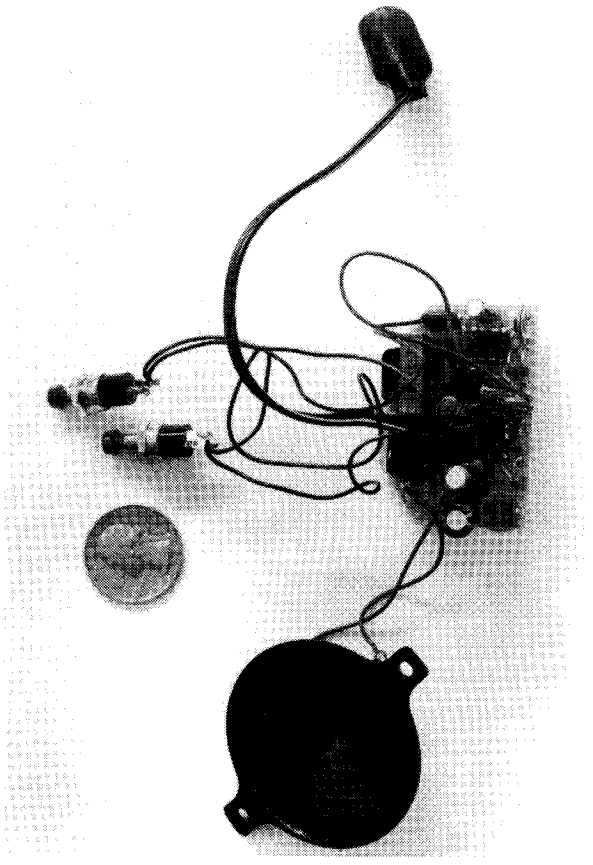
The latest wave is the 50,000-volt hand-held pulsed shocker. Information Unlimited sells plans and kits for 100,000 volt models, as well as devices that discharge considerably more current that ordinary shockers. These units are touted as anti-animal weapons.

These use the same principle as Taser, but eliminate the two-shot limit and uncertainty of a miss at the expense of distance: you must place this weapon in contact with the attacker's body for it to work. Its arc easily penetrates clothing. The maker of the Nova XR-5000[tm] stun gun recommends that the most effective means to apply the unit is to hold it at upper shoulder/neck, under the ribcage, or on the upper hip, preferably over muscle rather than fat. They warn that the attacker will begin to fall as soon as the unit is switched on, and further caution that too brief a jolt will let the assailant rise immediately and continue the attack if he's still of a mind to do so. They indicate that a prolonged application of 5 to 7 seconds usually leaves the assailant dazed enough that the user can escape.

The Nova birthed a number of clones, whose voltages range from 35,000 to 50,000. Nova is designed to work only with a 7.2-7.4 volt nicad battery, not a full 9 volt battery or an 8.6 volt nicad. They market a similar product called "Spirit" that uses only a lithium battery.

There was talk of "special" shockers for police that pulsed the voltage at a higher rate. The lure for police use lay in its power to incapacitate rowdy drunks and dope-fiends, who had shown resistance to tear gas and saps. Literature supplied by Nova states that the unit leaves only mosquito-bite-like marks on the victim's flesh....

It seems nowadays that concepts and products follow a cycle: introduction with the intent to let legitimate



LEFT: Nova XR-5000 Stun Gun, 50,000 volts arcing at the touch of your thumb. Author applied prongs to his thigh, triggered unit. Definitely not a toy; exercise never to be repeated. RIGHT: Innards of Information Unlimited's "Invisible Pain Field Generator."

users defend themselves against mutants. Use of product by police and then civilians with good effect. Use of product by criminals. Misuse of products by laymen and police.

The portable shocker proved effective, if a bit prone to abuse. Police work demands a degree of self-control that is unrealistic to expect from human beings. With no witnesses around, and with a violent subject who just bloodied his nose in the arrest-brawl, what human, even a sworn peace officer, could resist letting the ol' shocker run for a few minutes, now that the bastard is in cuffs? It has been reported that some police used their hand-held shockers to torture suspects. Shades of South America....

Each new menace spawns a countermeasure. Goons with guns led to body armor. Now we have clothing with built-in wire mesh or impregnation with carbon, like ignition cables, to short-circuit the 50,000-volt shocker...or have your old lady sew some aluminum screen in your jacket for nighttime streetwear....

You can get these devices through the mail for $35-$80, depending on model, features, and the nicad battery that seems always to be part of the package. Some states and municipalities have outlawed them, as with tear gas.

ELECTRIFIED CARS AND OBJECTS

One feature of modern-day armored limousines electrifies the hull with about 6000 volts so as to discourage kidnapers and terrorists. Yes, electricity has many uses in the spook business.

The genuinely determined homeowner can have his alarm trigger a relay that will electrify selected objects, making them theft-resistant and administering instant punishment to the thief. Information Unlimited sells detailed material about this. Careful, though. Remember that lawsuit (the report may have been apocryphal) of the burglar who sued a family whose house he'd just burgled, after he fell out of a tree in their yard and broke a leg. He is said to have won.

The same logic, or lack of it, would apply to electrified doors. Courts might regard this as a trap, although you would never set a lethal trap like the one that got national media attention. That poor fellow was justly acquitted, but might have avoided all the bad publicity if he had used, say, a fence charger he could have bought at the local hardware store for less than $20, instead of rigging the grill up to house current.

* * *

BB SUBMACHINE GUN

Believe it or don't, but a graduate student felt so bored with his studies in 1976 that he ordered the now-famous Larc International BB submachine gun. Guns & Ammo magazine had given it a splendid review as that rare something to bring back the kid in us all.

Well, that early model leaked a bit, and the gizmo that held the freon can (destroys ozone, right?) looked like a Rube Goldberg reject. But when it was working, it was something. The BBs spewed out so fast they hissed. You could aim at a stop sign thirty yards away, let fly with a half-second burst, then cower from the clang as a solid stream of copper-clad death slammed the target.

In general, shooting glass targets is a no-no; but at the dump, where there is no chance of anyone getting cut, this fiendish little gem comes into its own as a time-killer/bottle-smasher.

Time and dollar-cans of freon seem to pass instantly when you're having fun. Rests are a must to let the freon reheat to bring up the pressure, since each burst cools it rapidly. Aficionados of the unit spray-paint their freon cans black so as to absorb heat quickly in the sun. Eye protection is a must, and the weapon should be given the same respect as all firearms. Get the long-barrel model for higher velocity.

What practical use has this, other than fun? When dogs need punishment short of death for digging up your petulia bulbs or whatever, the Larc "Korrector" should do nicely, and leave the animal alive to suffer its welts overnight. At least you'll sleep soundly....

* * *

BODY ARMOR

It's been said that body armor was made to defeat the pistol bullet. Against ammunition available off the shelf at your local gun shop it has succeeded. What made it all possible was a chemist working for DuPont who came up with a synthetic fiber now known under the name Kevlar[tm]. Kevlar armor is effective to the point that most police officers on the street are likely to be wearing a 2.5-pound vest woven of this unique fiber. It displays the property of distributing applied force among its molecules as it ruptures, and that apparently accounts for its incredible strength and impact resistance. Scan virgin Kevlar through a microscope and it looks like any other synthetic fiber. But view fibers from a vest struck by a bullet, and we see that what were few have split into thousands. This redistribution of force provides resistance to penetration.

Naturally enough, Kevlar vests found first application in police ranks. Few other occupations expose the employee to gunfire as a daily hazard. But cops weren't the only ones who got shot, and soon assassination targets, or those who saw themselves as such, could buy the vests. Finally, ordinary citizens along with the criminal element masquerading as good guys added body armor to their repertoires.

The utility of a genuinely effective bulletproof vest could not escape the notice and fiendish ingenuity of the criminal subculture. We found holdup artists, bank robbers, assassins, and—most spectacularly—drug gangs operating in southern Florida using it to advantage.

In response to the non-threat, in any practical sense, posed to domestic law-enforcement by KTW ammunition, the Kevlar vest was beefed up first with a metal and later a variety of ceramic inserts that would stop it. A sad testament that the protection is needed in some locales, since the Eastern Bloc supplies terrorists with armor-piercing 9 mm rounds for its airport massacres....

An interesting and sometimes ignored benefit of body armor has been the chest-protection it affords officers involved in automobile accidents that would otherwise have led to serious thoracic injury.

* * *

ROCKET WEAPONS: THE BIG AND THE SMALL OF IT

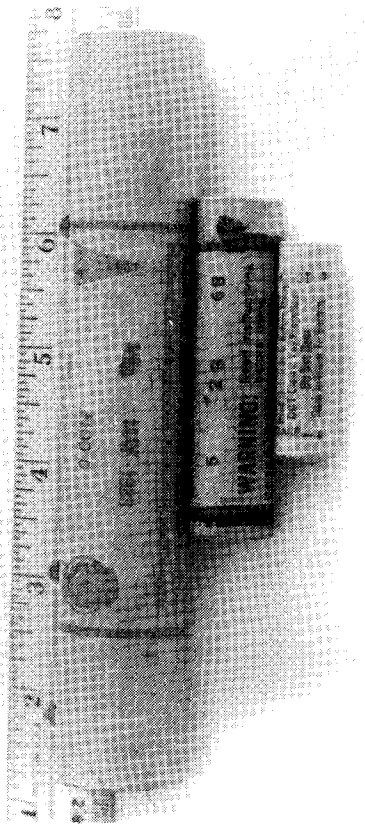
Many years ago—we can't shake the sixties mentality—Life magazine ran a piece on Gyrojet: a pistol that fired sharp, deadly, finned rockets smaller than a cigarette. In fact, rumor told that the missiles could be concealed in cigarettes and fired from those carcinogenic launchers. The rounds reached speeds of thousands of feet per second, given sufficient length of travel, and were thus capable of wounding seriously by hydrostatic shock. They proved ineffective close-in weapons, fired as they were from pistols. At 3 feet they had not achieved speed enough to do serious harm. Thus, they failed in the pistol's role of close-in defensive arm. The piece in Life ran a photo of a Gyrojet missile fired underwater. Some parents of soldiers stationed in Vietnam bought them for their sons, thinking they were giving them a super-weapon of sorts.

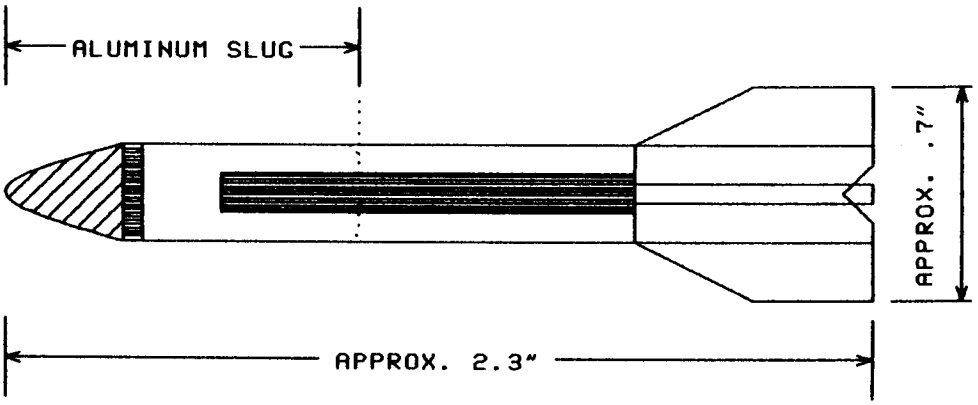
THIOKOL LILLIPUT

But Gyrojet, though extinct, saw and still sees so much press that it has taken on the air of myth. Few outside the rocket establishment know of another spawn of the same era, dubbed "Lilliput" by its maker, Morton Thiokol Corporation.

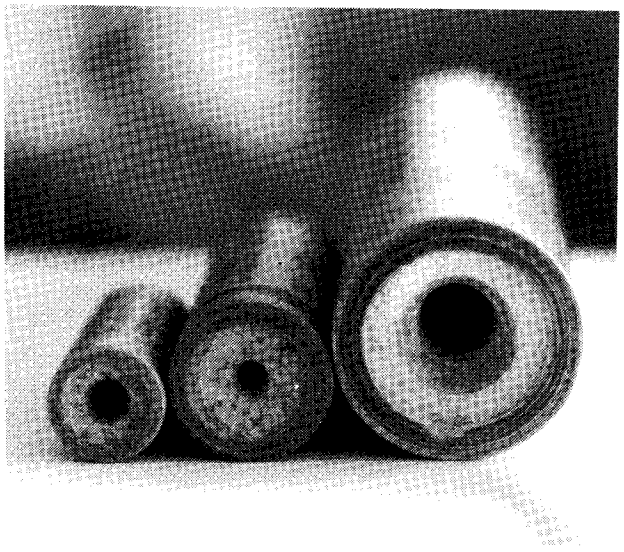
The 1964 Lilliput was probably the smallest professionally engineered rocket ever, even though it never saw full production. The missile, shown in a diagram drawn after reprints of the original production drawings, measured about 2.3" long by 0.305" (body) diameter. It bore an aluminum tip, weighed a few grams, and reached top speed of 2000 fps in its burn-time of 0.219 seconds. The maker pegged its effective range at 100 yards.

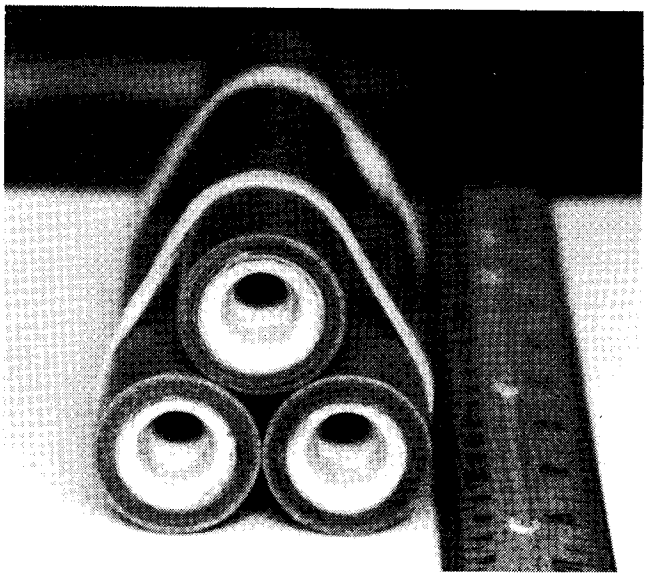
Designers saw it as a salvo-fired device, all rockets ignited in a bunch and directed to cover a kill-zone, much like a Claymore mine.





SEMI-SCALE DRAWING OF THIOKOL "LILLIPUT," PROBABLY THE SMALLEST PROFESSIONALLY ENGINEERED ROCKET EVER, THOUGH IT WAS NEVER DEPLOYED IN A WEAPONS SYSTEM.
DRAWING APPROXIMATED FROM ORIGINAL PRODUCTION SPECS.





TOP LEFT: 20 years of model rocket engines. Large F-class engine manufactured 5/88. Middle engine, a B6-4, from 5/68. Smallest engine is one of Estes' T-series, suitable for flinging small warheads away from a mother-munition. TOP RIGHT: Semi-scale diagram of Thiokol Lilliput. BOTTOM LEFT: Business-end view of A-, B- and F-class engines. BOTTOM RIGHT: Rubber bands hold deadly F-class cluster in place while epoxy hardens to form propulsion unit for serious rocket weapon. See text.

For whatever reason it never reached production, and one of few remaining prototypes, perhaps the only one, lies yellowing with age in a desk drawer at Thiokol.

That reminiscence of Gyrojet and Lilliput cannot help but resurrect studies of model rocketry in those who grew up in a decade that swung to the note of "Purple Haze," as if seeking some fresh and desperate fluid to flush the Sputnik syndrome from the blood.

HOMEMADE ROCKET WEAPONS

So many texts omit purpose and suitability from the equation when figuring design and deployment of homebuilt rocket weapons. There is little doubt that, with proper design and a great deal of testing, effective rocket weapons lie both within the realm of possibility and within our grasp. Yet it seems that the only nonmilitary literature dealing with rocket design is that of model rockets, flimsy units intended to fly straight up, forbidden ever from carrying destructive payloads. Rockets could be used to loft charges over a distance, just like a mortar, which would probably be the better choice.

But what comes to mind when we think of rocket weapons are bazookas, light antitank weapons, Panzerfausts, and the Eastern Bloc's ubiquitous and rightly feared RPG-7, recently upgraded by the Egyptians to defeat a mind-boggling 500 mm—19.6 inches—of homogeneous steel, this compared with 260 previously. These weapons loft an explosive warhead at slow pistol bullet velocities, with essentially no recoil, and with fair accuracy in trained hands.

Two questions: 1) Can we fabricate rocket weapons effective enough to justify investment in this complex delivery system? 2) Will we meet situations that call for rocket-propelled weapons?

The answer to the first question is yes. The answer to the second question cannot escape limbo. It is hard to dream up scenarios in modern America wherein Mr. or Ms. Doe must resort to a homemade RPG. But the same applies to much of spooklore. Situations that call for expertise in it seldom announce themselves in time to let us prepare as we might wish (witness the author's two demure encounters with real-world lock-picking). For discussion purposes, assume that conditions exist, out of whatever unlikely scene, that justify the risk to maker, user, and bystander of rocket weapons.

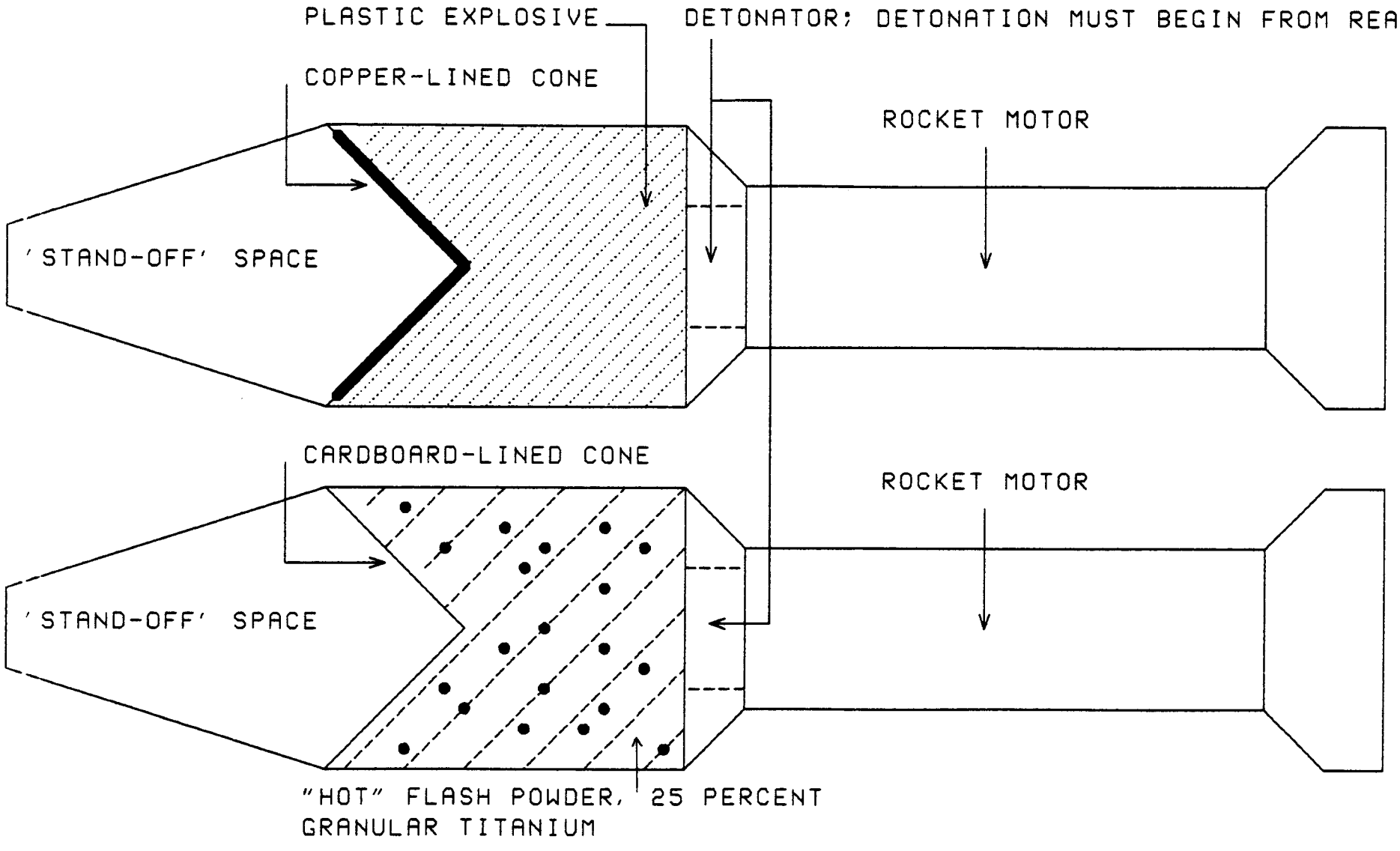
Model Rocketry touted its enviable safety record, safety being important when kids get to monkey with missiles traveling at more than half the speed of sound (and that was 20 years ago, with the old breed of class B engines; class G and beyond have pushed model rockets through the sound barrier). That fine record surprised few, since the missile spent its time and velocity traveling straight up, every millisecond taking it further from potential collision, then floated back to earth on the wings of a parachute or streamer.

The model rocketeer's pledge, or safety code, or whatever it was, provided that the practitioner would never aim the rocket at any target, anything on land, nor attach any sort of "pyrotechnic warhead" to it.

The fact that the pledge embraced those taboos may have meant that somebody, somewhere, sometime had done those things with harmless model rockets. In fact, the author could not resist the temptation to shoot a rocket at a ground target. The pledge had given him the idea. In 1966 he set the launch rail about ten degrees from horizontal, slid an Estes Industries Astron Streak that was ready for the trash anyway down the rail, loaded an engine, an A8-3 as it now seems, and fired it at a long-abandoned caretaker's shack in a vacant lot. Wellsir, the missile flew about ten feet before it zoomed straight into the ground, the rocket disintegrated, and there endeth the lesson. Further testing seemed pointless.

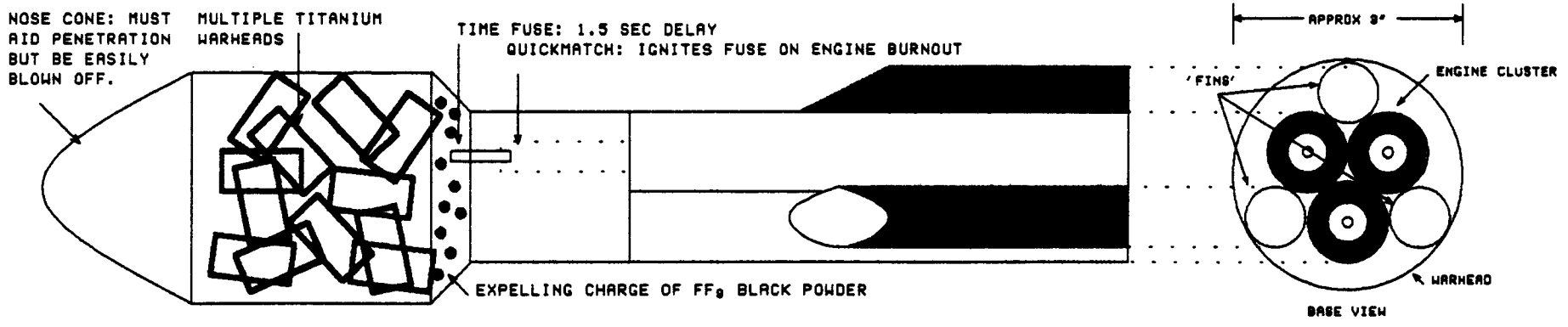
Which brings us to the issue: Can we convert model sport rockets with any success to genuinely effective weapons?

The first answer is, not without breaking the law. Model rockets designed to travel straight up can carry a maximum fuel load of four ounces, more than enough to make an effective weapon. Trouble is, according to law, once you aim an otherwise guileless model rocket at a ground target, or once its fuel allocation exceeds four ounces, it enters the forbidden zone of Destructive Devices. You will endure the same rigmarole that haunts silencers and machine guns to fool with rockets as weapons. Of course, as long as you maintain the appearance of sticking strictly to vertical travel you can pass yourself off as a model rocketeer.



158

TOP: CONVENTIONAL SHAPED-CHARGE WARHEAD BASED ON HIGH EXPLOSIVE. BOTTOM: SPECULATIVE LOW-EXPLOSIVE DESIGN BASED ON PRESUMPTION THAT EXPLOSION WOULD FOCUS JET OF BURNING TITANIUM PARTICLES FORWARD, AS WELL AS KNOWN EFFECT OF SIDE-DISPERSAL OF THEM.



SPECULATIVE DESIGN BASED ON 3-ENGINE CLUSTER (F-CLASS) AND MULTIPLE TITANIUM WARHEADS EXPELLED FROM MOTHER-MUNITION.

Second, not without endangering yourself or bystanders. The rocket weapons discussed shortly could strike targets over a mile distant under some conditions. That mandates fireproof testing grounds so far from innocents that there will be no chance of harming anyone save the rocketeer, whose actions silently condemn him to travel at his risk.

Third, about the only components usable off-the-shelf for serious weapons work are the engines. These offer reliability, consistency, and a great deal of safety, compared with making one's own engines from scratch. (Not that there isn't something to say for making one's own engines. The level of extra-pyrotechnic interest in this aspect of rocketry has burgeoned of late due to R&D and marketing of tools and instructions from Impulse Reactions and Teleflite). Still, rocket weapons fairly demand quality control which may lie beyond the reach of all but the most dedicated and well heeled researcher.

Paper body tubes, balsa fins and nose-cones might serve well for scale testing in research, but any terrorist or paramilitary unit that came under fire from such flimsy weapons would laugh them off, then turn the infrared scanner to discover your launch site and dispatch you with a single bullet fired from a night-scope-equipped sniper rifle. No, it would not do to tease a serious foe with kiddie weapons.

What do we see in serious, unguided military rockets, exemplified by the U.S. Army's LAW (light antitank weapon) and the USSR's RPG-7? A very special time-thrust curve: These rockets have burned out by the time they exit the launch tube, about a foot of travel in the case of the RPG-7, whose warhead sticks out the front of the launcher. Only its engine nestles in the firing tube. Their burn-times measure a fraction of a second. The military learned early that rockets which continued to ride a tail of flame after they quit the launcher had a grisly way of cooking the unprotected firer's face. Our Stinger shoulder-fired guided missile sports a two-stage motor. The first burns a fraction of a second, enough to clear the rocket from the launcher, then a sustainer engine ignites. In essence, rocket-propelled grenades accelerate to the speed of a slow bullet without generating recoil.

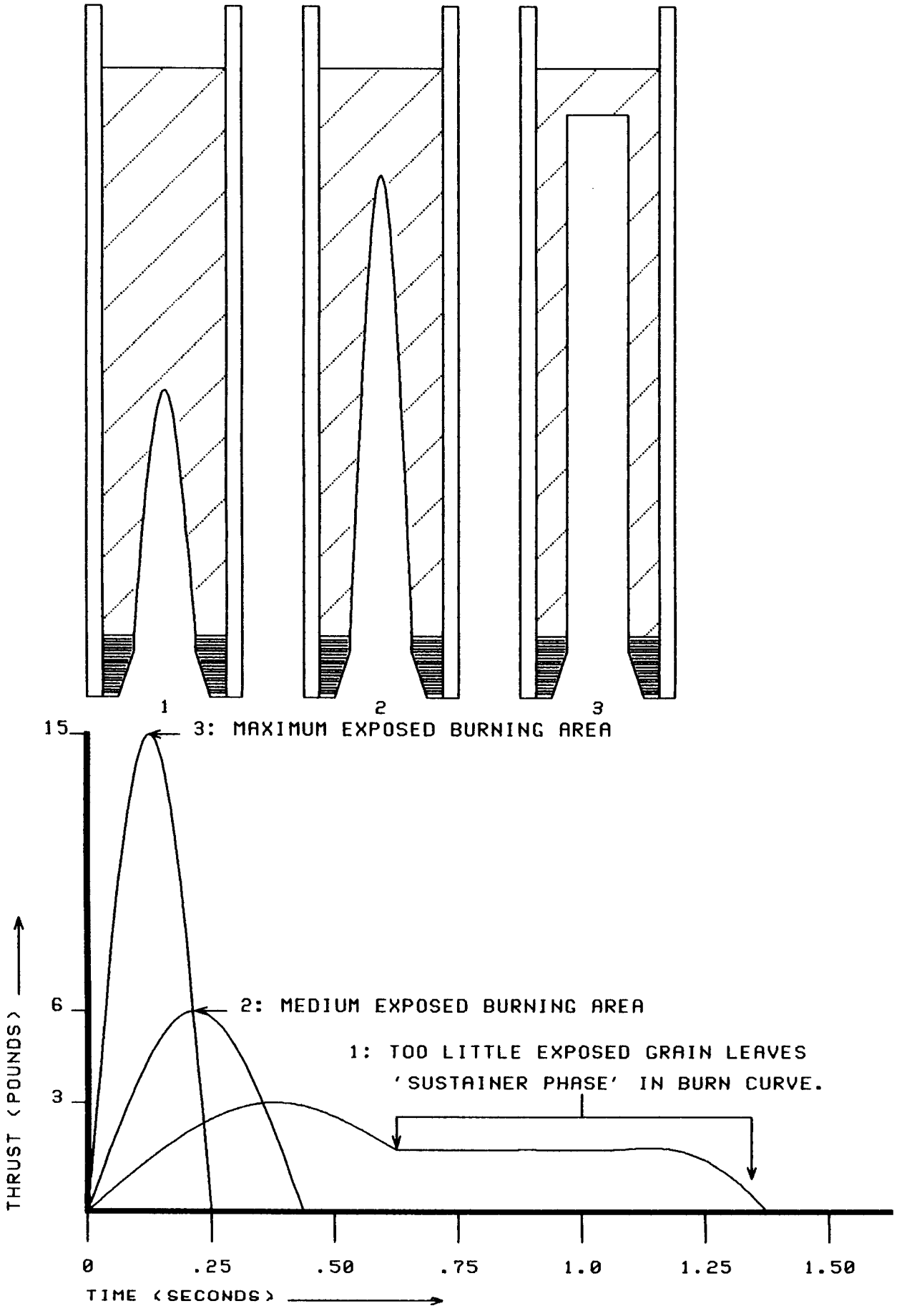
Britain's Starstreak missile exemplifies the third generation of portable antiaircraft weapons, this two-stage device tipped with three independent, maneuverable, explosive darts.

Return to this matter of time-thrust curves. No ex-model rocketeer can forget those wonderful illustrations provided in Estes Industries catalogs, back in the sixties, of two basic curves. The first type gave a medium initial surge of thrust followed by sustained thrust at lower level. That type would not suit the portable rocket weapon due to backblast and the laws of physics. The physics involved in predicting the behavior of a projectile that continues to accelerate after being fired horizontally rather than vertically is extremely complex. An unguided rocket fired essentially parallel to the ground begins to drop as soon as it leaves the launcher, no matter that it may be accelerating. Effective unguided rocket weapons toss their loads upward slightly, such that aiming is much akin to aiming a very slow, heavy bullet.

Thus, as we shop the pre-fab engine stock for raw material, we seek a short, sharp thrust, like that shown in the diagram. Eventually, we will resort to the most powerful engine of this type available, but we could well use smaller engines with similar burn-time for feasibility testing before working up to engines that cost five bucks apiece. At this writing, you can get 3 A-class T-series engines for less than a buck apiece by mailorder. They're dandy for scale testing. Black-powder-based F-100-class engines will loft serious warheads, particularly in clusters of 3, but go for five bucks each.

This type of engine bears a bigger nozzle coupled with a center burning grain. The propellant, most always simple black powder compressed into a hard grain in a hydraulic press, burns in a split second along its large surface area. Before Estes Industries changed to the metric system to designate its engines, the fabled B3 series reigned as king of the thrust peaks: about 9 pounds in a total burn time of 0.35 seconds. Launching a small rocket loaded with a B3-5 (5 seconds of smoke before the parachute deployed) felt like a 110-decibel sneeze, during which the rocket somehow vanished from the launch pad and its smoke trail materialized at 2000 feet....

If memory serves, Centuri Engineering, a now-defunct company formerly based in the desert southwest, sold engines with a 25-lb peak thrust, center burning grain type, circa 1968, an engine in the F-class. Total impulse delivered by an engine doubles with each successive letter. For example, a C engine delivers four times the impulse (thrust times time) than an A engine. An F engine is 16 times as powerful as a B engine. This is adequate to the needs of weaponry.


1
2
3
15
3: MAXIMUM EXPOSED BURNING AREA
6
2: MEDIUM EXPOSED BURNING AREA
1: TOO LITTLE EXPOSED GRAIN LEAVES
'SUSTAINER PHASE' IN BURN CURVE.
3
THRUST (POUNDS)
0
.25
.50
.75
1.0
1.25
1.50
TIME (SECONDS)

Engines currently in the Flight Systems, Inc. inventory include a few that could serve in serious rocket weapons. These are F-class engines. The major contender is the F100-X, with a peak thrust near 30 pounds. The unit measures 158 x 27 mm, the largest engine in the photo set. It could be clustered three or four in a launch tube three inches in diameter (cardboard or PVC pipe appear most readily available and least costly).

Ignition of clusters would have to depart somewhat from customary model rocket practice, which places an electrical igniter in the nozzle of each engine. Naturally, some igniters fail or simply lag behind the others. One failed ignition loses a third of the total thrust. Two failed means the warhead may land close enough to the firer to endanger him.

These engines sport capacious nozzles. The most reliable means to ignite a cluster at once is to neck the nozzle end with kraft paper, then insert a packet of two grams of FFFFg black powder configured as an electrical squib. A length of black match extends all the way up into the central core of each engine, and is secured at the base with tape or more permanent adhesive. In one POOF, all three engines will get enough high-pressure flame to ignite.

These engines burn for just over 0.5 seconds, about twice as long as we would like, but acceptable if the firer wears suitable protection or the launch tube measures longer than four feet. The main feature is the sharp initial thrust. Except in guided missiles, long burn-times waste propellant that could have given the missile greater initial boost that, coincidentally, gets it up to stable velocity fast.

The military has available to it rockets hardly larger than G-class model engines that will deliver thousands of pounds of thrust for about a quarter of a second. Ejection seats of fighter aircraft use them to boost the pilot free of the plane. These use exotic solid propellants and sophisticated manufacturing techniques utterly impractical for the amateur.

You could not make useful weapons without extensive testing for performance, accuracy, reliability, and consistency, and study against multiple types of targets. That would demand a BIG open space free of observers, along with proper licenses from Big Brother.

Better return on effort would come from learning to apply small arms genuinely <u>well</u>. Of course, the devilish experimenter in us all brings back that thought of sticking a warhead on the end of a model rocket. What kid in a fit of mischief has not glued a firecracker on the end of a bottle rocket, just for the intense yet indefinable thrill of it?

Fusing would pose problems. The major options are time fuses ignited by the rocket motor at burnout, and impact fuses. Amateur impact fuses have an uneasy way of detonating as we drop the product on the carpet. They may find use in serious insurgency cases, where the need for detonation on impact justifies the risk, but should be considered taboo otherwise. (As a rule, serious insurgents can find a willing supplier of military weapons, depending on which way they lean politically.)

Let's be straight in admitting that here we must cop out. We own neither the facilities nor the proper licenses to make and test completely configured rocket weapons. We can, however, pass along knowledge that appears fit in a truly practical sense to rocket weapons. Experimenters with no experience in model rocketry would do well to start with simple, vertically fired rockets armed with nothing more than a parachute. Start with small models propelled by engines in the A or sub-A category. It saves money and makes the rockets easier to recover. After building a few proven kits to get a feel for rockets, start working on your own designs, slanting them toward that rocket-propelled-grenade look....

First, select the engines, warhead, desired effect, and launch mechanism. Create a design on paper that intuitively looks stable. Make an inert mockup and test it for stability, using those ancient teachings: Tie a stout cord about 8 feet long around the rocket at its balance point, which corresponds to its center of gravity. Careful not to bean bystanders, hurl the rocket around you in a circle with its nose cone forward. A stable design should remain forward-oriented and stable. If it wobbles, it needs either more fin-effect (not necessarily fins; the fins could be changed in shape to protrude behind the rocket; or it needs more mass at its forward end: a heavier warhead, perhaps; or the length of the rocket needs to be increased). Remember

that the rocket will travel minus propellant weight; thus, for this test, a spent engine (or engines, if a cluster design is to be used) is appropriate.

Once you have a small scale design that looks theoretically sound, the only thing to do is try it out. Select a launch tube of appropriate diameter, mount it on a sturdy holder (you are not yet ready to hand-fire the device, even a scale model), and fire it. Note its stability, how far it falls before hitting/missing the target. If too low, adjust the sights so it aims above the target in order to strike it.

With all factors that have to be adjusted, count on trashing a hundred models before arriving at a practical design. And that's just for the rocket and launcher. Warheads, warhead ignition, prefabrication and storage would probably take many months, perhaps years, to master. Rocket weapons demand more R&D, patience, and money than any other weapons system. Discounting the amortized R&D cost, count on each full-scale weapon using a cluster of three F-class engines for propulsion to cost $30 to $50.

Pause here to consider the utility of one of the latest generation of video cameras in the R&D stage of designing rocket weapons. One would prefer to confirm that engine burnout has indeed taken place by the time the rocket leaves its launch tube. Mount the tube on a suitable horizontal test bed out at your isolated and desolate range, frame the picture such that it sees the entire tube and most of the left of the screen is blank. Fire the weapon by remote control at twilight, when there is still enough light to tape the tube and target, yet show any exhaust plume clearly. Play it back with its 1/1000 second shutter to freeze motion. Military arms suppliers employ exactly this type of setup in their design work. With an extra thousand or two, there is no reason the amateur cannot follow this same instructive procedure.

Again, only for those licensed to make destructive devices....

SERIOUS WARHEADS

What could we, realistically, expect from homemade rocket weapons? Short of arming them with shaped-charge warheads, necessarily based on high explosives, quite a bit.

First, we can mount what counter-terror squads have come to label "stun grenades." These produce a dandy local concussion and flash, hardly surprising since they are modified aerial flash salutes, optimized for lack of shrapnel. In the enclosed space of a room or airplane, they generate a significant concussion, enough to stun without producing injury, save for those within inches of the device. They are the rough equivalent of three-inch aerial salutes. That means several ounces of flash powder in a paper case that converts to confetti on detonation. Since the case will be flimsy, a rocket warhead could not be expected to penetrate doors or even tough windows without self-destruction. Stun grenades protect their charge with a re-usable casing that ejects the flash bomb an instant before detonation. A reliable mechanism could conceivably be fabricated for a rocket warhead, but if it failed, you would have to deal with unwanted shrapnel.

Second, for close-in antipersonnel effects, as well as a measure of incendiary power, the titanium flash bomb is hands-down the most effective warhead on a weight basis. Even M-80-size devices yield spectacular bursts. A hard paper unit an inch in diameter detonating in a room, car, or within ten feet of an enemy would produce shrapnel and incendiary effect, not to mention scaring bloody hell out of savages who've never seen combat.

Third, and a variation on one big titanium bomb, would be the cluster warhead: a solid-based tube with a nose cone to aid penetration of windows and such, with an expelling charge of black powder in the base to scatter, say, twenty M-80-sized units about the target. Though more irritating than devastating, such a device could find use in close quarters or against fire-prone targets. It is extremely difficult to convey the sense of awe and dread the titanium burst calls forth in those who have not seen it. Equipping the individual salutes with fuses ranging in length from 1/8" to one inch would prolong the time the enemy had to take cover until the effect of the warhead had spent. This would give an assault force precious seconds free of aimed return fire in which to advance.

What about rockets within rockets? Our military is now seeking to perfect the terminally guided submunition,

a large missile that ferries a dozen or so independently guided antitank rockets high over a cluster of vehicles, whereupon the released submunitions flash under their own power to individual targets.

Forget about making tiny guided missiles, but do note the potential for small prefab rocket engines to carry 8 to 12 M-80-size warheads hundreds of feet from the burnout point of a bazooka-size rocket. The Estes T-series fit the end of an M-80 case perfectly. Anyone who has fashioned a crude "bottle rocket" from one of these babies will testify that they move briskly, probably about 400 fps tops. Properly configured units could spread salute-size warheads over quite a distance from the impact point. The A8-0T, with a burn time of only 0.26 seconds, is the engine of choice.

Fourth, consider a canister of tear gas. It need not burn to be effective, as the "Clear Out" aerosol units have shown. One could use the rocket to launch the canister further, or with greater force to smash through a window, with some type of mechanical trigger to release its CS contents, which takes about 28 seconds, according to promotional literature for the device. An alternative would affix an M-80-sized salute firmly to the side or base of the unit. On detonation, it would rupture the metal, releasing the contents in one big puff. In fact, one could improvise easily here by surrounding the M-80 with four to six pocket-size containers of tear gas, depending on the size of the warhead. Naturally, testing would have to confirm that the small explosive would in fact rupture the containers reliably.

Here we must turn grim, always bearing in mind that this assumes a legitimate need for such fearsome weapons, and ponder the terrible consequences of substituting say, three large butane canisters for the tear-gas cans. These would fit easily in a warhead less than 3" diameter, with a long flash powder bursting charge placed in the center, perhaps with a few granules of titanium thrown in to ensure ignition of explosively vented butane. This would give us a warhead of serious incendiary power, at least against easily ignited materials, hardly something one would toy with out of idle curiosity....

It may have occurred to the reader to use gasoline in the warhead. Gasoline ill-suits rocket weapons for several reasons. It is cursed with a fierce vapor pressure. It will force itself out of the smallest cracks or openings in a glass or plastic container, which is subject to rupturing prematurely under the pressure. Gasoline dispersed and ignited by an explosive goes up in an impressive fireball that spends most of its heat in the air, rather than clinging doggedly to the target. Napalm might do if you care to make it. It is saponified gasoline, a jelly that burns slowly and resists many types of firefighting efforts.

Naturally, those who can get their hands on high explosives and detonators, and who make frequent trips to Afghanistan or other land under siege, should feel no compunction about raising the yield of rocket warheads as the situation dictates.

SMALLER....

Estes Industries makes a handful of engines 0.5" in diameter, but disposing of fair thrust for their size. These are the "T" series, the smallest engine shown in the photos. Taking the Lilliput as our model, note that burn-times of the two engines are similar, thrust for the larger engine heavier, but not increased in proportion to its weight. (Lilliput used so-called composite propellant. Most small model rocket engines use compressed black powder, which offers less thrust per unit weight than composite propellants.) Yet, the A8-0T, judging from its performance fired as an extremely crude and relatively heavy stick-rocket, easily approaches pistol-bullet speed, and would undoubtedly do better in a properly designed unit.

One design could wound through sharp, hard point and kinetic energy, just like a bullet, but be thrown out in salvos, much like the Lilliput. Another effective concept could be a variant of the "terminally guided submunition," with each T-series engine throwing an M-80-sized titanium warhead several hundred feet laterally from some mother-munition, either a mine or the tip of a larger rocket. Pure speculation, but not without grim potential, as anyone who has seen even a tiny titanium warhead explode will agree....

—YES, BUT HOW DOES THE WARHEAD TRIGGER?

A good question, one whose answers demand ingenuity and extreme caution. Ignition while the rocket is still in the launch tube usually means an abrupt and ugly end to your career as weapons wizard.

Ignition systems for the warhead will depend upon the nature of the warhead and the target. Detonation on impact is extremely difficult for the amateur to achieve safely. For example, one could conceive of a percussion cap or pistol primer mounted inside the explosive, at the end of a metal tube that houses a spike. The point of the spike rests on the cap, the blunt end rests flush with the tip of the warhead. When the projectile strikes the target, it's like a firing pin falling on the primer. Of course, should you drop the warhead on its nose accidentally, it would detonate.

One publication suggested an electrical ignition system using a doorbell button on the tip of the warhead. This in turn connected to a power source and an electrical squib. Question is, how do you keep tinkers from pressing that button out of curiosity? Buttons are meant to be pushed....

A more attractive option is delayed ignition depending on fire-transfer from the spent engines. This, after all, is the means through which they ignite upper-stage engines in multistage model rockets. A safety fuse exposed to the forward chamber of a booster engine has an extremely high likelihood of taking fire when the booster burns out. The delay would have to be short, two seconds or so, enough to allow for flight time and penetration of the target. Too long a fuse would let the felons throw the device back at the assault force.

* * *

MODIFIED SHOTGUN SHELLS

For those who care to master its terrible recoil, the standard 12 ga riot gun can be an effective weapon against soft targets. That scenario needs no further discussion because its particulars make themselves plain.

But the shotgun holds shells that fairly beg to be loaded with something other than bird shot. Be warned, though, that modification of commercial shotguns or shells, especially with explosives or incendiary loads, would contain strong elements of personal jeopardy, along with overtones of extreme irresponsibility and serious lawbreaking. For those and other reasons we recommend that no one actually carry out these horrible speculations.

That said, it is interesting to consider how much more a defender could get out of his 12 gauge shotgun with something other than lead shot in the tube.

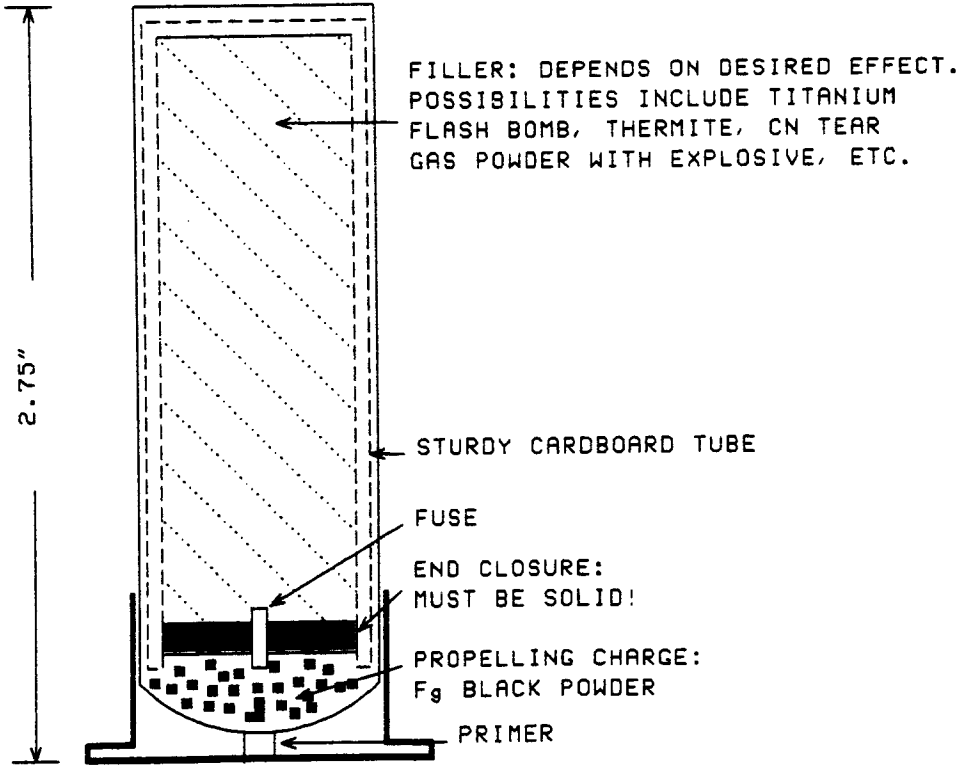
Casual experiments back in the late sixties showed that any number of stout paper casings designed for pyrotechnic purposes fit snugly inside an empty 12 gauge shotgun shell. Could a tube salute be fashioned? A titanium flash bomb? An incendiary of sorts? What would be the effect on the firer if it detonated on the breech or barrel? (The smart experimenter would sacrifice a cheap weapon to test it. The cost of the weapon is less than the use of your eyes. Would it ignite the remaining rounds?) What charge of black powder would be used to propel it?

Working up this type of round would have to proceed along the lines of working up other types of handloaded ammunition: start at the ground.

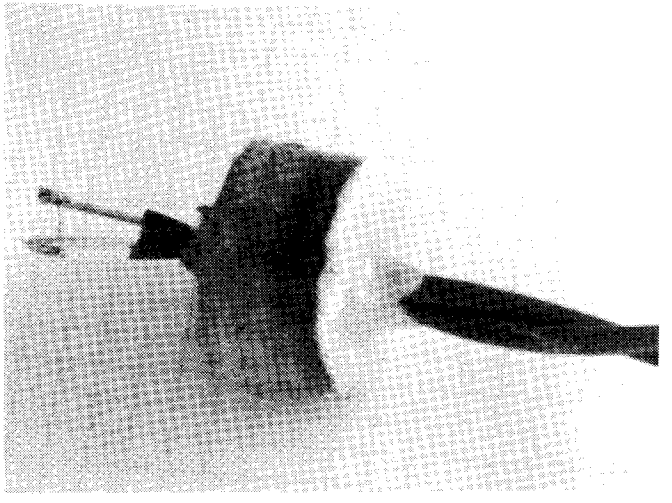
We can consider only one type of propelling charge: black powder, or its equivalent, a product called "Pyrodex." Black powder comes in various grain sizes. Of what is sold in gun stores, Fg is the coarsest, FFg the next finer, and so on down to FFFFg. It is theoretically possible to get what is known as meal powder—gunpowder dust—but the author has yet to see it on the shelf, or to have a gunshop owner say he could order it.

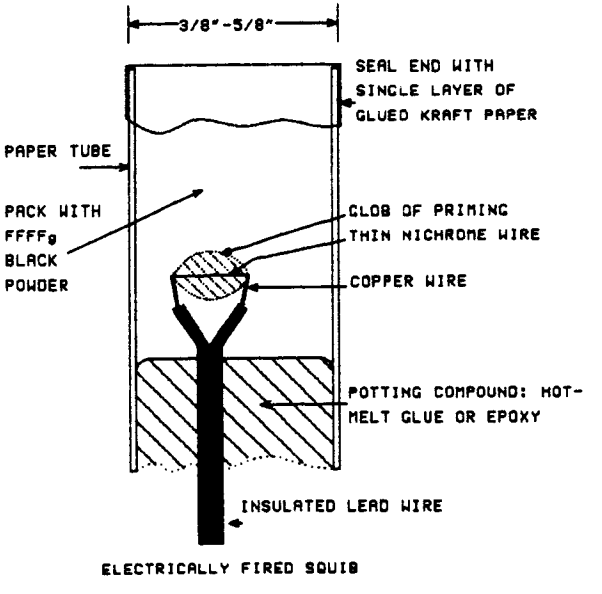
Grain size makes a difference because, the larger the grain, the less burning area exposed per unit weight of charge. In crude terms, that means Fg will generate a prolonged, almost gentle shove, while FFFFg would spend its energy quickly, giving us pressures so high that they might burst through the end of the casing, setting off whatever goodie you had loaded in the tube.

Why not use smokeless powder, normally used to propel bullets or shot? Here breech pressures rise into the thousands of pounds per square inch—50,000 or more for centerfire rifle cartridges. A miscalculation might not only set off the modified goodie, but could burst the breech in your face and detonate the other rounds in



THE 'MODIFIED' SHOTGUN SHELL: A PURELY SPECULATIVE STUDY....





ELECTRICALLY FIRED SQUIB

the magazine. No, smokeless powder should be used only with bullets, and then only by experienced handloaders who've fathomed its mystic ways.

For what we describe here, begin with dummy devices: physical mockups identical in size and weight to the contemplated finished projectile, yet utterly inert. You may fuse them, but load no thermite or whatever sinister flammable you cooked up. We must first establish that the casing has enough integrity to withstand being shot from a gun.

Assuming a 12 gauge shell, with a hard paper cylinder that fills its space as the payload, start with 0.5 gm of Fg black powder as your propelling charge. Use a cylinder-bore weapon. Fire for range, velocity. You must recover the test shell to see if its base (say, a 1/2" thickness of hardwood dowel glued in place) remained intact. It may be necessary to get fancy and turn a T-shaped end closure on a lathe so that blowthrough is almost impossible.

Now, half a gram of black powder will probably toss the projectile a ways, but we seek maximum range while maintaining complete safety. Begin incrementing the charge by 0.1 grain of powder each trial until you reach the point that you can almost use a set of sights to aim it. Max velocity will help it penetrate, say, windows in houses and cars; but it must be tough to avoid breaking up.

As for the other end, well, you could turn a hardwood nose cone of sorts, if penetration is important. You have no way to know whether this type of thing would tumble in flight. It may be best to view the modified shotgun shell as a mechanism for tossing things further and faster than you could with a slingshot. (Who can forget Russ Meyer's Supervixens? Remember Chuck Napier lofting dynamite sticks with that nifty little sling-shot/launcher? There's something for everybody in a Russ Meyer movie....)

Though scarce, commercial products that incorporate some of these features are available. For instance, one 12 ga shell fires a flash salute larger than an M-80 a distance of about 275 feet. Its purported duty is to scare birds away from crops. Phoenix Systems sells those shells. And one firm markets a hollow plastic slug filled with liquid tear gas that will penetrate light barriers, such as glass or thin plywood. Police only.

* * *

ULTRASONICS: EARPLUGS DON'T HELP....

It is by now common knowledge that high-powered sound above the range of human hearing can rid houses of pests, from bugs to rats. Their vulnerability to this attack lies in the fact that they "hear" what is for us inaudible. Some species use these frequencies in their reproductive cycle. Jamming them means death by attrition for the local vermin contingent.

Despite the fact that humans are not believed to hear ultrasonic sounds, it has nevertheless been observed that those exposed to extremely loud high-frequency (not necessarily ultrasonic) sound (10 KHz to 20 KHz) at levels well above 100 dB, display physical symptoms, such as nausea, headache, panic, fainting, irritability, and an urge to defecate. The reason for this response has not been delineated; all we can do is speculate. The symptoms are most compatible with activation of parts of the autonomic nervous system, itself an unconscious mechanism, perhaps equipped with ability to sense harmful energy that escapes consciousness.

And ultrasonic energy can be harmful. Small metal probes vibrating at ultrasonic frequencies can cut materials. An ultrasonic probe has found use cleaning teeth. It's not supposed to hurt....

If the role of ultrasonic energy as an antipersonnel weapon lies in limbo, there is no doubt that has use against dogs. Imagine the 120 dB siren of an ambulance right in your living room. The normal reaction is to get the hell out of there, pronto. Since dogs hear what is inaudible to us, we can devise fiendish devices to crank out ultrasonics at inhumane levels to keep the cursed animals at bay.

All that's needed is an ultrasonic oscillator feeding a high-powered audio amplifier, in turn driving one or more ultrasonic transducers. Back in the discussion of microphones, we met the crystal mic and its basis, the piezoelectric effect. The most practicable ultrasonic drivers happen to be horn-loaded piezoelectric

transducers. (A horn is the acoustic equivalent of an impedance-matching transformer. It ensures maximum conversion of diaphragmatic vibration into acoustic energy. The higher the frequency, the smaller the mouth of the horn can be without losing efficiency. Efficiencies for this type of transducer easily exceed 100 dB for an input of 1 watt at 1 meter, this compared to about 90 dB for typical hi-fi tweeters that will reach into the ultrasonic region. The piezo horn enjoys another advantage in that it will absorb genuinely huge amounts of power without self-destructing.)

To investigate this phenomenon first-hand, we built Information Unlimited's "Invisible Pain Field Generator," a kit selling for about $40 plus $5 shipping (innards in photo). The unit generates either a continuous tone at a rated intensity of 105 dB, or a tone-sweep at a rate of 1 to 10 Hz, sweeping an adjustable range, from 15 KHz to 25 KHz.

The unit performed as advertised in the sense of producing sonic and ultrasonic energy in the ranges noted. As to its moniker, "Invisible Pain Field Generator," well, it definitely triggered a headache in the author, not the typical migraine or tension headache; rather, an odd pain in the back of the head and neck that is hard to characterize. Exposure at a distance of less than two feet for ten seconds would do it reproducibly—but the effect was delayed. The sound does not instantly hit one with pain, but consistently produced a disagreeable sensation of delayed onset. Interestingly, silicone rubber earplugs did nothing to blunt the response, suggesting that the pathways involved do not require an open ear canal. (Earplugs attenuate high frequencies much better than they cut low frequencies....) In fact, holding the hand over the transducer had little effect.

The transducer supplied with this unit was in essence a piezoelectric cone tweeter, far less efficient than horn-loaded piezo tweeters. One could replace the existing tweeter with Motorola's horn-loaded unit, available from McGee Radio for $7.95, perhaps from Parts Express at $4.95, and gain 7 dB or so at the expense greater bulk. The piezo horn functions up to 27 KHz, while the less efficient cone goes up to 40 KHz.

I.U. sells far more powerful units based on this same principle. They generate greater power and feed an array of four highly efficient horn-loaded piezo tweeters that crank out this same fearful sonic energy at genuinely frightening power levels, more than 120 dB according to their literature. Theory would support the accuracy of that claim. That should be enough to drive an intruder out if the unit were configured to activate as part of an alarm.

This kit, and from the look of its literature, most of what Information Unlimited carries, is not for beginners. It demands considerable skill with a small-tipped soldering iron, and the instructions assume the builder has access to, and understands the use of, a VOM and oscilloscope. Fitting the finished board, transducer, and battery into the plastic case supplied would tax the ingenuity of the tyro.

Be aware of the legal concept of an "infernal device." Generally, this refers to what lawmakers anticipate wanting to have the right to strip you of or stop you from using if in the opinion of police or a judge it qualifies as an infernal device. Ultrasonic sound generators may fall in this category in some jurisdictions.

* * *

EXPLOSIVE DEVICES

REACTIVATION OF PRACTICE GRENADES

Most who have scanned the pages of military-oriented publications have seen ads for inert practice grenades, complete with moving parts. If indeed the item comes complete, including its springs, we might restore it to serviceable impact through simple means.

First we must understand the mechanism by which hand grenades function. Refer to the photo set of a dummy MK II grenade that saw use in WW II but has been replaced by newer models. Made of cast iron, the serrations on the surface mean nothing in a functional sense, since experiments showed that, to produce

fragmentation along furrows in metal, the indentations must line the interior of the grenade, rather than the exterior. Still, cast iron has proven brittle enough that it will serve, though this design generates a far less uniform spray of shrapnel than the latest generation of grenades, and weighs more.

Yet this outdated design is most suited to reactivation, since it does not require high explosives to achieve its effect. Perchlorate-based flash powder, specifically with sulfur, as reviewed in detail in the chapter on pyrotechnics, will suffice. (In genuinely urgent situations, say, when Ivan has just parked a T-62 in the front yard, one may resort to the chlorate, but ever so cautiously....)

To operate a live, conventional, time-delay grenade, first be certain that the safety retaining clip has been removed. This safety retainer serves as a backup during transport and rough handling. Remove it before setting out on a mission.

Grasp the unit such that the safety lever is held against the palm. Pull the pin. At this point, nothing further happens until the device is released, at which point the striker spring sweeps the safety lever around in an arc, releasing the striker. The striker snaps down hard on a percussion-sensitive primer, igniting a delay train of five seconds or so, which ends in a detonator, which in turn sets off the main charge.

Note that the time from release of the grenade to ignition of the percussion primer takes a fraction of a second. If any path exists allowing direct communication of fire from the primer to the main charge, detonation occurs within mere feet of the user, even if he has thrown it hard. Reactivation demands careful attention to this point.

The ideal restorable grenade contains all non-explosive and non-combustible components, including safety pin, safety lever, striker, and body with screw-in plug in the bottom. Such units lacking only the bottom plug are available as of this writing from Phoenix Systems at about $20 for single units, down to $17 per unit in quantities of 10. Greater quantity discounts may be available, though purchase in bulk might raise uneasy questions in some quarters. Contact the supplier.

Many other firms sell "practice grenades" whose complement of parts may range from complete to worthless. The advantage is lower price, about a third of what Phoenix Systems charges for single units. It might pay to check out samples from several suppliers.

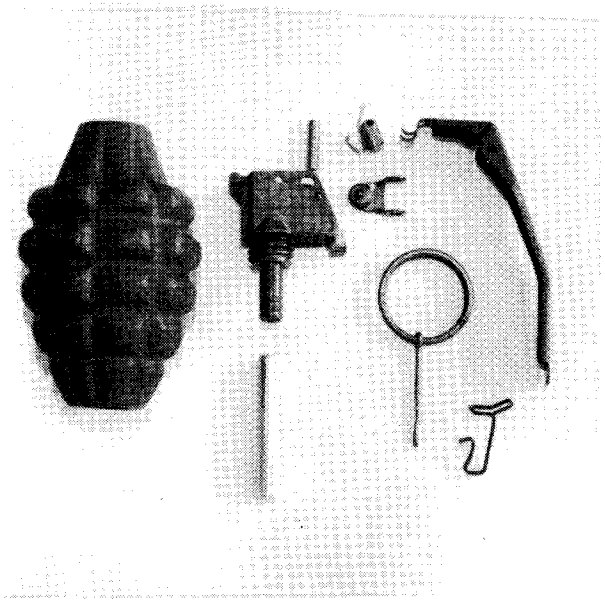
The main disadvantage in the unit we obtained from Phoenix Systems was its 7/16" unthreaded hole in the base. Firm closure is essential to maximum performance, and we may accomplish it in any number of ways. A tight-fitting section of hardwood dowel epoxied in place should serve. So might a plug of auto body dent-filler. We leave this aspect to the ingenuity of the licensed manufacturer.

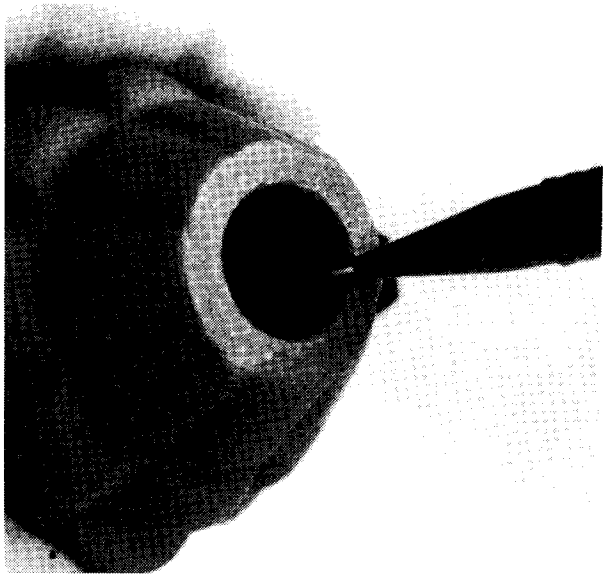
To get the inert grenade to function as God intended, we must restore 1) the percussion-sensitive primer, 2) the delay train, 3) the igniter/detonator, and 4) the main explosive charge. This assumes we do not have access to high explosives used in military issue units.

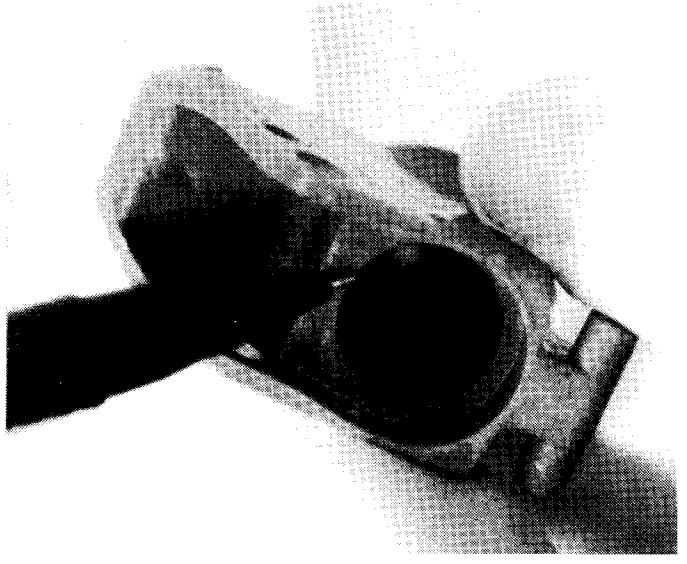
Start with the percussion-sensitive primer, since one main plus of this type of unit is that we need not pause to strike a match to light it. Any gunshop that caters to the black-powder trade will stock percussion caps. These differ from primers used on pistol and rifle cartridges in design and properties of composition. Do not try to use a pistol primer (the photo shows a cap and a primer side-by-side). Not only will it not fit well into the desired space, but requires too much force to initiate. And the cursed things give off a terrible report that one would never guess from their size. A large pistol primer fired alone equals the report of a .22 pistol.

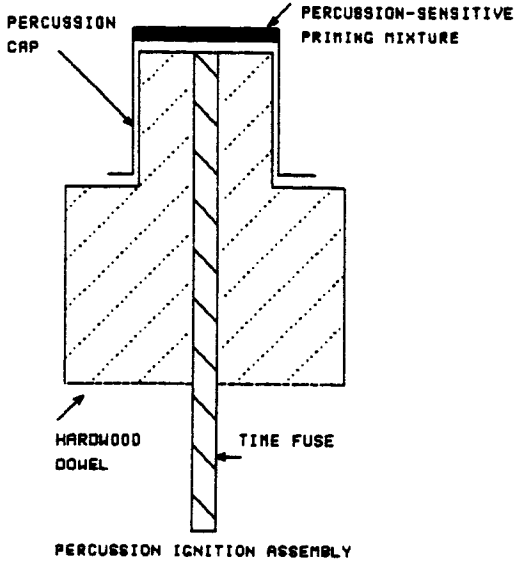
Percussion caps are milder, designed merely to transfer fire in black powder weapons, rather than the tamer smokeless powder. Since the delay line for the reactivated grenade will consist of safety fuse, whose core is black powder, percussion caps are ideal.

Note from the photo of the open top of the ignition section that we must fashion some mount for the percussion cap. Suggested details appear in the diagram. We wish the cap to seat firmly around its rim, and for the end of a piece of safety fuse to touch the priming material. A section of hardwood dowel of proper

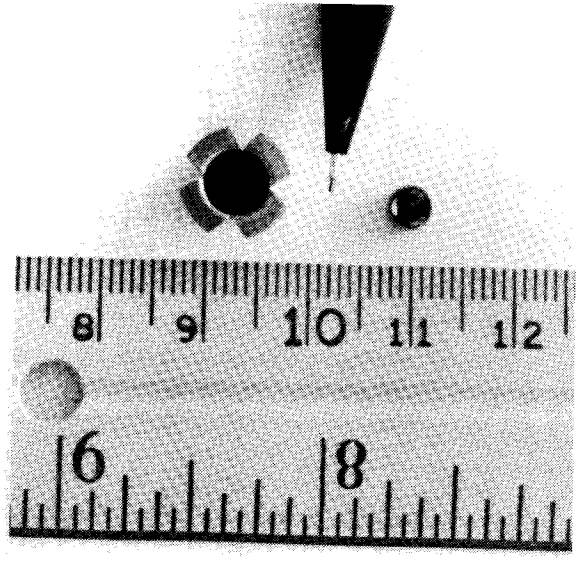


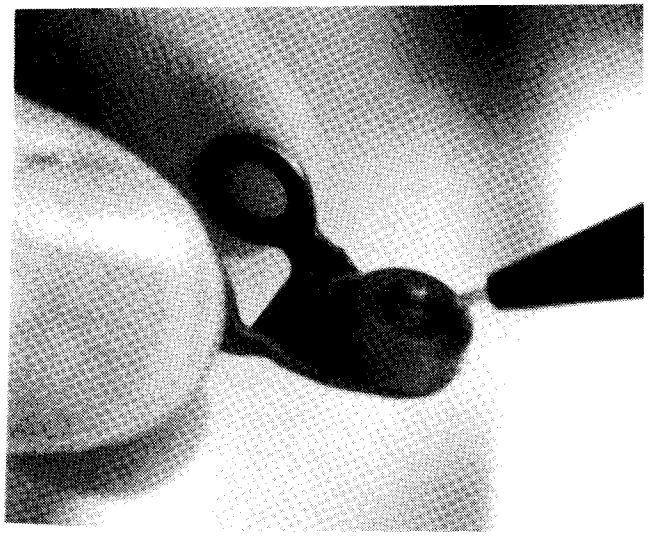




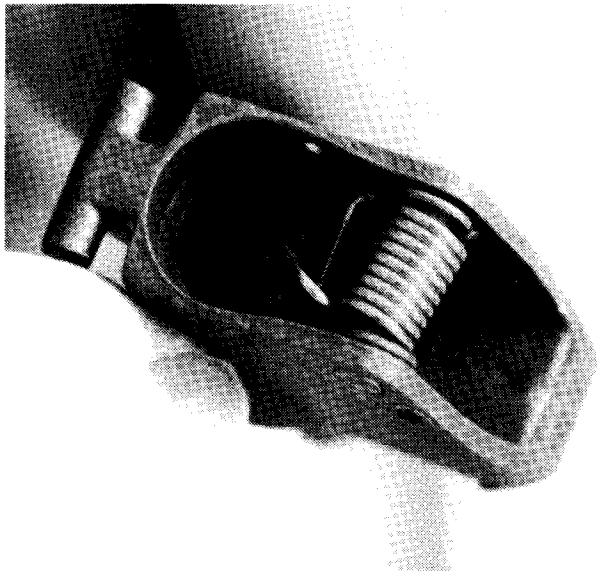
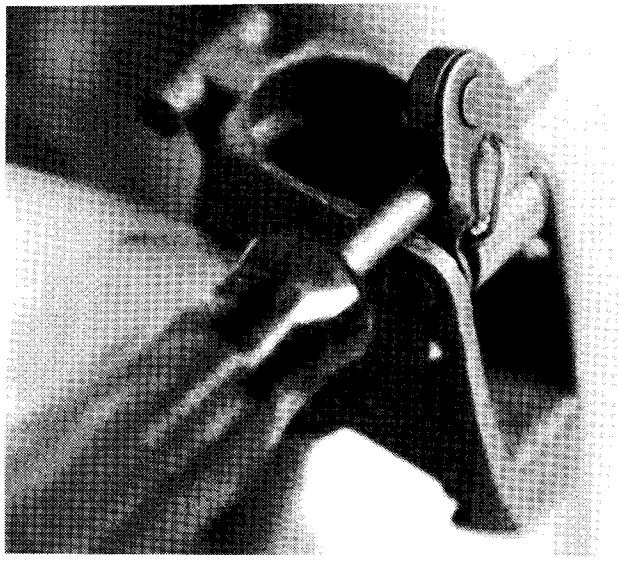
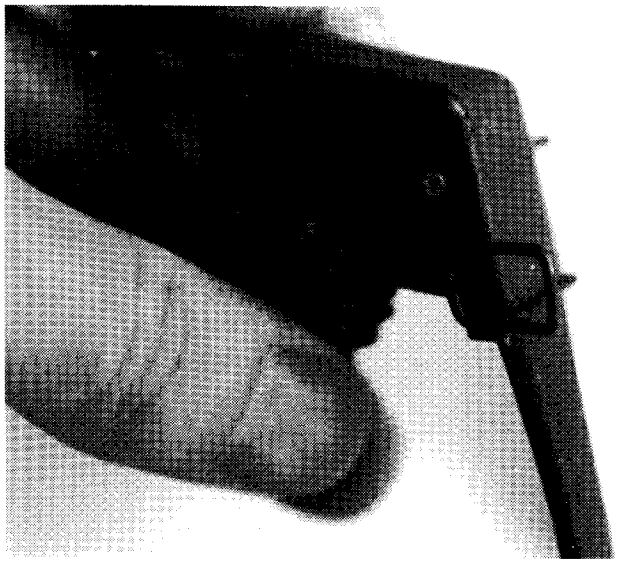
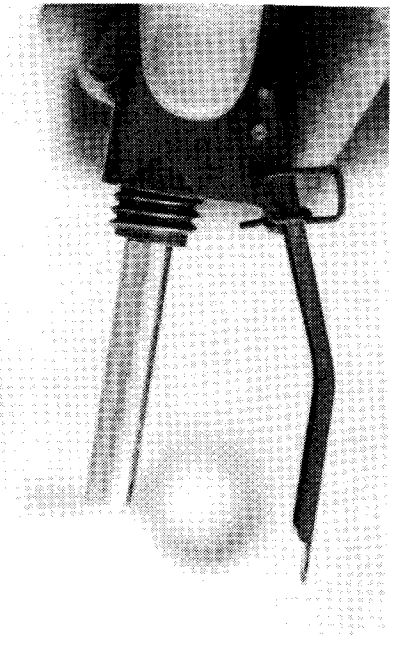
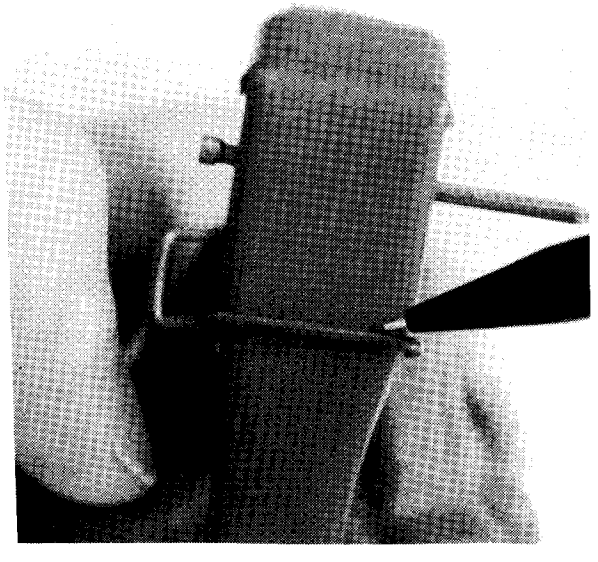
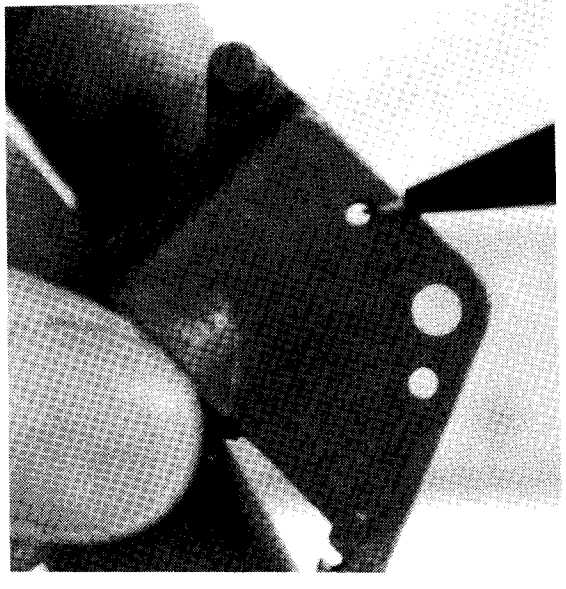


PERCUSSION IGNITION ASSEMBLY
GLUE INTO WELL AT TOP OF GRENADE





REACTIVATION OF PRACTICE GRENADE. TOP LEFT: Disassembled unit. TOP CENTER: Note absence of provision for sealing hole in bottom. Licensed experimenter must use his own ingenuity here. TOP RIGHT: Empty well for percussion primer. BOTTOM LEFT: One possible configuration for mounting percussion cap and fuse. Fixture made from hardwood dowel. BOTTOM CENTER: Left is percussion cap, right is large pistol primer. Only the cap is suited for this task out of its size and lack of deafening report as it triggers. BOTTOM RIGHT: Close-up of striker pin. (continued next page)

(continued from previous page)
TOP LEFT: Striker and its spring installed. TOP CENTER: Striker must be cocked all the way back into the hollow behind it. Spring is extremely strong. Exercise great care when dealing with live primer. TOP RIGHT: Striker has been fully cocked, and safety retaining lever put in place. Nail is in hole where pull-ring will ultimately go; note safety clip, a safeguard that must be removed prior to using unit. BOTTOM LEFT: Thin-walled aluminum tube that will be filled with primer/detonator. BOTTOM CENTER: Another view of safety retaining clip. BOTTOM RIGHT: Hole whose apparent purpose is to allow insertion of metal pin during process of cocking striker such that, if striker were accidentally released, it could not hit primer.

diameter and bored inside to accept the fuse, and of proper outer diameter to fit the cap should work well, though other materials could serve. A space will probably remain around this mount. Pack or shim the dowel to keep the cap centered. If you plan to make several tests of ignition, count on the dowel burning away a little with each, such that the shim should be temporary, to make way for more lasting stuff once you have the dimensions down pat.

It is vital that, in the final design, there be no direct path of fire from the percussion cap to the main charge. That would result in instantaneous detonation as soon as the cap was struck. Epoxy resin to fill all gaps should serve.

If used as-is, the minimum length of fuse is just over 1.5 inches. If tests show your fuse burns that up in 5 seconds or less, fine. If it burns considerably slower, you may have to cut off part of the tubing that extends beneath the threads.

Seal the edges of the fuse at both upper and lower portions to minimize the chance of fire getting to the booster charge prematurely.

Have the fuse protrude at least 1/2" from the end of the metal tube that extends into the body of the grenade. Fill the thin-walled aluminum tube about two thirds full of FFFFg black powder, or Pyrodex, whichever is available. Next, friction-fit the tube back onto the delay-train tube as it came from the manufacturer. If you had to cut off any part, a single wrapping of tape or a daub of epoxy will secure it. The tubing will blow off when the black powder ignites, providing a fine boost to the main charge.

Our main charge will consist of as much perchlorate-based flash powder as we can comfortably and safely pack into the grenade. Flash powder is discussed at length in the fireworks chapter. Since we deal here with serious weapons, we will assume otherwise unacceptable risks and note that chlorate-based compositions, with appropriate precautions against acidity, give hardier performance. However, the prudent artificer would use a mix of potassium perchlorate, dark pyro aluminum, and sulfur in a weight ratio of 2:1:1 or 3:1:1. Sulfur offers greater gaseous reaction products, which, at least in theory, gives improved performance over perchlorate/aluminum mixes. Follow the instructions for mixing given in the section on pyrotechnics.

Loading will be tricky. The case is metal. If an electrical potential exists between the powder and the case, static electricity could detonate it during loading. Best to place the powder out on a sheet of aluminum foil, then place grenade and foil at ground potential by touching the case to the foil before attempting to pour it. The same goes if you use a funnel.

Fill the case completely, but make no attempt to compress the powder. Sealing the end is a matter of screwing in the detonator, but note the hazard of detonating the powder from friction between metal threads. Coat the threads on the inside of the neck with a thin layer of petrolatum (Vaseline[tm]) before screwing it in. No one could fault the artificer who wished to leave insertion of the detonator until just prior to field operations.

One part missing from the unit but which may be valuable is a rubber seal/washer at the neck. In humid climates or exposure to water, it could keep the unit in working condition.

Depending upon circumstances, a potentially useful mod would add 25 percent by weight granular titanium to the main charge (see the chapter on pyrotechnics).

Although inert grenades of later generations are available, they will do you little good unless you can get hold of high explosives. Flash powder will fragment cast iron, but will not do much to the notched, coiled steel spring that forms the shrapnel of our army's "baseball" grenade. Not only that, you will have to get hold of a blasting cap to detonate the high explosive.

Be aware of the legalities involved. BATF spells them out clearly: You are creating a destructive device and manufacturing explosives. Several permits and/or licenses may apply. You will have to meet appropriate storage requirements. If state or local laws get in the way, either move to a properly enlightened locale, or don't do it.

In the course of preparing this discussion we did not mix any explosive nor create an explosive device. Our inert practice grenade/photo dummy was and remains only that, a lifeless piece of iron awaiting resurrection in some nameless future that sanctifies violence in the name of freedom, unlike the dreary present, where oppression has the upper hand and free access to powerful explosives....

SHAPED CHARGES: THE MUNROE EFFECT

If you took an inch-thick slab of plastic explosive and gouged your initials in it to a depth of one quarter inch, then set the piece initials-down on a sturdy slab of lead and detonated it, the blast would punch your initials, mirror-image, into the lead. The effect results from convergence of high-pressure shock waves traveling thousands of meters per second, creating local boosts in force above the terrible power of unmolded plastique. This phenomenon has come to be called the Munroe Effect after Charles Edward Munroe, credited with its discovery.

Through experimentation, it was learned that lining the cavity with metal—copper and tin proved most efficient—enhanced the effect, probably out of interaction among several variables: mass of the metal, the fact that the shock wave drove it to velocities measurable only in theory, and the fact that the metal vaporized, yet retained its density due to the equivalence of temperature and pressure in this esoteric brand of physics. (Focusing the energy of high explosives, rather than nuclear physics, proved the most difficult of problems in fabricating early nuclear weapons.)

The best known practical application has been with antitank weapons, since optimum designs can penetrate five times their own diameter of armor plate, incredible though that claim seems. But a look at standard antitank rockets with their seemingly puny warheads tells us that it must be true.

Cone-shaped charges focus their power to a point, but linear charges that look like angle-iron when viewed in cross-section have found application in cutting steel and even cutting man-size holes through brick walls. We see that construction invokes the same principle of focusing the energy of the blast and use of a metal liner.

What amateur weapons designers do not know is, how powerful an explosive do we need to summon the Munroe Effect? Can flash powder do it, assuming we achieve detonation? Must the powder be packed or loose? Must we resort to chlorate oxidizers, or will the perchlorate suffice?

Unanswered questions it would take much experimentation to answer. Some inferences we can draw with a fair degree of accuracy. First, forget homemade shaped charges, even those made with C4, that will defeat the full thickness of a main battle tank. Unless you live in Europe, Central America, or Afghanistan, you will not face tanks.

What about the platter charge, described in countless military manuals? In light of recent revelations about fire-formed charges, it is naive to believe that the metal slab remains flat as the explosive hurls it through a fence and into the enemy power station. If not bent exactly into optimum armor-piercing shape by the blast, it must at least be reduced to a glob, thus focusing it momentum better to aid penetration of hard targets.

Given that we will have only flash powder to work with, consider the speculative design in the diagram. Flash powder burns slowly enough that we must do something to help keep it from dissipating its force to the sides. The tube serves that end. Second, note the space between the metal circle and the business end of the charge. This is analogous the standoff required of shaped charged. It gives the explosive room to accelerate and/or deform the metal projectile before it strikes home.

Clearly, ignition should take place from the rear, with moderate packing of the charge, and we should use whatever means possible to see that it shifts into detonation as quickly as possible. Here the principles learned in fabrication of recreational salutes will serve, unless we have access to genuine blasting caps.

What about a stout paper cylinder filled with perchlorate flash powder with 25 percent by weight granular titanium, arranged as if it were a shaped charge? Would the explosion be swift enough to summon the Munroe Effect, and if so, would those tough, burning particles of titanium add punch to an otherwise breathtaking if unproven warhead? Move to the desert, get licensed, and experiment to your heart's content and at your sole risk.

Why speak this blasphemy at all? Times change, and who knows where time and fortune may take you. There are places in the world right now where this knowledge could prove valuable, if not decisive. Stinger missiles delivered clandestinely to the Afghans proved decisive. These grim ruminations qualify as last-ditch defensive or harassment weapons for use against hostile occupying forces, and then only when the plastique runs out....

The author once spent an interesting evening in a coffee shop swapping tales with a professional blaster. As many of that breed, he had been a basement bomber in his childhood—only this guy had taken it to the limit. Having gotten hold of Davis' text on explosives, he proceeded to synthesize a batch of lead azide, a detonator more powerful than mercury fulminate, the main ingredient in blasting caps. As the matter precipitated, it detonated, seriously damaging his hand and ripping a hole in his abdomen. Since we had both read Davis, we exclaimed at the same time, "But not in the presence of dextrin!" Lead azide precipitated without dextrin forms particles whose internal crystalline stresses detonate it. Had he added dextrin to the solution, it would have saved him that grim stay in the hospital.

We cannot overemphasize this point: Avoid trouble by obeying all laws decisively. Document everything. The hunch that you might have made a "live" hand grenade whips police-types into a state of enforcement hysteria. Mentally, they see you serving 10 years even before they get you to the station. You become an Extremely Dangerous Pervo whose felony-bust fattens their promotion file. Have the proper papers, permits, and storage documentation to back up your legal acts. It would not hurt to review the whole matter with a criminal defense lawyer before embarking on the project. Memorize his phone number and that of a bail bondsman.

MINI-INCENDIARIES

What would happen to a large, disposable butane lighter taped to a tube salute? The explosion would rupture the plastic, and in all likelihood, ignite the pressurized butane: mean orange tongues of flame licking out to get you....

Or, for the more determined artificer, why not one of the bulk butane containers used to refill non-disposable butane lighters? Their casings are thin aluminum, easily ruptured by a tightly taped salute. (An ancient photo illustrates the ease with which we can penetrate metal. It shows the remains of an empty but otherwise intact paint-can lid after an experiment out of the dim past: In a deserted part of the woods, an experimenter laid an M-80 holding 1.4 grams of flash powder on the lid, lit the fuse and retreated. The detonation punctured the steel lid, venting enough pressure into the can to blow off the lid and send it spinning into the woods. A nickel weighs about 5 grams....)

Think of these as energetic Molotov cocktails. What they lack in stickiness of gasoline, they make up in vigor.

THERMITE

Thermite is a mix of iron oxide and powdered aluminum in a weight ratio of 75/25. The iron is usually granular, since finely powdered ingredients can lead to an instantaneous/explosive reaction. Though so hard to ignite that special pre-ignition formulas are needed, once begun, the aluminum "burns" by stripping oxygen away from the iron oxide. This yields aluminum oxide and iron, but releases so much heat that it leaves the iron white and molten, flowing like fresh lava out for vengeance.

Thermite bombs form part of the military incendiary arsenal. Their major application is destruction of metal targets, and in field-expedient welding. The fact that they start fires is only a secondary, uh, benefit.

If you do manage to get thermite lit, the reaction will be over in a flash, and you will instantly find yourself with a puddle of molten slag iron burning down through everything: through the carpet, the floor, into the condo below, setting all of it on fire. What a lively surprise for the couple in the bedroom below to have their session interrupted by half a pound of molten iron tunneling down through the ceiling like the molecular acid in Alien....

The position of a thermite bomb makes a difference. As literature points out, this is a damned hard mix to light. It sustains its reaction best when lit from the top, such that the only way the molten slag can travel is down. This provides the needed heat to keep the reaction going.

Thermite bombs are usually placed upright, directly over the metal object to be destroyed, then lit. This results in a pound or so of white-hot iron at about 2500 degrees centigrade gushing down on the target. It can cut through an inch of steel.

In order to overcome thermite's notorious ignition resistance, scientists devised a variant called thermate, which adds barium nitrate and sulfur to the mix. It generates less raw iron per unit weight but burns more energetically.

* * *

ELECTRICAL IGNITERS

Situations that call for serious explosive or incendiary weapons usually do not give you time to light a match. That and the burning fuse betrays your position, if not your intent. No, the only satisfactory igniters for serious scenarios must be electrical, immediate, and reliable.

If you have access to professionally made electrical igniters and know how to use them, fine. If not, you must make them.

Conversion of electricity to heat forms the basis of most igniters, the most common version passes current through special high-resistance wire known as nichrome, out of its nickel/chromium alloy makeup.

The igniter, or squib, must possess properties not required of the simple igniters used in model rocket engines. They should be sturdy, reliable, generate a healthy flame, not be subject to melting of the nichrome at any point outside the powder contact.

Refer to the diagram of one possible electrical squib design that has proven reliable and effective. Note that all the nichrome wire lies inside the powder tube. Were it to protrude, local heat could melt it at that point before it lit the powder charge.

Second, note that the lead wire is low-resistance copper, significantly heavier gauge than the nichrome (we want thin nichrome, thick lead wire). It is embedded in a lump of tough material: hot-melt glue, epoxy resin, wax, and so on. The idea is to take all strain off the copper/nichrome junction.

Third, note that the nichrome wire is soldered to the copper lead. Now, do not depend on solder alone. Fashion a mechanically secure contact before soldering. That way, should the solder melt when current is applied, the wiring will remain intact.

Fourth, there must be enough powder packed in the squib such that the powder never loses touch with the wire. In fact, one could make a slurry the consistency of mud with black powder, water, and common starch, then press a lump of it onto the nichrome wire. It would dry into a hard grain that never left contact with the wire, no matter what position the unit was in. FFFFg black powder is probably the best filler from the aspects of low ignition temperature, vigorous burning, consistency, and availability.

Finally, if the completed device will be stored any length of time, waterproof it by coating with shellac or wax (do not dip the completed device in melted wax; it may ignite).

Where to get nichrome wire? Model rocket engines sold at local toy and hobby stores come with nichrome igniters, including a flammable coating that helps ignition. This type of purchase is so common as to be nearly untraceable. On the other hand, purchase of a hundred-foot spool of 30-gauge nichrome wire will generate a record. Fragments of the device will be checked for just such an alloy, easily matched by analysis to the manufacturer, and from there to supplier, and then to the careless artificer....

Before using an igniter of this type in a serious weapon, make and test at least ten. Determine delay between application of current and ignition. Determine what voltage and current will suffice. If the battery is to be placed within the device, resistance of cable can be ignored, except perhaps with typical 9-volt battery cables. These are thin and more resistive.

Some igniters and detonators in commercial use are sensitive to static electricity and even radio waves from nearby transmitters. The igniter we have just described is immune to such devils in any practical sense.

Electrical igniters of this type fairly drip guilt. If the Authorities discover them in your home or auto, or on your person, you will find them most interested to know more. They will probably visit your home with a search warrant while your bond hearing has been postponed...and what else are they likely to find?

* * *

THE MOST POWERFUL WEAPON

After all this scary drivel about lasers, armor-piercing ammo, shockers, along with foul hints at chocolate poisoning, not one individual in a hundred knows that he carries the most devastating weapon on earth in his back pocket or her purse: Money.

The spending of money occurs in patterns. Those patterns, in turn, determine the distribution of power in the world. And those who govern the flow of money rule the world.

But how do these patterns arise? Haphazardly? Laissez Faire? Hardly. Rest easy that you needn't brace for some off-the-wall global conspiracy theory. Yet, it's impossible to answer certain questions without concluding that men who wield power use human nature to shape spending patterns; or to believe that they themselves are ignorant of human nature's power; or that they have not used this knowledge to boost themselves and those ideas they favor.

Radical groups at both extremes draw press coverage when they decide to misbehave in nonviolent protest or —preferably, from the standpoint of television ratings—ultra-violent eruption. Yet these groups are destined never to rise above the sub-basement of televised notoriety. They have failed to learn from the true power-brokers of the world. One gets one's way quietly, slowly, over generations, behind the scenes, through organized campaigns that avoid the spotlight. This approach lacks the immediacy of a Marxist revolution or the sad pageantry of National Socialism. But those sorry fringe elements struggle to survive on a diet of sporadic violence, while powers with a genuinely long-range outlook continue to prosper and consolidate.

The average man in the street doesn't sense manipulation and thus does not resist it, cannot shape his own destiny. The slow, low-key approach has prevailed because it harnesses human nature. It makes people act like puppets because they believe they raise their own stations by doing so. This short-sighted tack never factors in the secondary and tertiary consequences of spending money.

It explains a number of domestic institutions. Take the IRS, for example. IRS did not come by its limitless power or bully-boy personality by chance. It has been groomed from the start as the enforcement arm of Congress. Though Congress has no executive power in the strict sense, it effectively has it through legislation. First, it passed laws that made an irresistible force of the IRS. Then it wrote tax laws to help its friends and destroy its enemies.

Big organizations—and Congress is the biggest—do not voluntarily cap their power. Human nature makes them expand it. Pathetic tales of taxpayers "accidentally" destroyed by the IRS fall on deaf ears. It makes a good show for TV, just like bloody disaster victims and their weeping families. We have yet to see meaningful change, hardly unexpected from a bureaucracy loosed upon us with the power to write its own regulations, which have the effect of law. (As this goes to press some manner of reform legislation is "pending." So is a cure for cancer....)

Glib philosophy feels uneasy in a hard-core tech book. Let's drop it before the reader nods off.

7
EXTREMELY DANGEROUS FIREWORKS

It's a boy.
—Edward Teller, coded message to signify success of early H-bomb test.

* * *

Batavia, Ohio, plays home to a well known mailorder establishment called Sporty's Tool Shop. One of their big items—literally—is a mailbox that weighs 50 pounds. Sporty's catalog touts it as immune to the blast of two M-80s exploding inside it simultaneously. Their promo prints a splendid picture of the big box a split-second after detonation.

Now, Sporty, if you would care to let our readers in on where the photo crew obtained these federally banned explosives, then have all involved turn themselves in to the nearest offices of BATF for arrest, confession, and sentencing....

What better testament to the popularity of tube salutes, banned though they may be, than their use in a catalog that sees nationwide distribution? Even the voice of Scramble Facts, detailed in the chapter on Security, invoked an M-80 to make a point. Cherry bombs and their cousins in the big-firecracker field fascinate people. They have defied a federal ban enacted in 1966 out of demand for them and continue to move at heavy prices on the black market. But why this enchantment with evil units acknowledged as A) dangerous, B) abuse-prone (who didn't vaporize a mailbox or two in younger days?), and C) federally banned?

First, the mere fact of being forbidden boosts worth. Prices of porn videotapes, for example, remained among the most resistant to cuts until porn achieved a degree of wretched acceptability the nation had to grant, if only by assent. After all, there couldn't be that many millions of degenerates out there buying all that recorded smut. Most of it had to be going to honest, clean-living folk.... Tube salutes retain their value and lure because they are forbidden and scarce.

Ground boomers, exemplified by cherry bombs and M-80s, hold two, maybe three grams of powder at most. Their internal volume comes up far short of a cubic inch. Compare those banned units with aerial salutes. Pieces a full foot in diameter, weighing 50 pounds and more, have been fired. Size aside, the two types differ only in that one explodes on the ground, the other high in the air. Every year firework-makers build units 3" to 6" in diameter by the thousands, both in this country and abroad. The Italians in particular show a special fondness for aerial salutes.

Devices we discuss here generate trivial reports beside such gigantic aerial bombs; but there is no quicker way to draw heat than to make or sell these banned tools of corruption. One reason lies with the ignorance

of the Authorities. They know a cherry bomb when they see one, but haven't the foggiest about a six-inch aerial salute that could flatten your garage.

Enough moralizing. We admit grudgingly that heavy ground salutes should be banned, not out of some inherent moral squalor that taints American Youth, but from a general decline of values in the grim wake of the Age of Aquarius, something that has twisted our views of many goods in these uneasy times.

This chapter explores ground salutes in depth. It provides so much detail that few readers who can read—and the Republic sees fewer literati every year—would have trouble building them. That happens to be the author's last intent in unraveling this arcane lore. Indeed. A recurrent obsession with safety and responsible behavior surfaces in this terrible tract. Furthermore, readers are advised not to make any of the devices discussed, nor to violate any laws. Read this as a vicarious experience, in lieu of, say, actually buying a bag of M-80s and terrorizing mailboxes....

Before getting into the varied and occasionally elegant methods used to crank these units into operation, it is extremely important to understand phenomena involved, as well as the properties of materials, both alone and in combination.

EXPLOSIONS, TYPES I & II

A stick of dynamite explodes if triggered properly. So, in a sense, does a balloon when it pops. The phenomena are the same: fast outward expansion, a sudden release of pressure. The difference lies in mechanism and degree.

Some types of explosive pyrotechnics produce the equivalent of a balloon-popping report, what we'll refer to as a Type I Explosion. It results solely from sudden release of pent-up pressure, as from rupturing of a stout paper enclosure. The maroon serves as case in point. No longer made or sold, at least not in the United States, these units were golf-ball-size cardboard boxes charged with black powder, then wrapped tightly with strong twine, three layers, at 90-degree angles, followed by a dip in glue and a final wrap of paper. This made for an exceptionally uniform case of great strength. It took a hellish mesh of pressure to burst, and this offered a decent report. The key lies with mechanism of the report. It resulted from rupture or popping of the case, with sudden venting of pressure produced by black powder burning in confinement. Strength of the casing determines size of report, in any practical sense. Most agree that black powder cannot detonate.

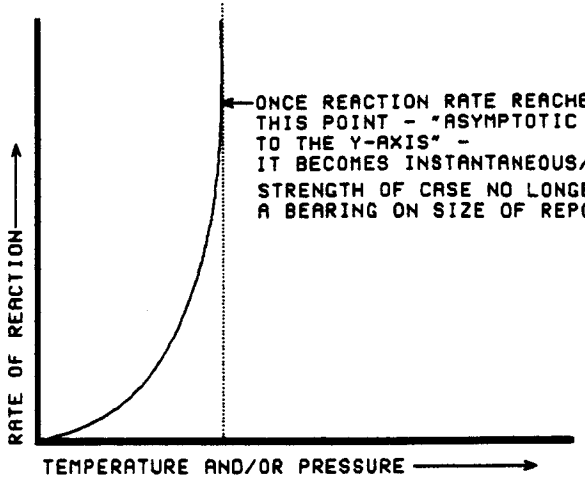
But tube-type casings used to make M-80s offer flimsy confinement compared to maroon cases. They suffer weak points at their end closures. Filled with black powder, they merely blow out the end caps, producing no report. Maroons give a clean if unspectacular bang when the pressure inside them suddenly pops the hard casing like a balloon.

Yet, experience proves that we can achieve loud, sharp, genuinely fearsome reports from the flimsiest of casings by filling them with compositions capable of detonation, the Type II Explosion. In this sense, detonation refers to propagation of the chemical reaction by a shock wave, rather than by rapid burning. The point at which rapid burning shifts into detonation is not always easily determined or clearly defined. Note the difference in the fundamental means of producing pyrotechnic reports. Type II Explosions depend upon the ability of the powder to detonate, as we have used the term here. Once detonation is underway, strength of the case contributes little to the size of the report.

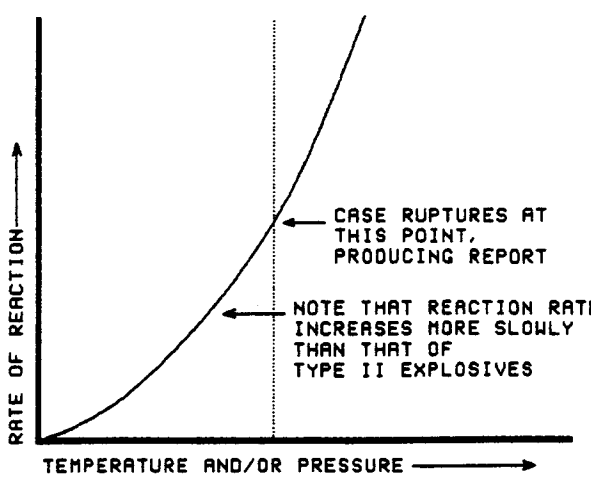
The diagram shows in highly expanded time frame that ignition of confined powder causes it to burn initially, but that burn-rate accelerates rapidly, until it becomes instantaneous. This, rather than rupture of the casing, generates a report.

On the other hand, note how sluggishly a Type I composition burns in comparison. At some point, determined by the strength of the casing, it will burst, venting pent-up pressure. That mechanism generates the report. Thus, strength of the casing means most in Type I, while ability of the powder to detonate means most in Type II.

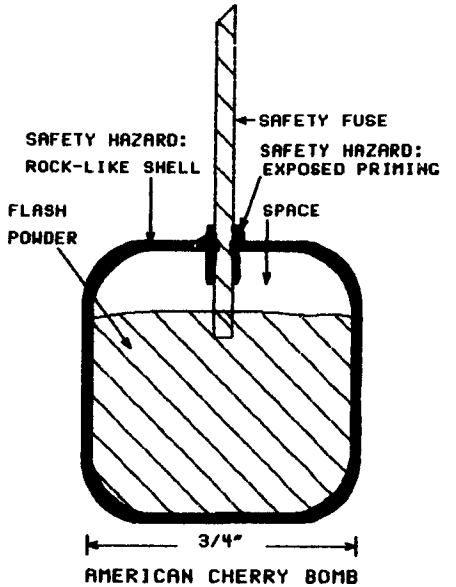
Black powder and weak flash powders, and this includes potassium/barium nitrate-based compositions, do not detonate. Those based on potassium chlorate or potassium perchlorate detonate. This makes for differences in



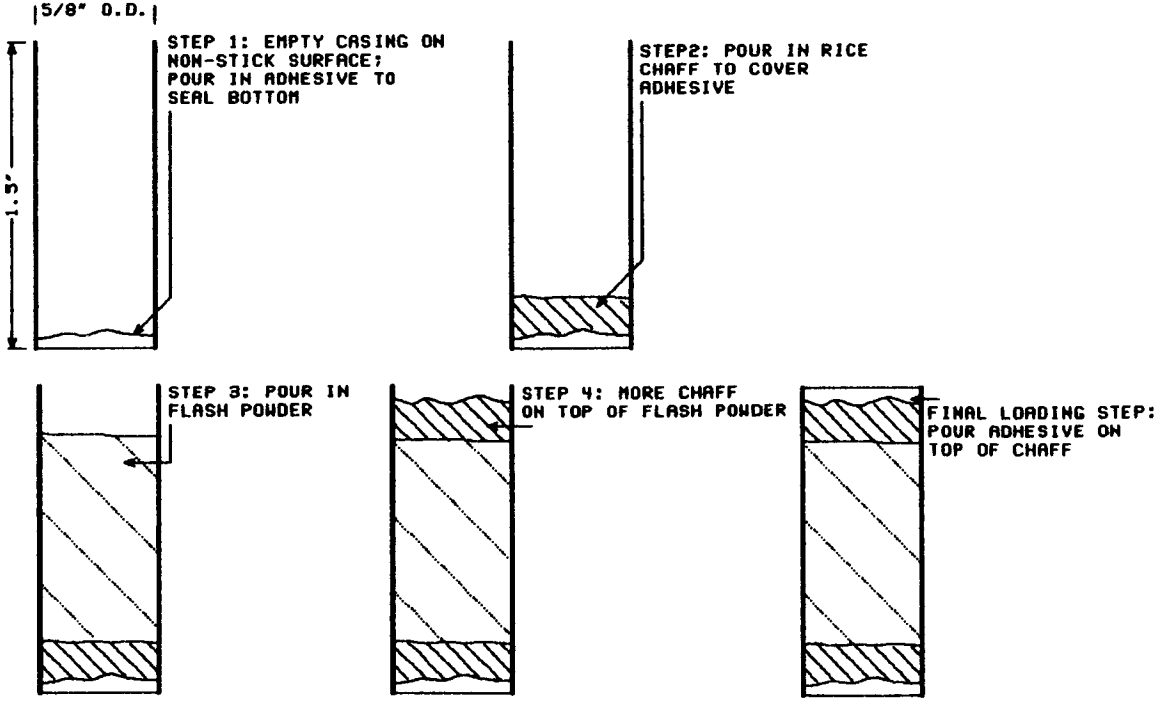
GRAPHIC REPRESENTATION OF PHENOMENA IN TYPE II EXPLOSION, OR DETONATION



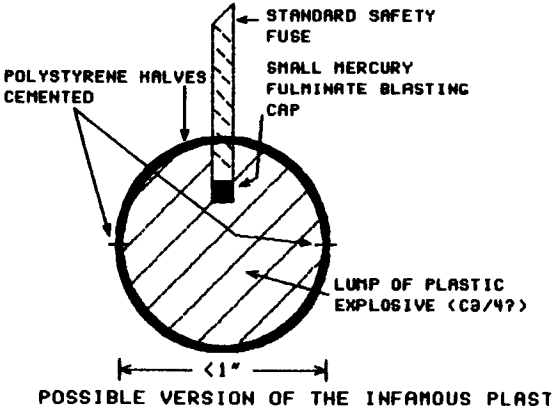
GRAPHIC REPRESENTATION OF TIME/PRESSURE PHENOMENA FOR TYPE I EXPLOSION



AMERICAN CHERRY BOMB



"BULK" MANUFACTURE OF TUBE SALUTES



POSSIBLE VERSION OF THE INFAMOUS PLASTIC CHERRY BOMB. RUMOR ONLY, OF COURSE.

their handling and loading properties we must observe carefully. To no one's surprise, powders capable of detonation are considered more powerful, and for that reason command greater respect.

Some compositions require no confinement to detonate in the truest sense. Silver fulminate painted on tiny toothpicks stuck in the ends of "exploding cigars," once sold as practical jokes, produces an extremely crisp, surprisingly loud report. Or take cracker balls, no longer sold, perhaps with good reason, since they looked so much like candy that the kids would sometimes gobble them, oblivious to their phosphorous or arsenic content. These too produced quite a sharp report for their size, and represented true detonation. (For readers too young to recall them, cracker balls were colored pellets about 3/8" diameter, made from tissue paper enclosing gravel and a friction-sensitive explosive mix that detonated when thrown against a hard object or stepped on. They're still sold, if you don't mind a trip to the Orient to get them.)

A badly made skyrocket, one with cracks in its propellant grain for example, will sometimes let fly with an impressive boom about ten feet off the launch pad. (Ex-model rocketeers: Didn't you once bore a hole into the center of the black powder propellant to achieve a sharper thrust curve? The engine blew up shortly after launch, destroying your rocket, yet you recovered the strong engine casing intact. Most agree that black powder cannot detonate under practical conditions. Another example of the Type I Explosion.)

EXPLOSIVES: THE WORD ACCORDING TO BATF

The author's first run-in with the Bureau of Alcohol, Tobacco, and Firearms, aka BATF, and the then-new explosives laws spawned by the infamous Gun Control Act of 1968, amended in later years, occurred in 1971. He had become involved in the pyro hobby scene, and had latched onto a source of special fireworks, the kind shot at public displays. It was near Christmas, so he decided to order a small ($125) selection of 3" aerial shells to liven up the New Year's Holiday for his family and friends, and fired off an order to a vendor.

Instead of shipping the fireworks, they sent him a polite letter asking to see his Federal Explosives Permit.

Explosives? What in the Devil's name had these innocent fireworks to do with explosives?

It took a visit to the nearest BATF office, but he found out quickly that the new law had placed display fireworks in the same league with low explosives, of which black powder is the prototype. At the time, the BATF agents (who, in truth and fairness, proved to be OK guys who went out of their way to help that bumbling 19-year-old comply with the law) allowed that anything that held more than 5 pounds of black powder was considered a low explosive, subject to laws governing purchase, transport, storage, and usage of same. That 5-pound limit later climbed to 50 pounds under pressure from the gun lobby, but special fireworks of whatever size or weight remained low explosives, or "Explosives - B." (Dynamite and C4, for example, are high explosives or "Explosives - A," while common fireworks sold to the public in some states qualify as "Explosives - C." These A-B-C categories originate with the Department of Transportation.)

Up until the time special fireworks became explosives by decree of law, BATF agents had had a pretty clear notion of explosives and their classification. Explosives were homogeneous materials used in blasting and munitions. High explosives were any materials that a No. 8 blasting cap would detonate when unconfined (that's a big blasting cap), while low explosives were materials, such as black powder, that could be caused to "deflagrate" when confined. Exemptions included matches, components of small arms, and small fuse.

But where in this formerly simple scheme did fireworks fit? BATF finally acknowledged their singular niche in its publication ATF P 5400.7 (11/82) by noting (that) "Their manufacture and distribution require the manipulation of explosive materials in a manner that is utterly unique in the explosives industry."

That innocent admission automatically tied fireworks to the explosives industry, a point many would challenge. Nobody gives up turf voluntarily, and BATF is as big-brotherish as they come.

So what does it all mean for those who wish to pursue pyrotechnics as a hobby? You must attempt to comply with a nebulous law as interpreted by BATF. Careful reading of its booklets shows that gray zones exist still; that apparent internal inconsistencies are symptomatic of BATF's essential ignorance of the many and varied aspects of recreational pyrotechnics. A Democratically controlled Congress made the law discretionary to a point that passeth all understanding.

Can you get into the fireworks trade? You can try. A few families and large companies who do not like competition have locked up the bulk of the commercial display business. (An acquaintance of the author's related an anecdote about the patriarch of one family. He alleged that the guy gave "carloads" of Class C fireworks to bidders' families and friends out of "consideration" for awarding him display contracts. This does not surprise those who know men and politics....)

A FLASH HISTORY OF AMATEUR PYROTECHNICS

Until the late 1960s there was no history worth telling not already told in grim, sporadic accounts of basement bombing, always with loss of sight or a few fingers when things went wrong.

The term "basement bomber" rises from obscure origins. Some believe it coined by the anti-homemade fireworks crowd. It described those who dabbled in explosive alchemy in the privacy of their homes and back yards. It was the late fifties, model rocketry's nascent time, and manufacturers damned well didn't want to lose sales to amateur engine-builders.

That early era thrust technology on us without preparation needed to handle some aspects of it safely. In the course of pursuing a government- and popularly-approved technological path—the "Sputnik Syndrome"—some young, would-be, poorly supervised propellant chemists injured themselves or started fires. They became known as basement bombers, and that foolish misnomer stuck.

True basement bombers are terrorists, criminals, and other vermin who fabricate explosives for the express purpose of causing harm, usually to innocents. The term has no business being applied to teenagers whose curiosity about and fascination with combustibles will not be denied. The author has known persons whose mastery of pyrotechnics could produce vast destruction if turned to that wicked end, something that has not happened. (And why should terrorists fool with the weak, low explosives used in pyrotechnics, when the Eastern Bloc supplies them with the latest in military plastique? The Reds will probably throw in a case or two of their famous Afghanistan grenades, which come disguised as toys and dolls, just the trick for maiming children, which surely rates high on any list of human priorities....)

Then in 1968 a place called Pyro Hobby Shop set up in Virginia. It sold raw chemicals and paper casings by mail. In addition to the traditional staples of salute chemicals, fuse, and casings, it offered tools of high quality and casings for roman candles, fountains, cones, and whistles. More, it offered literature—information, knowledge. At last pyrotechnics would be discussed like model airplanes or golf.

This opened the door to a renaissance in an art long kept secret. Pyrotechnic wisdom up to that point had been closely held by the few families who controlled exhibition fireworks, esoteric lore never shared with outsiders. The pyro cult grew to the point that, around 1969, it coalesced into an organization known as the Pyrotechnics Guild International.

It published its own newsletter of admirable but uneven quality—admirable given the resources and circumstances of it—and it grew. Two factions hooked up in the early seventies to publish American Pyrotechnist Fireworks News, a considerable jump in quality of publication over either of the two periodicals that melded to make it.

The PGI held meetings and staged displays, members exchanged correspondence. Pyro flourished. We saw new ideas, new material, innovation unlike anything seen in the previous 50 years in the space of a decade. Pyro Hobby Shop moved to Utah and resurrected itself as the now-defunct WesTech Corporation, the brainchild of Ralph Degn, lately of the display fireworks firm, "Fireworks West!" Years ago, Degn was cursed in some circles, praised in others. We suspect that history will recognize him as a major contributor to the advancement of both amateur and professional pyrotechnics—but that's another tale.

There were casualties. One particularly active pyro with whom the author exchanged letters and ideas circa 1971 was reported to have seen his lab go up in flame. He ceased (was ordered by the court?) all contact with former cronies in the pyro cult.

But sources began to dry up. BATF attacked, charging that vendors were selling "kits" for tube salutes and so forth. Some companies were in fact doing this. Late in 1969, one firm sold casings of excellent quality,

along with what it called "banger powder," which turned out to be a potassium nitrate/aluminum/sulfur flash composition that fluffed the end caps off when lit. The stuff proved about as mean as Jetex pellets (does anyone recall Jetex engines?).

The late 70s-early 80s were amateur pyrotechnics' salad days. Meetings, displays, shows of skill and craftsmanship that outdid the professionals in finesse, if not scale.

The future of amateur pyro does not exactly dazzle those who have analyzed large trends in human behavior, both here and abroad. That sour scene comes under review at the end of this chapter.

MATERIALS

Of dozens of materials used in pyrotechnics to produce those wonderful effects of color, glitter, whistle and bang, only a handful concern us here: oxidizers, fuels, fuses, cases, and "other agents."

Every fourth-grade graduate or Mr. Wizard watcher understands that burning involves combination of fuel and oxygen, usually with production of flame, or at least heat. Pyrotechnic effects call for this oxidation to speed up considerably. Salutes demand that it happen instantaneously.

We have powders, known as oxidizers, that yield oxygen to speed our fiendish reactions along. As the first block in building up to salutes and their mysterious manufacture, understand oxidizers and their properties.

OXIDIZERS

POTASSIUM NITRATE

The mainstay of all pyrotechnic oxidizers is potassium nitrate, chemical symbol KNO3. Gunpowder consists of potassium nitrate, charcoal, and sulfur in a weight ratio of 75:15:10, though the mix has to be moistened, ground in large mills, granulated, and otherwise processed before it becomes true gunpowder. A simple blend of these three ingredients without that special processing yields a composition that just barely qualifies as flammable, much less explosive.

Potassium nitrate is the most benign of our oxygen sources. We can mix it with most fuels without fear of ignition, much less detonation, until we light it.

Known also as saltpeter, it used to be that you could buy potassium nitrate at the corner drugstore. In some cases you had to sign for it, just like codeine-containing cough syrup today. (And as sources of social woe, what lessons come from the exponential rise in drug-abuse, compared with abuse of lil' ol' saltpeter....?)

Potassium nitrate suffers one major physical property that leads all who handle it to curse it. Left undisturbed for a few days, the powder hardens into a rock-like mass which, depending on poundage, may literally require blows from a sledge to break. From there, the chunks have to be re-powdered in a mortar, or, better, a motorized ball mill (a rock polisher loaded with 1/2" hard lead balls will do nicely).

Anti-caking agents help but do not eliminate the problem. Those who use potassium nitrate should perfect a system for powdering it that does not monopolize their time.

BARIUM NITRATE

This heavy-metal relative of potassium nitrate surrenders its oxygen less willingly. "Gunpowder" made with it is good for absolutely nothing. But when used in flash formulas listed in the table, for some reason it outperforms the potassium compound, though it too will give us only an explosion, not a detonation.

A mix of barium nitrate with sulfur and aluminum makes a flash powder hard to ignite, but which burns surprisingly fast when unconfined, and with a blinding light; yet confinement leaves us with that sorry limp report of the other nitrate-based comps. Indeed, in most cases, a nitrate tube salute will simply blow out its end-caps and fail to rupture the case at all.

Sources praise nitrate-based powders for their safety (though we find disagreement over the sensitivity of a mix of sulfur, pyro aluminum, and barium nitrate), but acknowledge that they lack power. In fact, to get a boom at all requires an extremely strong case of uniform strength that leaves no weak path through which pressure can vent. This gives a Type I or "balloon popping" explosion.

Barium nitrate plus aluminum and sulfur indeed makes flash powder, but one whose use remains obscure, primarily because it does not go BOOM under real-life conditions. Its own particle size and that of the aluminum affects its unconfined rate of burn, but even microfine powder will not get the composition up off its knees. For that we must turn to a serious oxidizer, potassium perchlorate.

POTASSIUM PERCHLORATE

Potassium perchlorate reigns as the premier pyrotechnic oxidizer for non-charcoal-based formulas. Most compositions that use charcoal as a fuel burn well enough with potassium nitrate, while those that do not use charcoal must step up to the perchlorate, chemical symbol $KClO_4$. Today it has established a place as the foremost oxidizer in salute powder, at least in the semi-civilized world.

This salt dissolves poorly in water and for that reason, once powdered, tends to remain so and resists that awful caking of potassium nitrate.

This compound contains plenty of oxygen and offers it more eagerly than potassium nitrate, yet not to a point deemed hazardous, at least by pyrotechnists' bent notion of danger. Nor does it call forth that grim specter of spontaneous combustion so common in obsolete formulas. Certainly, mixes of it with various fuels will ignite by friction, spark, and pressure; but spontaneous ignition is distinctly uncommon with sane compositions. We do not dread the perchlorate as we do its ferocious cousin, the chlorate.

POTASSIUM CHLORATE

Veteran pyros get tense when you mention chlorates. Although this compound ($KClO_3$) holds less oxygen per molecular unit than the perchlorate, it releases it far more eagerly. In fact, barium chlorate—don't even have a nightmare about playing with it—yields so much energy as it decomposes that the right impetus can detonate it. The barium compound has proven so unstable that it does not appear in the literature of salute compositions, even though it might give the greatest report per unit weight of all formulas, at least if you could get it mixed and loaded before it decided to blow off.

Potassium chlorate has shown a bit more stability, and has served for many years as an oxidizer that gets things to light and stay lit under extreme conditions. For example, a starshell bursting hundreds of feet above the appreciative crowd hurls burning stars outward at well over a hundred miles an hour. The wind at that speed will extinguish a match, as well as many star compositions not tenacious enough to resist it. Those made with perchlorate may lack the vigor to keep burning. Thus, we may have to resort to a stronger agent, the chlorate, to avoid "black shells," ones that burst but leave the sky empty of fire.

Some hold that chlorates give deeper color in stars. Barium chlorate makes the point. Its emerald green flame literally takes the breath away. (Useless fact: These stars give off a characteristic hiss as they burn.) Others acknowledge this edge, but shy away from barium chlorate out of sober fear. One of several tragic anecdotes George Plimpton recounted in his book, Fireworks, tells of a fatal blast that may have been triggered by spontaneous detonation of barium chlorate-based stars. How ironic that this type of mix is intended only to burn with a stunning deep green, not to explode.

As for potassium chlorate's use in salutes, we find it mentioned in countless older texts; but do not let that fact lull you into giving it serious thought. A portion of an Oriental fireworks text translated some years ago speaks of a chlorate-based composition—with the naturally acidic element, sulfur, yet—as if it were standard (at the time, it was); but chlorate-based salute powders pose unacceptable hazards. Here are the reasons:

In the presence of moisture and a trace of acid, potassium chlorate forms chloric acid, which will ignite spontaneously, and that usually means a big and highly destructive boom when we least expect it.

How do chlorate-based flash-powders come by moisture and acid? Atmospheric humidity is enough, especially in the presence of acid (the kind found in cardboard tubes that form salute casings, and in the glue used to affix paper end caps). Sulfur and sulfides use that same moisture to form variations on sulfuric acid, which will ignite chlorate-based powders on contact.

As if spontaneous surprises weren't enough, the mixing of powders subjects them to shock and friction, and often to static electricity. Chlorate particles seem to vie with one another to see which will be the first to ignite out of gentle rubbing.

The ideal means to combat the chlorate menace would be never to use the rotten stuff at all; but pyro evolved in that let's-take-a-chance era of the fifties and sixties, and it was considered quite routine to mix the old chloro with aluminum. Even further back, in the twenties, thirties, and forties, it was mixed with sulfur or antimony sulfide, practically guaranteed to detonate as you pour it into a casing....

Smart pyros saw the danger inherent in chlorates and undertook to minimize it while retaining the compounds as options for special comps. If acid formed in the presence of moisture was the culprit, might it not help to add a small amount of base to neutralize any acid?

The answer was yes, and the chemicals most commonly employed were magnesium carbonate and barium carbonate, known as "phlegmatizers" out of this taming effect. The recommended amounts were about 1/2 percent by weight of the oxidizer, mixed thoroughly with the chlorate before blending it with anything else. Magnesium carbonate gave us a freebie in that it retarded caking when added in proportions up to 3 percent.

Some compositions were by their nature so benign that we could use potassium chlorate with little fear. Analyze this formula for red stars, quoted in Ron Lancaster's book:

Potassium chlorate	70
Strontium carbonate	15
Red Gum (or equivalent)	10
Dextrin	4
Charcoal, 150 mesh or finer	1

That 15 percent strontium as the carbonate, which makes the comp burn red, is more than enough to neutralize any acid, though, given a choice, no one could fault those who would substitute potassium perchlorate....

On some points it pays to be repetitive. Cautions to avoid potassium chlorate, and especially barium chlorate, cannot be repeated too often. According to Weingart's outdated classic, Pyrotechnics, about 90 percent of industrial accidents of his era—the hubba-hubba forties—traced to combinations of potassium chlorate and sulfur-containing chemicals.

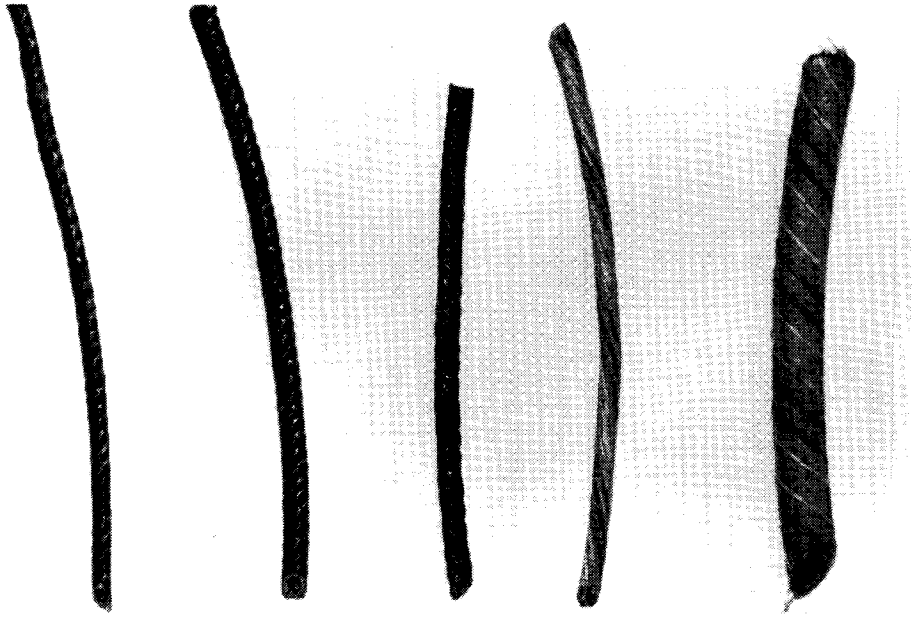
Regard chlorates as you would a foe: Do not underestimate them.

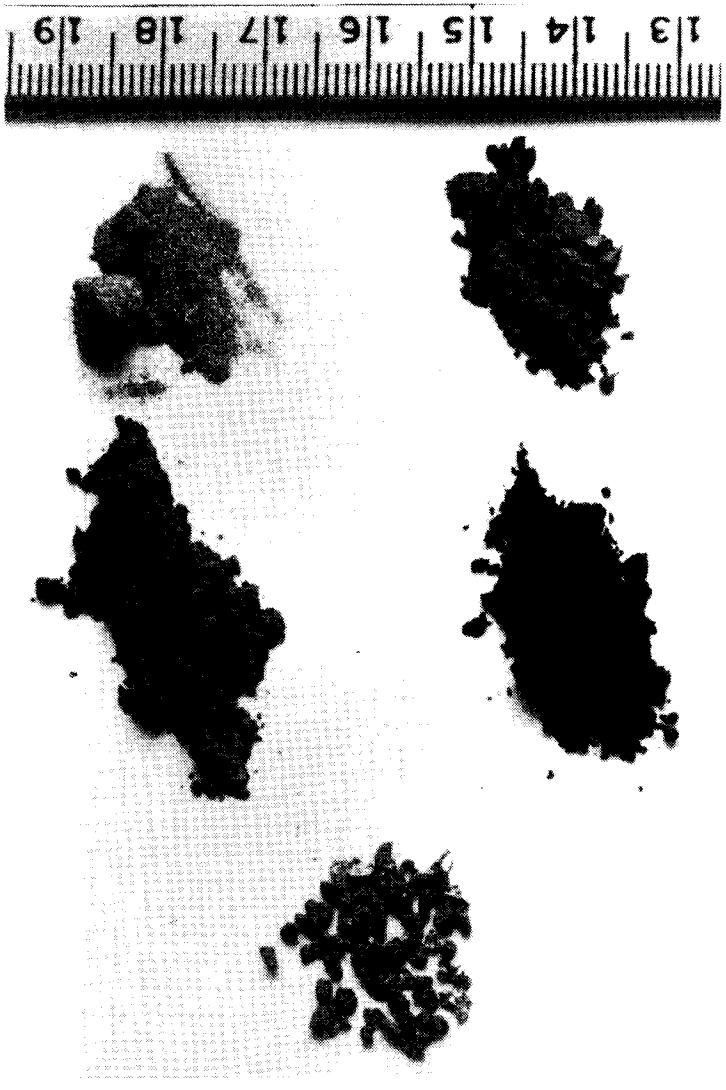
OTHER OXIDIZERS

Now and again we see mention of purple potassium permanganate, ammonium perchlorate (makes the best blues in all of pyro), ammonium nitrate, and a smattering of others. But as far as salutes are concerned, special drawbacks of these obscure chemicals take them out of serious contention as components in salute powder.

FUELS

Since even professional pyrotechnists aren't allowed to use report-makers that incorporate their own oxygen, i.e., high explosives such as nitroglycerin and the military plastic, C4, we must mix the oxidizer with





TOP LEFT: Fuse. From L to R: "small" red fuse; "large" red fuse; single-stranded-core green fuse; uncoated fuse; 1/4" time fuse used in aerial shells.
TOP RIGHT: Metal powders. Clockwise, starting from upper left: Mg/Al 50/50 alloy, approx. 150 mesh; dark pyro aluminum; true Black German pyro aluminum; granular titanium, 20-40 mesh; finally, aluminum purchased as "Black German" about three months after the true Black German, but this batch clearly lighter in tone, indicating larger particle size.

suitable fuel to have a workable blend. Of all combustible materials, a mere few have earned slots as staples in salute formulas.

ALUMINUM

Firecrackers, in the strictest sense, do not produce a flash of light when they explode. Flashcrackers do. Not only that, but to obtain equal reports from firecracker and flashcracker powder, we must use more of the firecracker comp, or a more virulent blend, almost always a mix of potassium chlorate and sulfur or one of the sulfides. As salutes evolved, economics came into play, and through some twisted Darwinian selection process virtually all salute compositions today are in fact flash powders, not firecracker powders. That means a mix of powdered aluminum, oxidizer, and sometimes other ingredients, such as sulfur or antimony sulfide.

Feeling the powder we rolled out of flashcrackers or that dribbled out of tube salutes, we saw clearly that it silvered the fingertips. Therefore, it must contain powdered metal. Aluminum proved the correct guess. Investigation showed that the particle size of aluminum that matched the appearance of salute powder to be 300-400 mesh.

A few words about "mesh." The most commonly used means to designate particle size in pyro is mesh. Thus, a 24-mesh screen has 24 wires per inch running at right angles with 24 other wires per inch. Particles that will pass this screen, but are not appreciably smaller, are said to be 24 mesh. Now, the diameter of the wire comes into play with much finer mesh, yet we still use the system to approximate particle size. Lancaster's and Ellern's texts provide tables of particle size in more conventional units that correspond to various readings of mesh.

We appreciate on an intuitive basis that, the greater the surface area participating in a reaction, the faster it proceeds. A log may take hours to burn, while several square yards of paper made from one log can burn in less than a minute, if spread out and given plenty of oxygen. Pyros knew from experimentation that bright silver aluminum powder—say, 150-250 mesh—burned more slowly, at least in the open, than did this dusky silver, nearly gray powder of 300-400 mesh, referred to as "pyro" or "dark pyro" aluminum. It was reasonable to suppose that more finely divided aluminum would offer even livelier performance in salute powder, so the call went out for the tiniest aluminum particles in the land.

The answer came as a dark, almost black powder that earned its distinctive tag, Black German Pyro aluminum; black from its appearance and German by pedigree. Hang around chemistry types long enough and you learn that all metals turn black if powdered finely enough. When first offered for sale in 1970, Black German's largest particles were pegged at 425 mesh. The latest catalog from Square Lake Enterprises claims 600 mesh.

Refer to the photo of several metal powders. Both samples labeled as Black German Pyro aluminum came from WesTech Corporation in 1970, yet one powder is clearly darker. The other lay between true Black German and conventional dark pyro in its shade, indicating a particle size somewhat finer than dark pyro but not up to the real thing, Black German.

Eerie things happen when we work with fuel this finely divided. For example, flash powder made with bright or regular pyro aluminum burns aggressively in the open, but not enough to intimidate us. A tiny pinch of the black mix goes up in a startling WHUPPP! when lit, without the slightest confinement.

In a fit of madness in the summer of 1970, one young pyro mixed 16 grams of potassium perchlorate and 8 grams of Black German Pyro aluminum, because he had tired of mixing 2-gram batches for individual salutes. He handled the stuff at arms' length, and protected his face, eyes, ears, and hands. He blended the deadly matter openly on a sheet of paper, with precautions against static electricity. When the concoction was ready, he poured it into a paper cup.

A little devil lives in us all. This experimenter had seen how fast, almost explosively, the new black mix burned, unconfined. So late one fated July afternoon he decided, purely for the sake of scientific research, to see what would happen to 24 grams of this strange and deadly mix ignited in a paper cup. He stuck one end of a 2-foot length of green fuse in the open container, placed it on a lonely mound of dirt, lit the fuse, then sped to a safe distance.

Special contexts activate intuition. This decadent experiment was one of them. By the time that grimly spitting fuse had crept to the edge of the paper cup, our young pyro had sensed what would happen....

KA-BOOOOMMMM!

Burn? Unfettered and open in a paper cup, the powder detonated. Particle size is but one factor that determines rate of a chemical reaction. As a rule, speed doubles with every ten degrees centigrade rise in temperature. This makes for an exponentially accelerating curve that quickly becomes asymptotic to the Y-axis, i.e., happens so fast it constitutes an explosion. Temperature is directly proportional to pressure. Increased pressure, as from a confinement in a paper case, can detonate an otherwise sluggish powder.

But flash powder made with this impalpable black aluminum burned so quickly that it generated a pressure wave. This confined it as surely as a paper casing would have. It behaved accordingly and exploded. It could have done so while being mixed.

After this seriously depraved exercise, those 2-gram batches seemed plenty big....

A stark and sordid tale with important lessons for those who contemplate working with Black German Pyro aluminum. The smart would-be pyro would think four or five times about fooling with it. A smarter one would conclude that there are safer ways to make a bang.

(One further observation points up the quizzical and sometimes paradoxical conduct of explosives. The paper cup had its bottom ruptured, but otherwise survived intact, this despite a blast that shook the neighborhood. Destructive effects of pyrotechnic explosives, in contrast to high explosives that generate far more gaseous reaction products, seem sharply localized, to mere inches in the case of tube salutes. Thus, use of thick gloves and fairly unpretentious tongs can save your hands in the event of premature ignition. A word to the wise....)

MAGNESIUM AND MAGNESIUM/ALUMINUM ALLOYS

Initiative is another fiend that possesses the soul. It might make the ambitious craftsman want to get his hands on magnesium, which, last time we checked, came in powders as fine as 325 mesh. Now, 100 mesh magnesium mixed with bland potassium nitrate burns so fast it's scary. The thought of mixing 325 mesh mag with any oxidizer probably inspired Hieronymous Bosch for a few brush-strokes of "The Garden of Earthly Delights."

Anachronisms aside, this metal fires the pyrotechnic imagination, at least before considering its minuses, out of remembrance of that high-school chemistry experiment in which the instructor gravely donned safety gear, then held a two-inch strip of pure magnesium to the mean blue flame of a Bunsen burner. We had to shield our eyes from the blinding light when it took fire. Wow! A metal, of all things, that burned! You couldn't do that trick with aluminum. And once it got out that powdered magnesium was available....

But magnesium offers no advantages and too many headaches. Cost ranks first. It ranges from outrageous to lethal, depending on season and source. Second is reactivity. Mixed with an oxidizer, magnesium will ignite from friction, static electricity, and shock more easily than the same blend with aluminum. Third, it does not wait for ignition to begin oxidizing. Even chunks of the stuff grow a coat of dark gray magnesium oxide merely from exposure to air. If mixed today, the stuff may be unusable next week. (And if you added sulfur, do plan to store the stuff out of doors. Atmospheric humidity and chemical reactions tiresome to recount generate hydrogen sulfide. Imagine the stench of fifty rotten eggs and you get the point.)

We are concerned mainly with communicating the way to make effective bangs, but will note in passing that magnesium powder was once used to produce colored flash reports. Skipping the electron orbitals of it, note that "burning" barium gives green light, strontium gives red, sodium gives yellow, copper gives blue, and certain mixtures give purple. Look over the magnesium/nitrate flash formulas quoted in the table. Supposedly, the report-flashes were colored (polyvinylchloride and hexachlorobenzene furnished chlorine to the reaction to intensify the color). But with nitrates alone, the bangs weren't worth much, and addition of potassium perchlorate killed the color. Besides, the powder quickly oxidized in the case. If you mix it today, better torch it tonight.

We also have magnesium/aluminum alloys in various ratios, 40/60 to 60/40 being a common range. The photo shows a 50/50 alloy powder of near to 200 mesh. These are more expensive than plain aluminum but less so than magnesium. Though more stable than magnesium, they show greater reactivity than aluminum. They offer no advantage of worth in salute powder but have found use in special star compositions.

The safest, simplest flash formulas contain various mixes of oxidizer and aluminum, reported ratios ranging from 2:1 to 4:1. Flour-like potassium perchlorate mixed with dark pyro aluminum serves quite well, thank you. The well-heeled pyro might step up to Black German aluminum, at least if he is willing to travel at his own risk....

Other formulas call for sulfur or antimony sulfide, usually in the same weight proportion as the aluminum. Authorities state also that this heightens the sensitivity to friction, pressure, and flame. Get by with the safest mix possible.

We have quoted those fearsome chlorate-containing formulas purely out of indecent historical interest, just as some medical texts mention the ancient customs of leeching and bloodletting. None have a place in modern practice.

TITANIUM

Pyrotechnics has a way of flawing beauty with danger, a perverse irony that plagues many of its best effects. The titanium flash bomb is one of the simplest yet most beautiful and spectacular of all pyrotechnic effects—and one of the most devastating should it ignite prematurely.

All metals burn if powdered finely enough. Titanium lies above magnesium but below aluminum in the size of particles that will burn easily. Small gravel-sized, known in the trade as 20-40 mesh, with a spongy texture, is used with good effect. The source of this otherwise expensive metal is said to be the leavings of the aircraft industry, which uses titanium for its high strength/weight ratio.

And all that need be done is dump in a helping, say, 30 percent of the weight of the flash powder, in the casing, and—presto: titanium flash bomb. An M-80 so made will throw out a gorgeous, brilliant sphere of burning titanium in a 20-foot radius. Absolutely breathtaking.

Of course, if it went off while you were holding it, or maybe inside your car...well, wouldn't we want pictures of the carnage for the Enquirer? If you were looking at the damned thing when it went off you could be blinded. Your car could go up in a fireball; the house could burn down. If you shot one on dry grass, you have a fire the size of a tennis court on your hands (and take it from those who have been there, the flames will defy all attempts to stomp them out).

So, though you see titanium mentioned in other texts, believe it that it belongs only in the repertoire of seasoned pros. Remember that those who would work with pyrotechnics must take precautions against the absolute worst that could happen. Assume as much risk as you want with your own hide. But be damned careful of the lives, health, and property of others.

Titanium has enjoyed huge popularity, and has found use in fountains, stars, and so forth, beyond this limited scope.

OTHER AGENTS

CAB-O-SIL

This concern with prevention of caking led to introduction of anti-caking agents, of which Cab-O-Sil was the main one, sold under the proprietary name "Salutex" by WesTech corporation and lately "Chemite" from Square Lake Enterprises. It is composed of silicon dioxide (sand) in particles on the order of a micron in diameter. The name "Salutex" apparently derived from the theory that it made for a bigger bang by keeping the particles of a flash mix separated on a microscopic level, thus exposing greater surface area for burning.

Cab-O-Sil did indeed prevent caking, especially of potassium perchlorate. As to whether it gave more bang in the bargain, the author cannot verify. Prior to 1973 he made salutes both with and without Cab-O-Sil, and could discern no change in performance.

MAGNESIUM CARBONATE

Already mentioned in connection with chlorates. In addition to neutralizing acids, it helped keep powders free-flowing in a 1/2 to 3 percent mix.

BARIUM CARBONATE

A base, but lacks the anti-caking properties of the magnesium compound.

POWDERING AND MIXING

Pause here to admit that blending these deadly ingredients requires a bit of different technique than that of your last failed brownie mix. In addition, we seek a property few brownies possess: elegance. We achieve elegance, like Nirvana, by thoroughly mixing ingredients which themselves have been prepared by grimly determined powdering.

Start with the oxidizer. Powder it as finely as practical. Rarely, it will come out of the shipping container in a fine-mesh state, preferably finer than 200 mesh, but even then is likely to be caked badly. These clumps must be broken. For small quantities a porcelain mortar and pestle and enough effort to blister your pestle-hand and make your wrists ache for a week can grind it into something that approaches flour or confectioner's sugar in consistency: an impalpable, white powder.

The first of many cautions: NEVER GRIND MORE THAN ONE CHEMICAL IN A MORTAR. Grinding produces conditions conducive to detonation. Potassium perchlorate and sulfur, ordinarily "sensitive," yet not in the same ticklish league with chlorates and sulfur, can detonate if ground together in a mortar.

Second, if you have occasion to grind fuels or oxidizers, procure separate mortars and pestles for the two and don't get them confused. Use one only for oxidizers, the other only for fuels. (The powdering of chlorates should never come up, but we might as well mention a third lesson while we're about it: if you intend, out of whatever demented motive, to grind chlorates, use a third mortar and pestle set exclusively for them. Never confuse them. The error could cost you your sight or hands. Mark them with indelible ink so as not to mix them up.)

To the end that the oxidizer remain free-flowing, add an anti-caking agent prior to powdering. Magnesium carbonate or Cab-O-Sil in 1/2 percent by weight of the oxidizer should suffice; but do not expect miracles from these agents. Mix the oxidizer and fuel(s) as soon after the powdering as practical.

You will not be using a mortar and pestle to further reduce the particle size of aluminum. You may, however, have to break up hard clumps that form in Black German Pyro aluminum and extremely fine magnesium powder as it sits on the shelf, years, unused. But you cannot, or at least should not, use porcelain. Porous, unglazed porcelain takes up particles of the metal. Once you have used a mortar for aluminum you can never use it for anything else. Ideally, you should used a glass mortar and pestle. It has smooth, nonporous surfaces, and the forces involved are simply those required to break up chunks, not further powder the material.

How can you tell when all the lumps are gone? Pass the powder through a 40-mesh brass sieve, though 24-mesh—about the size of common window screen—will do in a pinch. Take the globules that accumulate and run them through the mortar again until all material passes the mesh freely.

Use separate screens for fuel and oxidizer, and a third one solely for chlorates (in fact, the fireworks trade commonly keeps entire buildings separate from the rest of the compound if chlorates are used in them).

A poor man's method for re-powdering fuels is to place the caked material in a 1-gallon plastic freezer bag, then roll the lumps out with a rolling pin. This suffices in most cases, but be aware that it punches tiny holes

in the bag, such that your work surface and work room should be prepared to handle stray fuel; and, as always, you should wear a respirator when working with finely divided matter. Adding 1/2 percent by weight of Cab-O-Sil to the fuel at this stage will not hurt.

Flash compositions that use more than oxidizer and aluminum demand another stage in mixing: blend the aluminum with other fuel elements before mixing it with oxidizer. This can be done by passing the ingredients repeatedly through a 24 or 40 mesh sieve, with exemplary results, but inevitably produces clouds of finely divided aluminum that could explode from a static spark. An alternative method is to mix aluminum and sulfur by placing them in a gallon plastic freezer bag and rolling them between the fingers until a homogeneous mix results.

At this point, we have oxidizer and fuel or fuel-mixture. We must combine the two. Here things get nervous, because the combination produces an explosive that we must handle and store.

Older texts casually recommend passing the whole works through a sieve. The Japanese used screens made of hair, with the caution not to "force" the mixture. The Americans merely warned the operator not to scratch a metal screen with the fingernails, since this could detonate the mix. As far as this text is concerned, do not blend flash powder by passing it through a sieve of any kind, even though that method produces genuinely thorough mixing.

One technique the author used years ago without accident was to place oxidizer and fuel on a large sheet of paper and roll the two powders back and forth using a smooth metal or rubber spatula, carefully avoiding friction with the paper, until a uniformly dark appearance is achieved. Another technique calls for pouring oxidizer and fuel in one of those gallon plastic freezer bags, then gently rolling the mix to uniformity with gloved hands (right....). Seriously, that second method could be used for bright aluminum/perchlorate compositions with little relative risk. It would not suit dark or Black German aluminum.

As we have mentioned previously, and illustrated in a grim incident, the particle size of the aluminum determines what mass of powder constitutes an explosive when unconfined. With a mix of sulfur, bright aluminum, and potassium perchlorate, this mass probably rates 200-300 grams, extrapolating from what other sources have quoted. With ordinary dark pyro aluminum, a hundred grams of this formula should be considered tops. Black German Pyro comp occupies its own ruinous class. Consider it explosive, unconfined, in any quantity. Consider potassium chlorate mixed with any fuel explosive whether confined or not.

FUSE

Unless you intend to fire them using electrical squibs, you will need fuse in order to construct tube salutes. Of the several types that could be had, only that known as plastic-coated safety fuse will suit, in addition to being about the only thing you can get nowadays....

This refers broadly to "green" and "red" fuses, used for decades in the manufacture of domestic fireworks, and, to a lesser extent, in the blasting industry. One sees this same green fuse poking out the center of silver salutes, or out of cherry bombs like some evil stem. The author has never seen true 1/8" fuse offered for sale to amateurs, though it can still be found on "M-80 Smoke" and such, limp remnants of finer days. Purists sometimes buy those sorry smoke pots to salvage the fuse, just to maintain a sense of spiritual righteousness in salutes they use it to concoct.

The fuse you are most likely to find sold via mail measures 3/32" diameter, carries a green plastic coat, and a single-fiber stranded core. Other than lacking the charm of the larger fuse, it serves well for its purpose, the delay and sure transfer of fire.

Green fuse—all coated fuse the author has tested, in fact—burns underwater, a point of dubious benefit to hobbyists except when that little demon inside makes us tape a rock to a salute and toss it in the creek, a depraved act good for a startling WHOOMPH!, with appropriate distress on the water surface, strangely reminiscent of a midget depth charge.

Examine a length of coated fuse. It resists breaking except to a full pull. It burns reliably underwater. In

fact, you can tie it in knots, twist it round and round, then crush it in a vice—and it will still burn reliably end to end while still clamped in the jaws of the vice. Green safety fuse has proven a surprisingly durable and dependable staple in pyrotechnics.

Other incarnations used to be sold. There were two varieties of red plastic coated fuse, one thinner than 3/32" the other just under 1/8" diameter, both with single-stranded cores. (Strands refer to lengths of thread-like fiber, not the powder core. In general, the heavier the powder core of the fuse, the more strands of fiber required to help it maintain its integrity.) Some sources held that the red fuse designated lack of side spit. To demonstrate the point, take a length of your green fuse (and samples of red fuse, if you have any left over from the Woodstock era....) and arrange them to burn while you observe.

As you light the green fuse, it will spit yellow flame and sparks two to three inches out the end. This is known, appropriately enough, as end spit. But watch the fuse as it burns. It throws out sparks and flame from the sides as it consumes itself. This is known as side spit. The more end spit and side spit a fuse has, the better we expect its fire-transfer properties to be. Remember side spit. The concept will resurface as we dissect the terrible past of tube salutes.

Red fuse has plenty of end-spit, but is said, or at least rumored, to lack the good side spit of green fuse. That functional difference, more than cosmetic appeal, explains the coloration.

Firecracker fuse is suitable for little save lighting firecrackers. Though simple in construction, it proves surprisingly hard to make. You must start with material rarely found in the West, a paper known as Gampi tissue, far stronger yet more pliant than our own wrapping tissue. The fuse comes into being by rolling/twisting lengths of tissue formed into troughs, into which a gunpowder-like composition has been poured, but this oversimplifies the operation considerably, as those who have tried to make it will attest. Unless you get seriously into pyro, forget about making or using firecracker fuse.

At the thick end of the spectrum we have time fuse. This ranges from about 1/4" to more than 1/2" in diameter, and finds use as the fire-transfer delay in professional aerial shells used at public fireworks displays. Still available, though usually imported, you have no use for its special properties, nor its high cost. The photo shows a length of 1/4" time fuse.

In a practical sense, any coated fuse the experimenter can get his hands on is likely to suffice as reliable ignition for a ground salute.

SALUTES: TYPE AND MANUFACTURE

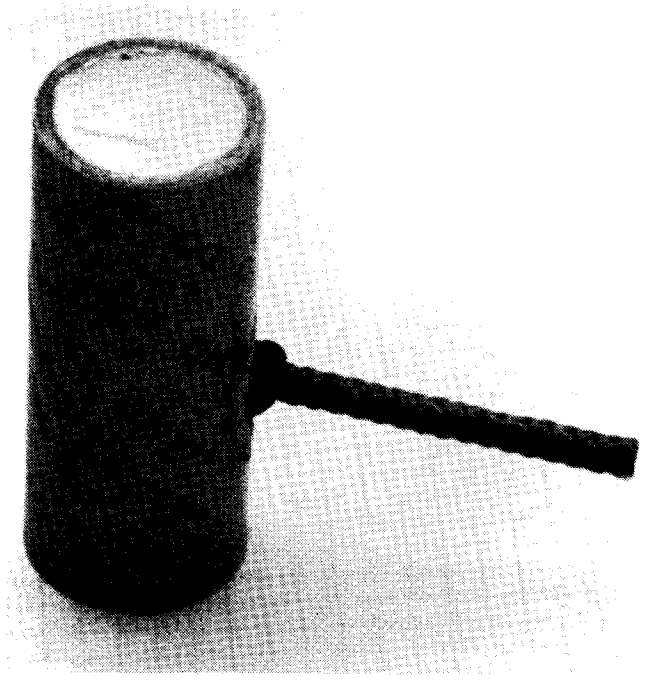
At this point we have oxidizers and fuels whose mixtures form combustible blends that, in most cases, simply burn brilliantly out in the open. We have a reliable means of delayed ignition in the form of plastic coated fuse. All that remains is to confine the powder in some sort of casing, since confinement ordinarily proves necessary for a report.

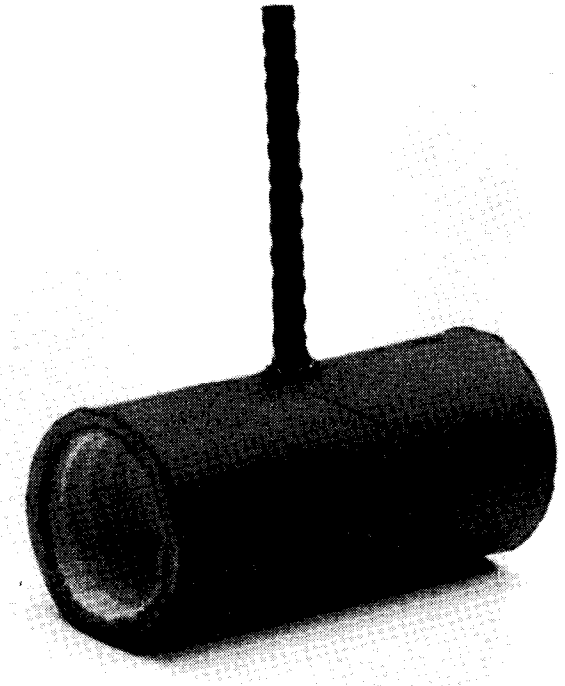
The cases used to confine flash powder introduces us to a world of variety and creativity, tradition and economics, safety and hazard. This final phase is the how-to-do-it of producing explosive sound for pyrotechnics.

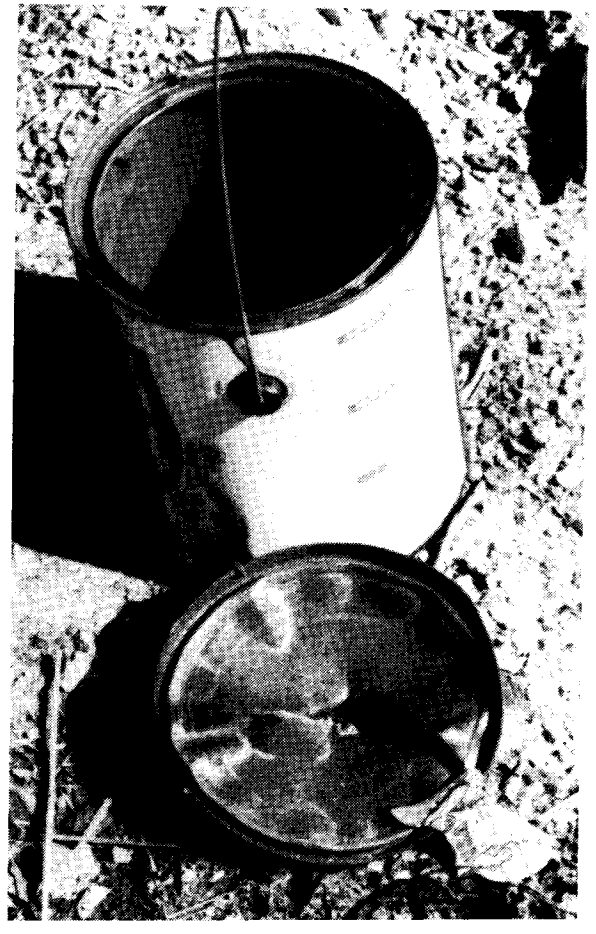
TUBE SALUTES

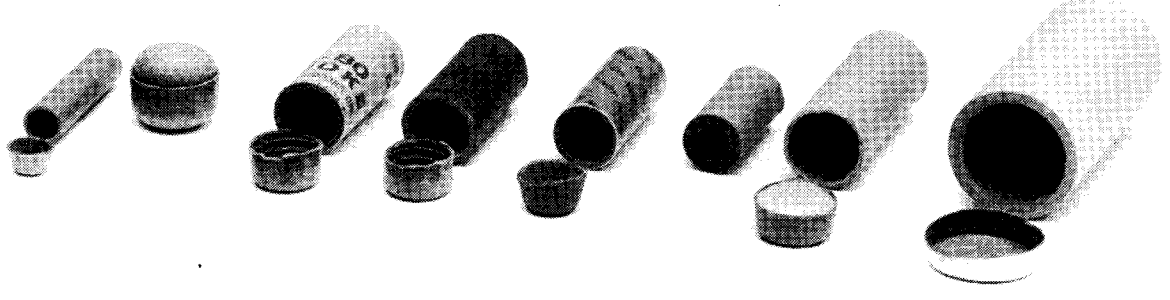
"M-80" is a military designation, just as "M16" designates an assault rifle and "F16" designates a fighter aircraft. M-80 refers to a "ground report simulator," something to go BANG in lieu of live ammunition, just the ticket to give the troops a bit of a rush out on maneuvers. Used in military training, reports lend the action a fine, realistic flavor.

The M-80 is the prototype of the tube salute. It enjoys popularity on the black market equal to that of the silver salute (aka TNT). They are identical but for 1/16" greater outside diameter for the M-80, and for the distinctive outer wrap of each. Both are cardboard tubes 1-1/2" long filled with flash powder, sometimes with other materials. Refer to the photo for examples of salute casings.









TOP LEFT: The real thing, ancient photo of silver salute purchased November, 1969 at open-air market somewhere in the deep South, for ten cents. Note the two key safety hazards: 1) end sealed with rock-like adhesive that fragments into deadly missiles upon detonation, and 2) dark clump of material at base of fuse: priming, exposed to an accidental spark, which leads to detonation milliseconds later. TOP CENTER: Dummy of modern "safety" salute. Note paper end cap and absence of exposed priming. Fuse held securely by glue not visible in photo. TOP RIGHT: Ancient photo of paint-can lid punctured explosively as described in text. BOTTOM LEFT: Parade of salute casings purchased circa 1970. From L to R: 5/16" inside diameter casing w/end cap; mated pair of cherry bomb cups; M-80 Smoke casing; true M-80 casing (the only difference between the two is color and labeling); silver salute casing; thick-walled casing w/o end cap; 5/8" inside diameter aerial salute casing; 1-1/8" inside diameter aerial salute casing.

In the classical design, the fuse enters the casing through a hole in the center. Some sources maintain that lighting the powder in the center of its mass makes a louder report by starting a flame-front that advances in two directions at once, rather than from one end to the other, as expected with an end-placed fuse. We might agree with this intuitively, but one commercial manufacturing technique precludes end-placement, as we will see shortly.

The ends in this traditional and charming design are closed with a rock-like adhesive based on calcium carbonate and a syrupy solution of sodium silicate. Here we meet a clear safety hazard. The explosion reduces the casing to fine particles of paper that lose destructive power within inches of travel. Not so the rock-like end-closure. Depending on thickness, which varies greatly among different, ah, brands, the adhesive may split into chunks big enough and flung fast enough by the explosion to do serious harm, such as cause blindness.

Probably the worst safety hazard arises from the practice of priming the fuse. Priming is black powder (gunpowder; not smokeless powder, the propellant used to make small arms ammunition) mixed into a slurry with water and dextrin, a crude sort of glue. One end of the fuse is dipped in priming, then plunged into the casing's center hole. As it dries it acts as an adhesive to hold the fuse in place.

Priming helps assure ignition of the flash powder (fire from the fuse alone will not light some flash mixes reliably), and to ignite as much powder as possible in as short a period as possible, since priming burns briskly. Ignition of more flash mix in a shorter period is felt to enhance the report.

The problem, at least from a safety standpoint, lies with the grim fact that priming presents an exposed combustible that takes fire more readily than the fuse. A spark that falls on priming will light it, and a split second later the bomb will vaporize, along with your fingers if you happen to be holding it. (Return to the comments about side spit of green fuse. The fuse could be your undoing. It could pop a spark onto the priming, which would light the bomb in your hand. If you have occasion to discharge ground salutes, never do so without safety equipment that will protect you completely in the event of premature ignition. Assume the worst, because it will happen. More grisly detail under Cherry Bombs, below.)

MASS MANUFACTURE OF TUBE SALUTES

Amateur pyros most always begin with tube salutes, before becoming bored with them and graduating to the true craft and art of pyrotechnics. But tube salutes are damned time-consuming to make. First, you have to glue in one paper end cap, then punch a hole for the fuse and glue it in place. Next, mix the flash powder (in SMALL quantities, often no more than two or three grams at a time, enough for one salute) and load it. Then glue in the second end cap. That last cap takes much longer than the first, since you must wear a great deal of protective gear to handle the unit safely, because it has become a finished explosive device as the second end cap is glued. Clearly, this "safe" method takes too much time to turn out products intended for the black market. Let's look in on the mass method, one way the pros did it, and, for all we know, may still be doing it....

It began with a piece of quarter-inch or 3/8" plywood drilled with holes whose inside diameter just equaled the outside diameter of the salute casing. Boards had to hold at least 49 to be economical, so rows of at least seven by seven became common. Some were much larger, holding well over a hundred.

Empty casings were inserted into this upright holder, which, itself, rested on some non-stick surface, usually waxed paper or a floured formica counter-top.

Next, the operator poured a small portion of what came to be known as "professional pyrotechnic adhesive" into each casing. The amount had to be enough to seal the bottom completely to a thickness of at least 1/16", often 1/4" when things got sloppy.

Now, with wet adhesive sitting there, nothing further could be done until it dried—you couldn't pour flash powder onto wet glue—unless some inert, dry buffer were placed between the adhesive and the powder. Rice hulls and coarse sawdust saw duty here. Just enough was poured in to cover the adhesive to keep the powder off it; then the flash powder was added.

TABLE OF SALUTE COMPOSITIONS (PARTS BY WEIGHT)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Potassium Perchlorate	50	70	50	75	60	50	80				1						60		60
Potassium Nitrate										5		12	6	6	50				
Potassium Chlorate								50				60							
Barium Nitrate									4		1					50			
Strontium Nitrate																		50	
Aluminum, bright																			
Aluminum, dark pyro	25		25	25						2	1								
Aluminum, Black German		30							2										
Sulfur, flour	25				40	20			1	3	1	23	3	2					
Antimony Sulfide, black			25			30						5							
Arsenic Sulfide, red								50											
Charcoal, dust							20						1						
Antimony, metal powder														1					
Magnesium, 100 mesh or finer															50	50	40	50	
Magnesium/Aluminum alloy, 150 mesh or finer																			40
Polyvinylchloride/Hexachlorobenzene																1		1	

By no means a comprehensive listing, this matrix sketches the violent nucleus of powders commonly used to make salutes. First rule: ALL FORMULAE THAT CONTAIN POTASSIUM CHLORATE SHOULD BE CONSIDERED SUICIDAL. DO NOT MIX THEM. Simplest, safest mix for small salutes contains potassium perchlorate and dark or Black German aluminum. Oddly, this mix loses some of its punch in bulk, say, that needed for a 3" aerial bomb. In that case, addition of sulfur or antimony sulfide—gas formers—restores body to the blast, and allows use of the safer bright aluminum. Formulas that contain only nitrate oxidizers suit only extremely strong cases, since they lack the kick to detonate. Formulas 16 and 18 are examples of powders fancied to give colored flash reports. Most of these mixes have been quoted in other texts; a few represent minor variations on otherwise standard formulas. Clearly, many of these chemicals are poisonous, and demand precautions in addition to those applied to flammable mixtures. Related only for informational purposes. Get an explosives license and proper training if you would mingle in this forbidden realm....

Sealing the upward end worked in reverse. The operator poured rice hulls in on top of the flash powder, followed by more liquid adhesive on the hulls.

It takes less than 15 minutes for this type of cement to solidify to the point that the tubes can be plucked from the mold and put aside to dry fully while the next batch comes through.

Some felt the rice chaff served a dual purpose in that, as the salute was handled, it dispersed through the powder and prevented caking. Since the loudest reports were believed to result from loose powder, this was desirable.

At this point in manufacture we had closed paper tubes filled with flash powder. It was time for fusing. We can see now, working backward into the process, why fuses came to be placed in the center of the casing instead of the ends, as was the case with firecrackers. Putting a fuse through the end closures of granite-like adhesive would have proven impossible without a carbide-tipped drill, and would have wasted time.

The most practical route lay through the soft paper of the casing. An awl, or just a nail (a dull one, from the look of samples the author bought late in 1969) was used to punch a hole into the casing, and the fuse was inserted.

The cheapest way turned out also to be best from a theoretical/intuitive standpoint. Center placement of the fuse started the powder burning outward in two directions at once, rather than from end to end, as would have happened with an end-placed fuse.

Left in that state, with nothing but friction to hold the fuse, flash powder would leak, and the fuse would fall out with minimal handling. This led to the practice of priming, which, again, served dual ends. The end of a 1-1/2" length of 1/8" green fuse was dipped in priming, then stuffed into the hole in the case, and the assembly set aside to dry. Look at the old photo of a silver salute purchased at the fabled open-air market in November, 1969, for the then-outrageous price of ten cents. The black ring at the base of the fuse is priming.

They called it priming because it took fire far more easily than flash powder, and made for fewer duds. But here again, the pluses of priming proved flawed in a way that, perhaps more than any other aspect of tube salutes themselves, led to the real notion that these engines held danger.

To serve its dual purpose of securing the fuse and promoting ignition of the flash powder, the priming came to be exposed on the surface of the casing, which meant that a stray spark from any source—sparks thrown off by the fuse as it was lit, for example—could set the device off instantly, and sometimes did. Priming was used on both cherry bombs and tube salutes. We see it still on Oriental "cherry smoke balls."

From time to time we come across entrepreneurs who step up to the old cannon-cracker class of salutes, with inside diameters exceeding 3/4" and lengths of three to five inches, with fuses poking out about four inches, a good safety measure for a naturally unstable unit. These bombs surface in country-store type places, and the right code words may put you onto a source from a class C stand in some venues. The old-boy network helps, just like the street drug gig, such a sad testament, since the last thing these entrepreneurs want is to cause personal or property damage.

TUBE SALUTES IN THE MODERN ERA

Thus it was in the old days, and modern pyros, despite the fact that they dealt with banned devices, were quick to spot the hazards. The initial remedy took the form of all-paper construction. Instead of silicate-based adhesive, they sealed the ends with paper caps. That eliminated the showers of granite-like shrapnel. Second, though some purists still primed the fuses, they dipped one tip of the fuse in priming, let it dry, then inserted the fuse up through the interior of the casing, leaving all of the primed part inside, and secured the fuse in place with standard white glue. This left the outside tip of the fuse as the only exposed, flammable surface, and made the device literally immune to ignition from stray sparks, except one hitting the end of the fuse.

If the purpose of tube salutes in the first place was to make a bigger bang than firecrackers, at least the new wave of pyro wanted to have complete control of when the device would detonate. Formulas based on potassium chlorate certainly gave more bang per unit weight, but left us with that uneasy feeling that the stash in the garage might not wait until the Fourth to kick off. Chlorate-based blends, especially volatile ones like flash powders, had a way of detonating spontaneously. To some stalwart souls that meant simply adding magnesium carbonate or barium carbonate to the mix and hoping for the best. But to the genuinely safety-conscious it meant turning to another source of oxygen, potassium perchlorate.

—which, truth told, was not bad. The perchlorate proved itself plenty potent as long as we paid attention to details: particle size and mixing. We understand already that reaction rates increase with surface area. Potassium perchlorate supplied was usually powdered finely enough, about 200 mesh. But many pyros took to grinding it into flour-like dust using a mortar and pestle. Some upmarket hobbyists resorted to ball mills made from rock polishers and loaded with special hard/dense lead alloy spheres that yielded incredibly fine powder.

While this helped, it reached the point of diminishing return rapidly. Powdering for five minutes in a mortar gave no better performance than letting the stuff go for days in a motorized mill. The limiting factor turned out to be the particle size of the fuel. For flash mixes, that meant aluminum. The fearsome tale of Black German Pyro aluminum has been told.

SYMPATHETIC DETONATION

From time to time we heard tell of explosions of entire boxes of cherry bombs or M-80s, often in the back seat of souped-up cars driven at top speed by callow youths who terrorized neighborhoods by tossing the deadly units out the window. (What a better time it was, too, when that lewd delinquency was all the terrorism we knew....)

The point at issue is, Why and how could a box of overgrown firecrackers explode all at once? Didn't you have to light the fuse to set one off? After all, it wasn't as if the boys were carrying dynamite or plastique.

Analyze the physics of it in light of what you already know of salutes. Caching tens of them in even a flimsy box produces confinement. The explosion of one adds much more by its pressure wave. That wave is strong enough to rupture one or more other casings, letting the wave impinge unblunted on the next powder charge, and the next, all of it in a split second. One modest boomer blossoms into the equivalent of a 3" aerial salute popping in the car. That's enough to blow out the bottom chassis, the windows, and the youths' eardrums, a fitting punishment for young reprobates.

The lesson of it is, never stock completed devices in quantity. Their proximity and the laws of physics create an extreme hazard. The laws against possession (that number would probably qualify you for the added charge of "with intent to distribute") prohibit it altogether. Just for information.

CHERRY BOMBS

The manufacture of cherry bombs, M-80s, and silver salutes grew up as a cottage industry in back rooms and basements in parts of Ohio and Pennsylvania, lately of California, simply because these devices are so easy and relatively safe to make, and always because as banned items, they bring a sagging bag of cash.

First, they are federally verboten, meaning that it's illegal to make, possess, use, sell, transport, or think about them. They probably should be banned because of what mutants, cretins, and other low-lifes found in large cities do with them. Country folk use cherry bombs for harmless pranks, such as blowing up mailboxes. But in cities, they get dipped in glue, then rolled in BBs to make tiny grenades for gang fights between fourth-graders. In one city, a "fan" threw a cherry bomb at a professional baseball player. It detonated close to his head. The blast knocked him cold. Had he been looking the wrong way it could have blinded him. Harmless fun.

But what irresponsible, depraved, and sinister urge would prompt a surveillance writer to reveal the secrets of these dread devices? Paradoxically, a concern with safety. The author lived his basement-bomber days in the 1960s, when you could order cherry bombs by mail, along with the chemicals and casings to make them. (In fact, you could order them as late as 1968 from at least one company that advertised in Popular Science,

on the strength of a signature from an unspecified local official....) The author went on to a degree in chemistry—none of the knowledge ever applied to explosives and propellants—perhaps reflecting his concern with safety. Knowledge of how accidents involving these fascinating devices happened provoked him to write this, both to explain how they work and to warn those who buy them of their hazards.

Companies catering to the pyro hobby used to sell pairs of what were called cherry bomb cups. These manila-colored paper hemispheres consisted of a smaller and a larger cup, one to fit inside the other. The method of manufacture suggested by one vendor was to pierce the center of the larger cup, glue a good length of green fuse in it, prime the interior segment of fuse if desired. Next, fill the smaller cup with flash powder, then place the larger cup over it. Secure the two with a dab of glue or paste.

Next, dipping: To get that red, rock-like outer shell, the hallmark of a cherry salute, the completed devices had to be immersed in a mix of fine sawdust, red coloring (powdered tempera paint served), syrupy sodium silicate, and calcium carbonate. The consistency of the dip had to be adjusted such that a solid, even shell of 3/32" to 1/8" thickness would adhere to the cups, and not sag to the bottom as the finished product was held by clothespins on its fuse while it dried.

Some early literature commended chlorate-based compositions, but with all the moisture likely to seep into the case that course seems insane.

This amateur method never produced quite the same product one found sold at roadside stands. It lacked that professionally made look and feel of the real thing. One gets the impression that commercially sold cherry bombs were made by the barrel technique described in Davis' The Chemistry of Powder and Explosives, in the same manner outlined for manufacture of torpedoes, and which is used also to make spherical stars for Oriental fireworks (the pharmaceutical industry uses it, too, to make pills, even the good kind....).

In this case, the two cups would be assembled, sans fuse; dumped in masses of hundreds into a rotating bin, into which a dilute solution of sodium silicate would be poured or sprayed, along with dashes of calcium carbonate, red dye, and fine sawdust. The rolling action accreted an extremely even, smooth layer distinct from that of the dip method. As to how the fuse holes were made, we can only speculate. One cannot imagine a sane person drilling into the device, since that is practically an invitation for detonation from friction. Yet commercially sold cherry bombs the author saw in the early sixties always wore priming around the fuse, on the outside, meaning that insertion of the primed fuse had to be the final step in manufacture.

Cherry bombs: What an irresistible blend of charm and danger. Sold in boxes of half a gross, the last one the author saw being about 1962, and bearing a price tag of something like $4. But what a premium they command today, so much so that organized crime is rumored to have a hand in distribution.

CHERRY BOMBS & SAFETY

Cherry bombs suffer a safety record, or the lack of one, worse than that of tube salutes. The reason lies with their construction. It makes them tiny fragmentation grenades, along with the risk of unpredictable ignition due to exposed priming.

Upon detonation, their tough outer shell fragments into an expanding sphere of eye-piercing shrapnel, just like a grenade. Some years back, the papers reported a genuinely tragic tale of a man who lost sight in both eyes when the cherry bomb he was lighting exploded. The story told that he believed that he was being careful. He was not holding the device, thank goodness, and sought to light it at arms' length with a sparkler.

Needless to say, the shower of burning iron from the sparkler hit the exposed priming before it lit the fuse, and the unit exploded milliseconds later.

Exposed priming, fragments produced by explosion, and a fair degree of power. These three factors explain why cherry bombs and tube salutes are, and probably should be, banned.

A corollary holds that those who wish to take risks and survive a mishap with 20/20 vision and all their fingers MUST assume that premature detonation will happen, and don safety gear to eliminate risk of injury when it does.

Never handle salutes except with tongs, or if you must use your hands, wear thick leather work gloves and grip the fuse, not the body of the unit. Second, do not approach finished salutes unless you are wearing goggles, preferably polycarbonate, the kind that resist the impact of bird-shot fired at point-blank range. Full-face protection of similar stoutness couldn't hurt. Third, your ears can do without a 150-decibel blast two feet away. Wear hearing protectors. Fourth, never let multiple small explosive devices accumulate. If one goes, they all go, instantly.

THE LEGEND OF THE PLASTIC CHERRY BOMB

Some years back, the sixties it now seems, there were said to have been sold cherry bombs—black market of course, and of limited distribution—that differed from the standard type in having a red plastic case, probably cheap polystyrene. In addition, they were so much more powerful than common cherry bombs as to question whether they contained high explosive, such as the military staples, C3 and C4, perhaps more freely obtained back during the Vietnam era. One source reported that, where the ordinary cherry bomb did nothing to his concrete driveway, a plastic cherry took a fist-sized divot out of the rock and sent shock waves booming across suburbia like a flight of F4s scorching the treetops with their afterburners.

Careful reading of texts that deal with the effects of explosives tells us that detonation of several ounces of, say, mercury fulminate, a high explosive used in blasting caps (blasting caps initiate detonation of other high explosives, such as the now-outmoded dynamite, as well as military plastic explosives) fails to do more than minor local damage, despite a fearsome report. That calls up a speculative reconstruction of the plastic cherry bomb as shown in the diagram, one that would explain its ability to dent concrete. C4 has become harder to come by, what with cessation of the Vietnam conflict, and plastic explosive coming over from the other side of the iron curtain has been earmarked for more politically specialized use. Perhaps that explains the disappearance of the fabled plastic cherry bomb....

"PROFESSIONAL PYROTECHNIC ADHESIVE"

Pyros paid a dollar each to learn the formula back in the early seventies. Two versions have been reported. The least expensive and easiest to make—the choice of pros for those reasons—was nothing more than finely powdered calcium carbonate (chalk) mixed with a syrupy solution of sodium silicate. Those who owned chemistry sets purchased prior to 1964 will recall sodium silicate solution as "water glass," used to paint eggs in one fondly recalled exercise. But that solution was far too dilute for use in an adhesive/end-plug. No, it must be of a concentration to give it the consistency of Kayro syrup. (The figure that comes to mind is 42.2 Baume', but that may be the author's memory playing sinister tricks....) Mixed with calcium carbonate, it forms a thick, sticky mass that dries rapidly to concrete-like hardness. (Do not stir it with any tool you plan to re-use. Once hardened, and submersion in water does not prevent hardening, the stuff is all but impossible to chisel off.)

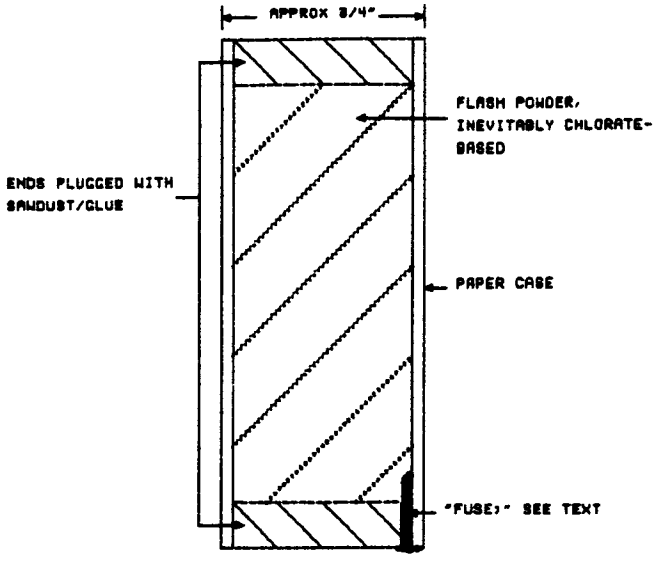
The second formula, one that, at least in the author's hands, always left unsightly lumps when it hardened, called for the addition of finely powdered zinc oxide in a ratio of 1:1 by weight to the calcium carbonate. This gave the finished product more of a gloss-white look. Its effect on hardness or tack was not apparent.

The important qualities of PPA were its thick consistency, which let it serve as an effective seal and not run as would conventional white glue; the fact that it maintained its bulk as it dried; and dry quickly it did. It was by its composition alkaline, a balm to chlorate-based powders despite its moisture. Finally, it was strong, literally rock-like in hardness.

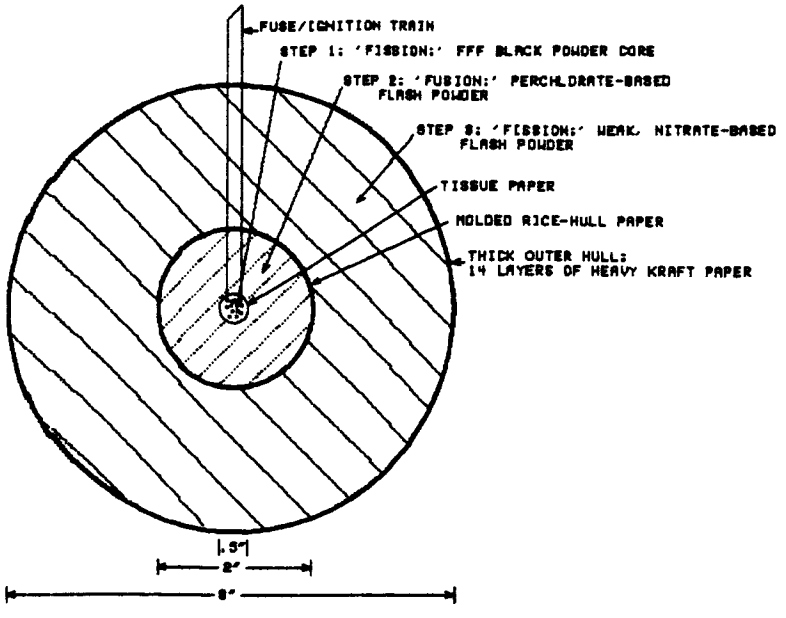
This adhesive was a true hero of the tube-salute business. But, like all heroes, it suffered a fatal flaw: its great strength and hardness, which made for so sturdy an end closure, broke into a spray of eye-penetrating shrapnel when the device was set off.

OTHER GROUND SALUTES

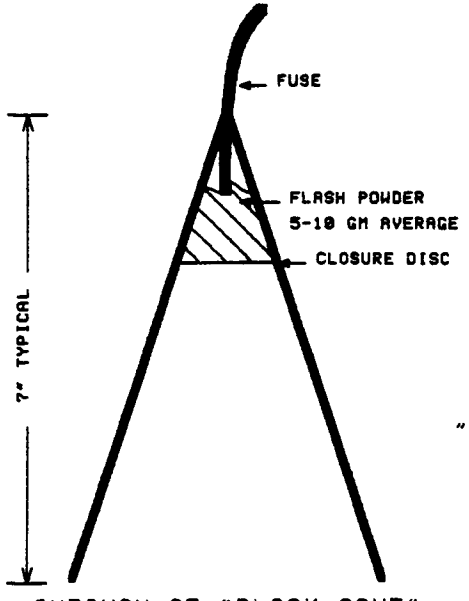
First off, to be intentionally repetitive, it is illegal to make these devices; it can be extremely dangerous to do so; and you have no business messing with it. Read this purely for informational purposes. The fact that so many people seek these units, and the fact that a few will brave criminal conviction to make and sell them, means that public interest in them remains at fever pitch. It is human nature to wonder about what is forbidden.



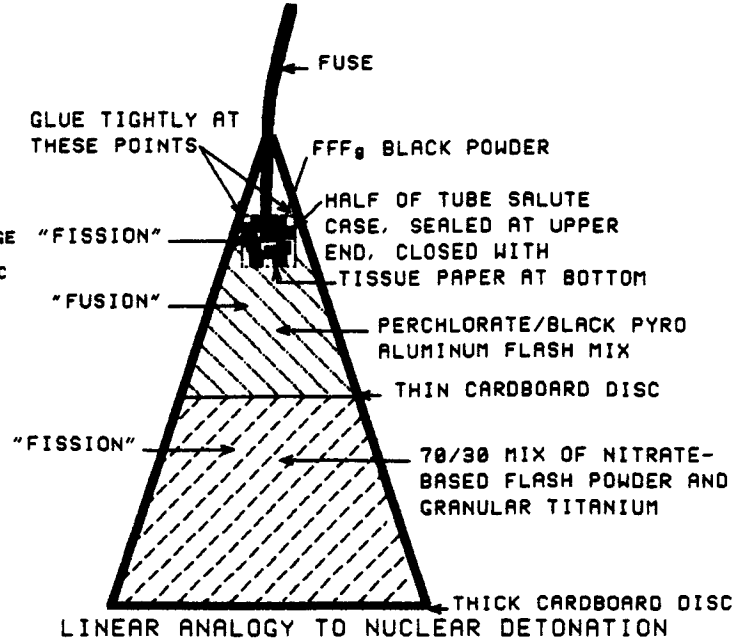
"BRAZILIAN" SALUTE



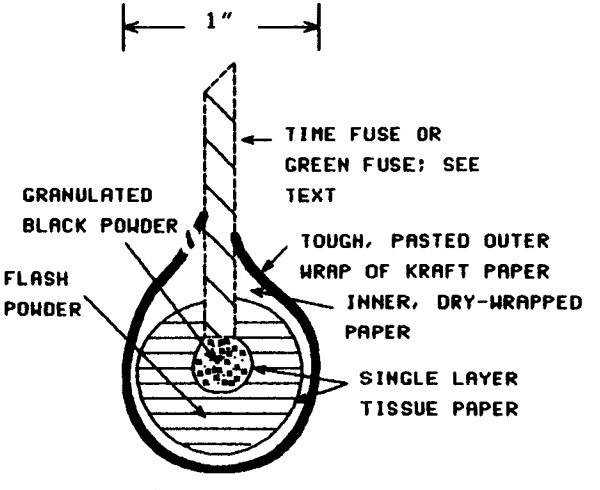
THE INFAMOUS 'FISSION-FUSION-FISSION' SALUTE



CUTAWAY OF "BLACK CONE"
NOTE OUTER SIMILIARITY
TO HARMLESS CONE FOUNTAIN



LINEAR ANALOGY TO NUCLEAR DETONATION
SEE TEXT



"ORIENTAL" SALUTE

So why say anything at all? Well, the author has been involved with their manufacture, in small quantities and NEVER for sale, and for that reason knows a bit about them. (And all that took place well over fifteen years ago. There is no longer any physical evidence from those easy days, and the statute of limitations has long since expired. That means the author can speak frankly.)

Second, the author still has all his fingers and unimpaired sight and hearing because he practiced safety obsessively. He wishes to convey this safety-minded approach to those who may have gathered crude details for making cherry bombs from other texts, or to those who purchase contraband and are at risk because of safety defects already detailed.

Again, read this the way you read a tale of mayhem in some action novel, purely for vicarious gratification. DO NOT MAKE ANY OF THE DEVICES DISCUSSED HERE.

There is much more to pyrotechnics than ground-boomers. Explosive sound occupies a legitimate place in fireworks. Indeed, it is hard to imagine a professional fireworks display without the flash-KaBOOOMM! of aerial salutes. But explosive sound is like punctuation in a paragraph: indispensable, yet meaningless without words to pace.

What about whistles, fountains, roman candles, rockets, star-shells, set-pieces, and wheels? We could tell all this and more, but it would be a repetition of what's in Weingart and Lancaster. Much of what we have offered here is not found in the major fireworks texts, has interest and positive safety value for pyro dilettantes and casual readers.

BRAZILIAN SALUTES AND THE CULT OF MACHISMO

—because one look at them, one audition of their fierce, chlorate-based detonation, and you bloody well know it takes balls to make them. Here is the method, but don't do it:

Take a stout paper tube about 3/4" outside diameter, 1/2" inside diameter, 2" to 3" long. The interior of one end paint with a 1/8"-thick train of priming about 3/4" long. Make sure the priming comes fully to the end. Let it dry. Believe it or not, that's the fuse. Plug the fuse end with a crude, sticky mix of glue and sawdust about 1/2" thick. Use a dowel to pack it tightly. The priming must remain exposed for the salute to take fire. Then fill the casing thus prepared with flash powder and seal the other end with the same sawdust/glue mix. This blend of simplicity and economy is reminiscent of Oriental devices; yet the unquestionably violent chlorate-based composition would give even the Japanese pause.

Brazilian salutes usually fire from mortars or roman-candle-like units. Two or three of them are stacked vertically in relatively spacious launch tubes. This lets the flame of the lifting charge reach the priming and ignite it. A second later, tubes high in the air, it fires the flash mix, which tests in 1973 showed to be a pure evil blend of aluminum, sulfur, and potassium chlorate. Few pyrotechnic comps are deadlier.

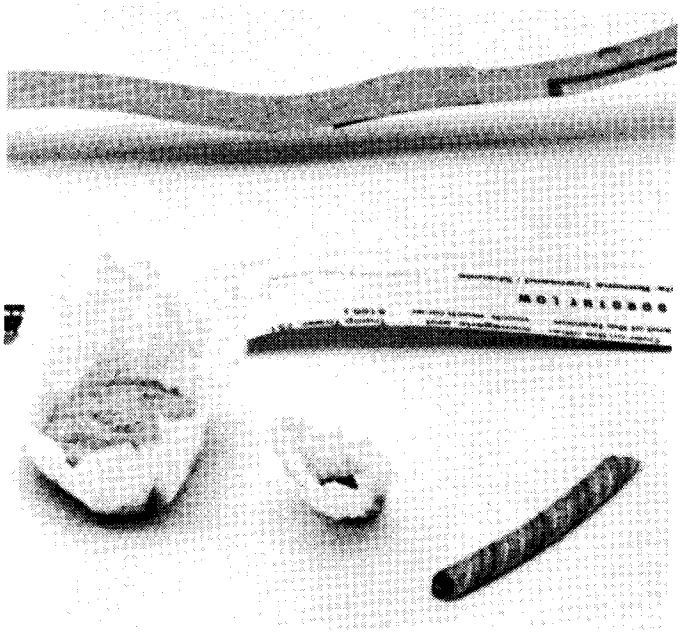
THE ORIENTAL METHOD

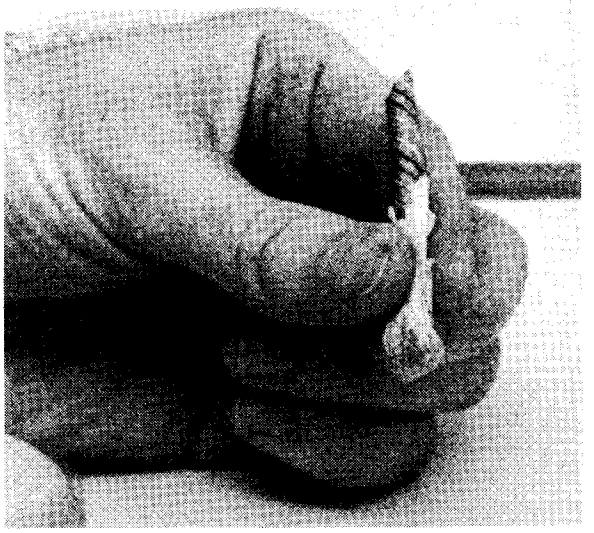
The good news is that these salutes use a comparatively insensitive mix of potassium perchlorate, sulfur, and bright aluminum, in a weight ratio of about 2:1:1, respectively, this data from samples analyzed in 1972. The bad news is that making them requires prolonged handling of the device well into the stage at which, should it accidentally detonate, loss of fingers or hands would probably result.

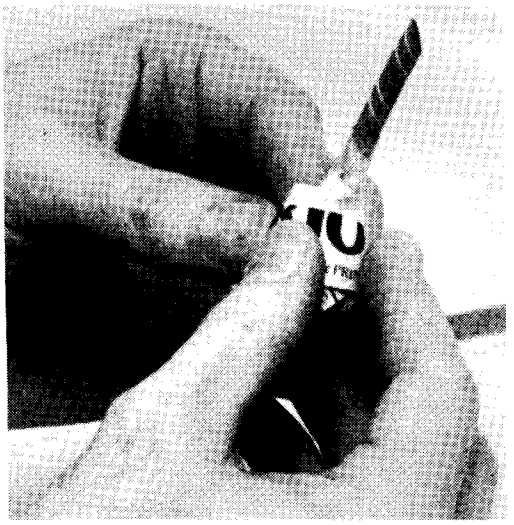
The only pre-manufactured part of the Oriental salute is the fuse, and here the thick time fuse is used in aerial reports, while conventional green fuse can be substituted with good results for ground salutes as long as care is taken to protect it until it reaches the center ignition point, lest its side spit light the flash powder prematurely.

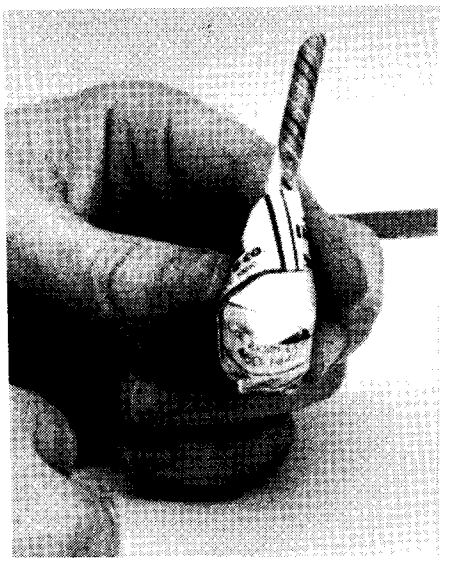
Refer to the photo set. These devices look like small pears. Construction shows us why. It begins with a length of fuse, the length determining the time for ignition. For ground-based devices, it should protrude at least two inches outside the salute to allow time to get away safely.

A pinch of black powder of FFFg grain is placed in the center of a 3/4" square of tissue paper (use the fabled

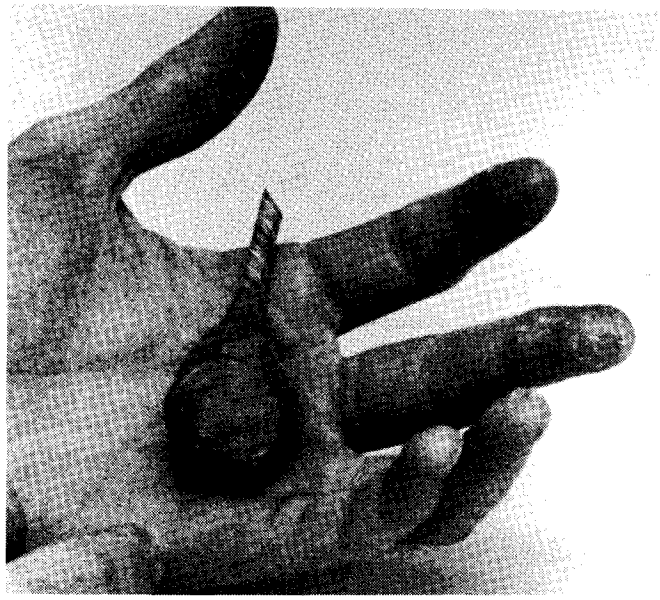




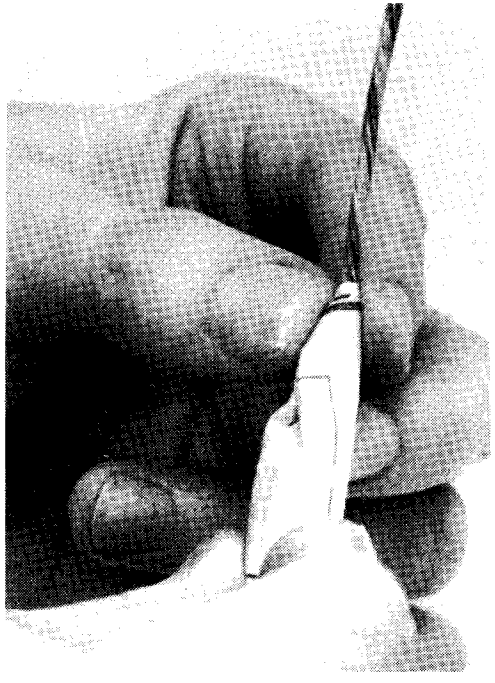


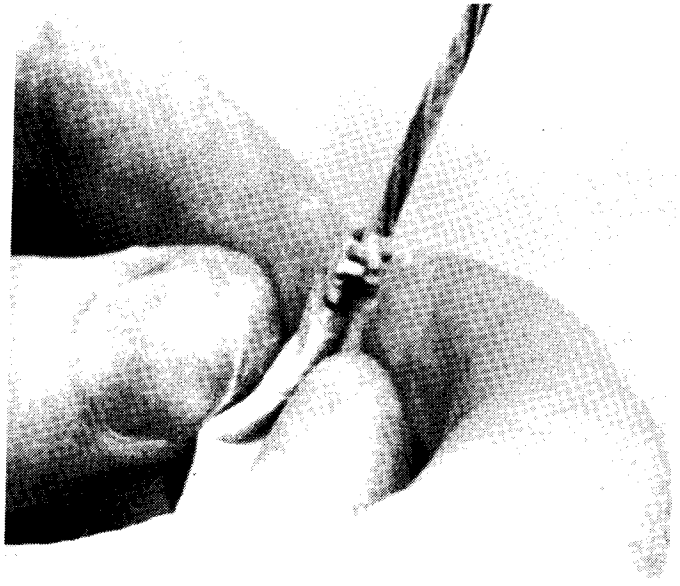


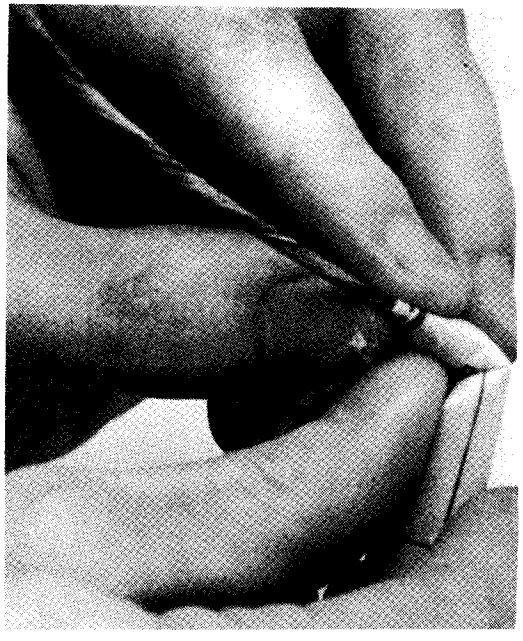
MANUFACTURE OF ORIENTAL SALUTES. TOP LEFT: The components: kraft paper, newspaper, fuse, primer in tissue paper, flash powder in tissue paper (all powder in photo sets is non-flammable). TOP RIGHT: Form primer at base of fuse, secure with paste. MIDDLE LEFT: Insert primer into mass of flash powder. MIDDLE RIGHT: form sphere of flash powder around primer, secure with paste. BOTTOM LEFT: Wrap resultant sphere evenly with layers of newspaper folded double along its length. BOTTOM RIGHT: Resultant unit, ready for outer wrap of kraft paper. (continued next page)

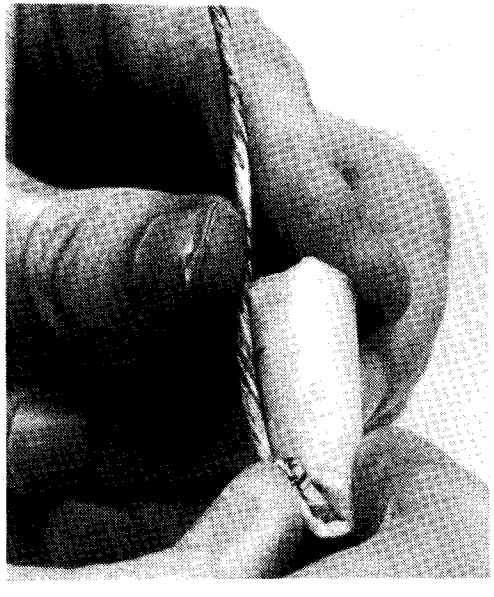


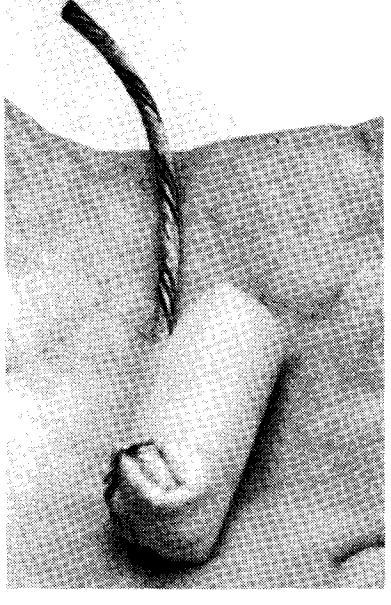
TOP LEFT: Continuation of Oriental salute manufacture. Begin wrapping paste-soaked kraft paper in even layers to give finished device (TOP RIGHT). Dried unit clacks like wood when struck on hard surface—incredibly stout casing.
BOTTOM LEFT: Start of manufacture of field-expedient salutes. Roll paper on whatever form you have chosen. BOTTOM RIGHT: Fold and seal bottom with tape to give hollow, closed tube.
(continued next page)











(continued from last page) TOP LEFT: Insert fuse along edge of casing, fill w/buffer, flash powder, and more buffer as described in text. Fold paper around fuse. TOP MIDDLE: Rub paste into paper forming neck around fuse, fold it in as tightly as possible. TOP RIGHT: Fold fuse at 90-degree angle. BOTTOM LEFT: Fold fuse again at 90-degree angle. BOTTOM RIGHT: Secure fuse to side of case with tape. Check case for leakage. Unit is finished. As with triangle crackers, choice of paper and dimensions not critical.

Gampi if you can get it). One end of the fuse is then placed in this powder and the tissue folded around it to form a lollipop-shaped igniter. It is vital that the fuse ignite only the black powder.

The next step is a repetition of the first, only here we use a larger square of tissue paper (the size of the paper determines the size of the salute) on which the flash compo has been centered. Let's assume a cherry-bomb-sized device and go with about 4 grams of composition (this powder will be compressed, and for that reason more of it can occupy less space; see the discussion below of theoretical differences between American and Oriental salutes). Place the pouch of black powder in the center of the flash mix, then pull up the corners of the second layer of tissue and twist it around the fuse. We now have what looks like a bundle of flash mix held to the end of a length of fuse by a single sheet of tissue paper.

Ignited as is, it would go up with a brilliant and smoky but unimpressive WHOOSH. To get a BANG, we must subject it to confinement. In typical Oriental waste-nothing/make-something-out-of-nothing style, we create an extremely strong casing from two types of paper. In bulk manufacture, there are, of course, ideal thicknesses that allow for minimum wrapping with optimum strength. But here we can go with just about anything available, including newsprint.

Start by cutting long but thin strips of two types of paper. The width of the strip should be proportional to the contemplated size of the device. For this small one, about 1/2" will do. Begin by wrapping dry paper (we used strips of the Village Voice in the photos; we did not use real flash powder) around the core of flash powder in a non-overlapping pattern while applying moderately firm pressure to keep the unit in the shape of a sphere with the black powder at its center. Two to three layers should do it. Now, some experimentation will be needed to find the method that eliminates lumps of paper accumulating at spots on the case. A good trick is to cut the strips of paper 1" wide, them fold them lengthwise so that fewer layers of the doubled paper are required. After you get these dry layers on tack the tail of the strip with a dab of paste.

This first layer provides strength and, just as importantly, prevents the composition from getting too moist when the next layer of paper is wrapped. This layer differs from the first in that we use kraft paper soaked with paste. Cut the strips, lay them out on a formica surface, and rub them thickly with paste. It is almost impossible to use too much. Saturate them with it. Here again, wrap on two or three layers (or more: the final strength of the casing will have a bearing on the report, and it depends on the number of layers of paper). Press and smooth each layer to keep the pear-shape symmetrical and free of paper blobs. Experience with these has shown that practice with several will be needed before cosmetically passable devices turn out.

Once the last layer of paper is on, set it aside to dry. The best place is shade on a sunny, dry day. NEVER PLACE A PYROTECHNIC DEVICE IN AN OVEN IN AN ATTEMPT TO DRY IT QUICKLY. Not only is that practice insanely dangerous, but results in a less professional unit.

It goes without saying that absolutely no combustible surface should be left exposed except the end of the fuse. Remember the lessons from the old and devilish American ground-based salutes. If you have used regular green or red fuse, it will be necessary to wrap the inside portion with two or three turns of masking tape before beginning the salute, since its side spit could get to the flash powder before it gets to the primer of black powder. If that happened, it would weaken the report.

Now look at what you have: a hollow sphere—more or less—of strong paper, enclosing a hollow sphere of comparatively safe flash compo, in turn enclosing a sphere of black powder. Proper ignition sequence will light the black powder first. This will burn through the tissue paper instantly, igniting the flash compo along the maximum possible surface area (the entire surface of the innermost sphere). The flash mix will begin burning outward in all directions at once, but in the confinement provided by the strong paper case will detonate quickly.

Given that we are dealing with perchlorate oxidizer, with its limits on power but advantage in safety, Oriental salutes produce the best reports per weight of composition of all designs. They also demand the greatest effort to make, but do not suffer any limitations on materials. Paper can be had literally in the nearest trash bin. (Shopping bags are one of the best sources of cheap, thick, tough kraft paper, though many stores have supplanted these with plastic bags.)

Some reinforce the casing with a layer or two of twine. Frankly, the less you have to handle an explosive

device, the better. Oriental salutes are intriguing, efficient, and admirable in their makeup. But you would not catch the author making them. He likes his fingers and hands intact....

Commercial Oriental salutes find use in aerial reports, usually timed ones (time fuse with a length difference of, say, 1/4" produces a regularly spaced string of aerial reports that form part of the standard repertoire of pyrotechnic displays). The fact that they have gained such acceptance with relative safety is probably a testament to their tame composition. Amateurs inevitably try to go the pros one better and use pyro or even Black German pyro aluminum, or—god forbid—chlorate oxidizers. This accomplishes nothing, since such vicious formulae do not need design advantages to give a huge report. You could wrap them in a single turn of newspaper and they would detonate.

Note another important difference between the American and Oriental methods. American salute theorists, if such exist, hold that powder should fill 1/3 to 2/3 the case-volume, or a softer report results. Yet, with the Oriental method, we actually achieve compression of the flash powder compared with its density in the open state. The reported value is about 1.2 times open density. This is said to help the report. Now, the Japanese have considerable experimental data to back them up when they opine that this is best. We must take note of differences in materials, formulas, and construction when comparing the two. Americans rely on a comparatively flimsy case with a fast but hazardous compo, while the Orientals use a safer compo but one that demands a stronger case and a hotter start from the black powder primer.

FISSION-FUSION-FISSION: A BIT OF TERRIBLE SPECULATION

Remember the World Book Encyclopaedia? Is it still around? The author's family got hold of a set in 1959, and the 7-year-old experimenter's curiosity forced him to read the whole thing. One unusually suggestive piece appeared in volume H, under "Hydrogen Bomb." The sinister ignition sequence began with fission. Every third-grader knew in those carefree days that fission sprang from exceeding the critical mass of nasty isotopes of uranium or plutonium.

This provided the conditions needed to trigger the second stage: fusion. Tritium, deuterium, or lithium deuteride, under incomprehensible conditions of heat and pressure, would fuse, releasing far more energy per unit weight than fission. This two-step gave us the hydrogen bomb.

But physicist Edward Teller had seen beyond this simple device to what had been called the superbomb, a term now lost out of disuse. It added a third stage to the fun. By encasing the works in otherwise tame uranium 238, even that meek isotope would undergo fission under bombardment by high-speed neutrons and other menacing particles thrown out by the first two stages. This added a megaton or four to the yield, in addition to producing some dandy fallout nearly absent from the "clean" two-step hydrogen bomb. (There has been much speculation and ballyhoo over the design of multi-stage nuclear weapons, especially over alleged secrets that made it into print. One called for the fusion stage to surround a rod-like core of plutonium which would be forced beyond critical mass by the temp and pressure of fusion, thereby upping the yield.)

Where do we get off jumping from nuclear weapons straight down to sub-military pyrotechnic units? Because the principles involved may, at least in theory, give us a fine, sturdy report from comparatively safe materials. Consider this diabolical speculation:

First, take a core of about 1/2" diameter made up of FFFg black powder, enclosed in a layer or two of tissue paper. The fuse or other initiator, such as an electrically fired squib, rests here also. Ignition of this black powder alone would give us no more than a quick flash and a puff of smoke. It corresponds to the first, or fission stage of the device.

Next, we must add the fusion component. Appropriately enough, this yields the greatest amount of energy per unit weight. As with the Oriental salute, we will make this a hollow sphere of perchlorate-based flash powder (3:1:1 of perchlorate, aluminum, and sulfur). Furthermore, we will use only the safer, bright aluminum, since other factors obviate the need for that restless dark variety.

We will arrange this in a 2-inch diameter sphere around the black powder initiator. From the discussion of Oriental salutes, we already grasp the workings of this device.

But this 2-inch sphere, although productive of a credible report if confined in an extremely strong case, would waste itself unless used as a trigger for safe material that would not explode satisfactorily under other practical settings. We will add a third layer, corresponding to fission because of its intrinsic benignity, yet propelled by the laws of physics into respectability from intense heat and pressure generated by detonation of the second stage: Center the existing 2-inch sphere in a 6-inch sphere filled with barium nitrate flash powder (4:2:1 barium nitrate, black pyro aluminum, sulfur).

Finally, form the outer casing from twenty layers of thick, heavy, pasted kraft paper to provide maximum strength.

Now step back and analyze the detonation sequence. The black powder will ignite the inner, potent flash mix on a spherical front, start it burning outward in all directions at once. Burning will shift quickly to detonation out of the exponential rise in temperature and pressure. The huge compression afforded by the mass of the outer layer of flash powder will add to this. By the time the shock wave reaches the inner border of nitrate-based flash powder, it will have created conditions of heat and pressure otherwise unobtainable by practical means. This will cause it to explode soundly, where it would otherwise merely offer a bright if uninspired flash.

Now, such a device clearly weighs several pounds; yet holds merit, despite its power, on safety grounds. Of all materials that might be used to produce a genuine gut-thumper (and this would find application in aerial displays, never on the ground....) surely this is the safest. The most dangerous portion of it all is the perchlorate-based flash mix; yet, use of bright aluminum rather than dark renders this combination as safe as it is possible to be.

Pure speculation. The author has never made such a device. Only desert-dwellers with proper credentials and licenses should even contemplate it. Still, the concept makes for compelling speculation....

BLACK CONES: DEADLY PRETENDERS

Practically everyone who has had the slightest contact with commercial fireworks has seen cone-shaped fountains. That shape, and what charm it holds, with its colorful wrapper and fiery memories, arose out of its analogy to the cone-shape of a volcano (and in fact some brands openly compared their products to Mt. Vesuvius).

The second point is that cone fountains contain about ten percent pyrotechnic compo by volume. The rest is nothing but space, wrap, and charm. The mark buys what appears to be a large item with a suitably large price. But upend the damned things: the actual compo in a foot-tall cone extends less than 2 inches down from the point.

Cone and other types of fountains have been labeled "safe and sane" in some states, meaning that they do not leave the ground (usually; some energetic Chinese fountains have been known to blow out the bottom and leap the roof...), nor shoot "flaming balls," and, most importantly, do not explode.

But it wasn't always so. In finer days long gone, so-called Black Cones were sold; black from the color and cone from the fact that frugal manufacturers thought they had found another use for the cones they used to make fountains. But these little devils sprayed nothing. They were small cannon-crackers in terms of weight of flash powder they contained. The diagram shows a generic example. Weight of composition ranged about 5-10 grams, the equal of several cherry bombs.

Variations existed. The cone that whistled before it blew was a real crowd-pleaser.

Now as to the mechanics of making Black Cones. First, this is a hypothetical discussion. Don't make any explosive device. That said, we see that we must first obtain the cones. Years back, these were available from pyro supply houses of which there were never more than a handful at a given moment. They are nothing more than the paper cones used as cores for skeins of twine, and should be obtainable from the appropriate textile source.

We can see that even the small 7" cones would take us into the Bomb category if filled completely with flash

powder. Thus, we need a cardboard disk, say, 1/8" thick, and of a diameter to give us the distal 1/4 to 1/3 of the cone, which is still only a fraction of its volume. Experience in the early 70s showed that this would comfortably hold about ten grams of flash powder, enough for five M-80s.

Stick a 4" length of green fuse through the top hole (NO EXPOSED PRIMING!), glue it in place, let it dry.

Next, upend the cone in a proper holder, pour in the powder, then seal the cavity with the disc and some glue. (It is considered bad form to get glue on the powder. This holdover comes from the days when flash powders used potassium chlorate. Many glues contain acid, death where chlorates are concerned.)

Ah, but we deny ourselves such sophistication with this simple approach. Could we achieve a louder report with safer powder by using an initiator? Refer to the speculative diagram. Here we have glued a paper tube of 3/8"-5/8" inside diameter securely into the end of the cone (half an M-80 casing will do), and sealed its end with glue. Inside this cylinder, we have loaded a gram of FFFg black powder, and sealed the end with a layer of thin kraft paper. When the fuse ignites this black powder, it will spray the flash powder with hot gasses at extremely high speed, giving us much the same effect we have in the Oriental method, though with some loss of efficiency, but still a hardy gain over one limp spark from the fuse.

From here the imagination takes a dark turn, seemingly unable to refrain from comparing itself to nuclear devices, as with the ominous fission-fusion-fission aerial salute. We see that we have the makings of a linear, rather than a spherical device, one with unusual properties when used with titanium in the final stage, discussed momentarily.

Our basic initiator is a fission-fusion stage corresponding to black powder starting ten grams or so of flash powder. (Sorry, but we cannot get away with the safe, bright pyro aluminum. Truth told, the Black German variety works best here, but we needn't resort to chlorates.)

What begs to be used is all that space beneath the strong flash powder. What if we were to pack it with, say, the barium nitrate flash mix which happened to be a third by weight granulated titanium, 20-40 mesh?

Detonation of the overlying salute would subject it to conditions of pressure and temperature difficult to obtain without a metal casing, a taboo under all but military circumstances. Those do not interest us.

Construction of this device proved easy in 1970. Its detonation (so far out in the desert, away from any flammable materials that you could've tested a real H-bomb without fazing old ladies pumping slot machines in Vegas) produced A) a damned impressive report for its size; B) a genuinely blinding flash; and C) an existential experience: No one can forget films of the Castle Bravo test—an early test of the hydrogen bomb, out in the pacific. Some have rated its yield at 15 megatons. Its most striking feature was the fireball, miles wide, blooming fast, then pausing like an eerie breath of Hell suspended in the air. Well, the burning titanium here disperses in exactly that terrible hemisphere of a pattern, and with the same sort of slow-motion at the end. The hackles rose when the author saw this, so closely did it mimic the thermonuclear fireball recalled from fine nuclear training films shown to third-graders in the 1950s....

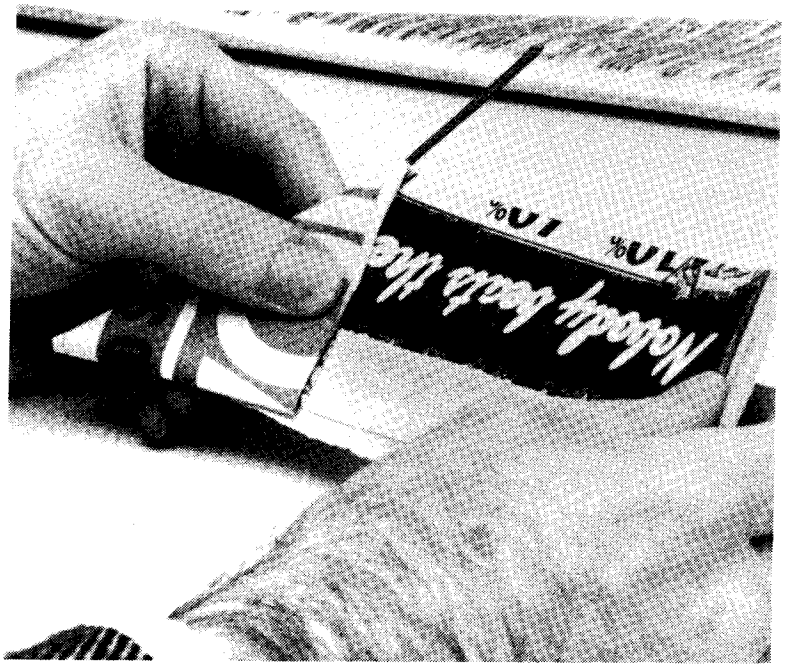
Incidentally, the length of fuse protruding from the end of the cone should be long enough to give you enough burn-time to get to a distance safe from the blast radius. At 3 seconds per inch, and assuming you run the hundred in ten flat, that means about a foot of fuse.

Intriguing speculation, for grim groundburst fantasies only. At least you won't have to worry about electromagnetic pulse....

With that sick fantasy out of the blood, go back and remember the one deadly point about cone salutes: Cones had come to be identified so much with harmless fountains that kids thought all cones were fountains. Some found out the hard way that they weren't. That alone is enough reason to leave black cones on the pages of sordid tales such as this, rather than in your hobby shop.

TRIANGLE CRACKERS/ANY PAPER CASE WILL DO

In the frenzy over the sale of "kits" with which to make ground salutes, we have seen a vengeful stupidity



TRIANGLE CRACKERS. TOP LEFT: Start with strip of paper 1-3/4" wide. Fold at 60-degree angles to form pocket (TOP RIGHT). Fill pocket w/flash powder and fuse. MID LEFT, MID RIGHT: Continue folding at 60-degree angles until all paper used, seal with paste to form completed triangle cracker (BOTTOM LEFT). Width and type of paper not critical. Use whatever's handy.

that prompts laws that cramp the innocent more than the guilty. In case it isn't obvious yet, flash powder in any casing will produce satisfactory results. Witness the triangle cracker.

American travelers returning from Mexico smuggle triangle crackers back across the border. To make them, cut a strip of paper about 1-3/4" wide and a foot long. Fold to form a triangular pocket at one end. Pour in 2 grams of flash powder and insert a length of green fuse. Then fold the rest of the paper at 60 degree angles until it is sealed, hold the end in place with a daub of paste, then seal the corners with glue so they don't leak powder. Voila: the triangle cracker.

The two minutes it takes to whip one up is shown in the photo set, using dummy flash powder. Because of the relatively weak casing it is necessary to use either perchlorate with Black German Pyro aluminum, or a chlorate-based comp. In practical terms that makes these little bangers too dangerous to handle.

A more elegant set of instructions for making them appeared in the early 1970s in American Pyrotechnist Fireworks News, but the author was not able to tell any difference in performance between those made with this eyeball-it method compared with measure-and-cut methods.

Here again, triangle crackers demand that you handle them well after they have become explosive. They illustrate the lunacy of banning cases marked "M-80."

FIELD-EXPEDIENT SALUTES

The Fourth, or perhaps New Year's Eve, is tomorrow, and you haven't a thing combustible in the house. No time to order casings, end caps to whip up a few bangers for festival. But there is hope. You will need flash powder (instead of mixing your own, with its risks and getting on surveillance lists, get it out of ready-made crackers) and green fuse (push-to-shove: buy legal Class C pyro devices and scavenge the fuse).

You will need a wooden dowel about 1/2" diameter by 6" long. It will make it easier to handle if you sand it smooth and coat it with a touch of flour before you begin rolling cases.

Next, cut strips of newspaper 2" wide, about 8" long (the photo set used newsprint and inert powder). Roll them into tubes with 1/2" protruding from the end. Secure the roll either with tape or a bit of paste. While the tube is on the dowel, fold the ends over to seal that end, then secure it with two strips of tape, at right angles. Remove the tube from the dowel. Make as many as you think you'll need.

Next, dump in enough fine, dry sawdust to prevent any powder from leaking out the bottom of the case, and insert a 3" length of green safety fuse. Then pour in 1 to 3 grams of flash powder (depending on how loud you want it, how many crackers you are willing to dismantle per banger). Tap the tube gently on the table to get the powder to settle; you do not want it to mix with the sawdust.

On top of the powder, pour in about 1/4" of sawdust or rice chaff. The fuse should lie at the edge of the casing, not the center. Tamp gently. Now fold in the remaining paper starting with the side opposite the side of the fuse, then fold in from the sides adjacent the fuse. The objective is to get the paper wrapped tightly around the fuse. The fourth and fifth folds will bring the fuse over at 90 degrees, then another 90 degrees so it ends up pointing toward what was the bottom of the salute. Secure the folded newspaper and fuse with tape.

In case it isn't yet clear, there should be absolutely no exposed powder or other place where ignition could take place prematurely.

What you have constructed is a variation on a device known to Europeans as "petards" (modesty curbs translation....). True petards are made this way, but substitute bare black match (string impregnated with black powder; a highly ignitable and quick-burning fuse that sees countless uses in pyrotechnics). Handfuls of petards fill aerial shells. When the shells burst, petards explode half a second later in a barrage. The ground salute with its 3-inch fuse will give the shooter time to retreat.

One source recommended use of potassium chlorate and Black German pyro aluminum as the flash mix for petards, but we must take issue with that on safety grounds. We found the perchlorate quite satisfactory,

back in that grim summer of Watergate, and less prone to bring out sour sweat from worry over premature detonation.

WHAT NOT TO DO

Consider any casing that throws off hard fragments taboo. That includes all metals, PVC pipe, glass and ceramics, and anything with clumps of the professional pyro adhesive described previously (a thin film of it won't hurt).

In addition to their deadly fragments, these casings predispose to premature detonation. For example, with metal pipe you have to screw on the end caps. Friction created at the threads can set off the bomb in your hand. PVC pipe is prone to accumulate enough static electricity to ignite many aluminum-based mixes.

MIX YOUR OWN FLASH POWDER?

As an alternative to mixing flash powder from raw chemicals, use the powder contained in commercially available flash crackers (firecrackers, flashlight crackers). You do not have to buy strange chemicals that move your name and address to the top of a surveillance list and get your phone tapped. Plus, it eliminates the mixing process, one of the riskiest parts of manufacture.

In 1969 the author use a pair of nippers to halve firecrackers and remove their precious powder. Each could hold the then-legal maximum of 2 grains—about 120 milligrams. He loaded the powder from a dozen, roughly 1.4 grams of powder, which filled an M-80 casing less than half full, into each bomb. The source-firecrackers happened to be Black Cat Brand, which, as the package states clearly, "Black Cat Is The Best You Can Get," or at least it was when a firecracker could hold more than the 50 milligrams of powder it's held to in these thin times, a token charge that has trouble bursting a flashcracker case. This powder burns with disarming sluggishness out in the open; yet these salutes gave more bang for their size than any the author made in his entire depraved career as a pyro, which fizzled well over 15 years ago. Friends used to comment that it was embarrassing to shoot these salutes, even though we had skulked out into the woods and presumably were the only ones to hear their devastating reports. They exploded so fiercely that, thrown on a highway, they left a splotch as if the red paper case had been laminated to the pavement. No home-brew mix ever equaled that grim feat. The photograph shows the top of an empty gallon paint can found in an illegal trash dump deep in the woods some years ago. When discovered, the can was intact and closed. A single Black-Cat-derived M-80 was placed on the top, then detonated. It punctured the top, venting enough pressure into the can to blow off the lid and send it careening into the woods. Such was the power of these fearsome salutes.

Using premixed powder has its risks. Since you do no mixing, you do not know what the powder contains. You can see that it contains aluminum, or at least some powdered metal. But what you do not know may be the most crucial piece of safety-related information about a tube salute: Does the powder contain potassium chlorate?

If so, and if you carelessly let an acid-based glue drip on it before sealing, you are setting yourself up for a spontaneous detonation. The reason is that potassium chlorate mixed with a fuel ignites spontaneously in the presence of acids. Never mind the obscure chemistry of it; it happens (in fact, a test for the presence of chlorate is to take a small sample of powder, put it on a brick, then, with appropriate safety precautions, touch it with a glass rod which has been dipped in concentrated sulfuric acid; chlorate-containing mixtures will ignite). So, anyone who actually made tube salutes with unknown flash powder, and we do not recommend the making of tube salutes, puts himself and bystanders at risk. Act responsibly.

When salvaging flash powder from firecrackers, carefully extract the fuse before halving the cracker, about midway between the ends. Then take the halves and turn them mouth-down and roll them back and forth between your thumb and forefinger. The powder will pour out.

That approach made more sense years ago because crackers held more powder than they do today. Assuming a potent formula to begin with, almost certainly one containing the dread chlorate oxidizer, you could in theory buy flashcrackers in bulk and remove their powder. At less than 50 milligrams apiece, it will take 25-30 per salute; fewer, if you can get by with a less robust report. If Black Cat has not changed its formula, nothing the author has seen can touch it in terms of raw power.

Another word about safety. Whenever you handle finely divided chemicals, no matter how harmless or inert they seem, wear a respirator that will keep them out of your lungs. Charcoal, finely divided aluminum, and especially known poisons such as arsenic, get in the lungs and can cause emphysema as well as poisoning.

A PHILOSOPHY OF PYRO

Those who just have to play with this stuff should understand that there is a right way and a wrong way. The right way costs money—lots of it, in fact—and means heavy sacrifice and loss of privacy, perhaps a life of hermitage.

That grim other route, the wrong way, means eventual injury to self and bystanders, possibly death, along with an ugly media splash and a trip to the big house when you are discovered, a certainty.

Only a fool would choose the wrong way. We won't even discuss it. This outlines the right way:

STEP 1. If you do not already reside on barren, open land, free of the risk of forest fire, so far from the neighbors or a secondary road that you will draw no attention, buy the land and move to that secluded and desolate spot.

STEP 2. Construct your hobby shop such and locate it far enough from the residence and other structures that no damage will result even if it all vaporizes at once. (If you plan to store chemicals in bulk, particularly the militant oxidizers, it might not be a bad idea to get a steel door and some locks and alarms, in case you become a target of thieves.)

STEP 3. Obtain all necessary federal, state, and local permits and licenses to engage in the manufacture of explosives for non-commercial use, unless you intend to make a go of it as a business; or perhaps hold yourself out as being engaged in research. This is a legitimate ploy, since who knows what you may stumble upon. This will mean letting BATF in on everything you do, keeping records of how much of this and that you buy, where it goes, what you made, whether you distributed any of it to third parties. It also opens otherwise verboten sources of chemicals. The feds will run a background check on you, print and photograph you—and the boys will want to keep in touch. They may not choose to make that on-site inspection during daylight hours....

BATF "knows" about the pyro underground, and could bust thousands of weekend, non-commercial cherry-bomb makers if it wanted to (uh, yes, if you bought chemicals, fuse, and casings by mail, BATF can pull your name and address up on their computer in the time it takes to punch in your personal BATF ID number...) But it infiltrated the fraternity long ago, found it harmless—patriotic, in fact—and elected to leave it alone, at least until the political wind in D.C. chills and blows left. It has no qualms about busting wholesale manufacturers, and who can blame it? Human nature allows no other behavior.

STEP 4. Act responsibly. Do not let third parties fool around in the shop, and NEVER let them get their hands on chemicals or finished goods of any kind. Drop no casual remarks as to what you have mixed with what. Many an oaf would take it upon himself to try it, with horrendous results.

STEP 5. Tell others about your strange hobby only on a need-to-know basis. People talk. Tell your most trusted friend anything and you have told the world, populated by generally conniving and worthless people.

STEP 6. Do yourself a favor and observe all safety precautions rigidly. Observance does not guarantee that an accident will not maim or kill you. But give yourself the best break, know what kind of risk you are taking.

STEP 7. Learn the properties of all materials you handle. You can learn it without a chemistry degree, but that sheepskin and the ancillary matters behind it (physics and physical chemistry, for example) makes you more aware of chemical interactions, static electricity, and other forces not chronicled in the literature of pyro, and puts you onto information sources the unlettered might never consider.

STEP 8. Don't even think about steps 1 through 7 unless you have reached the age of 30. They say life begins at 40. Those who have been there will testify that those under 30 can act pretty irresponsibly. In general, folks under 30 have not acquired enough judgment to take proper precautions. Sorry, no exceptions....

For some, the Pyro Way is the only way. It gets in your blood, like the sea or the wild or a strange affinity for strong drink. Just be sensible about it. Know the pitfalls, avoid them through information and preparation. Teddy Roosevelt said to avoid trouble by preparing for it.

CHEMICAL SOURCES IN THE AGE OF PARANOIA

Popular Science has traditionally reserved a section of its classifieds for "Science and Chemistry," a carryover perhaps from the days when those terms called forth images of Mr. Wizard and rocket scientists the country craved in the desperate wake of the Sputnik incident, and which it saw arising naturally from the pool of eager young minds that defined American Youth. Interest in such matters was openly regarded with approval; experimentation deemed a natural outgrowth of curiosity.

But times change. Today, knowledge of chemistry—or electronics, computers, or firearms—has come to be tied almost solely to money and power. No one has to say that the most profitable of all uses for this knowledge are illegal ones, or that the most heinous are political through their abuse of innocents.

For a while, PS warned readers that one or more classified ads under the "Science and Chemistry" section had been reported in another publication to have been placed not by chemical dealers, but by the Drug Enforcement Administration. Folks who wrote for these tainted catalogs found their names and addresses on surveillance lists. Those who ordered the mixin's for, say, dextroamphetamine sulfate found themselves with even more. Federal scams aside, the chemical companies proved only too happy to turn in those whose ordering patterns rattled the DEA or triggered an alarm.

Today our keepers see yet another reason to check access to certain chemicals: terrorism. The fantasies outlined in these pages could be blown, so to speak, into proportions involving hundreds of pounds of material, in which case devices intended to provide little more than harmless excitement on New Year's Eve would be perverted into dreadful instruments of harm. Unfortunately, enough mutants are willing to corrupt this knowledge that a formerly totalitarian attitude toward chemicals has taken on a rude cloak of legitimacy. The cyanide/Tylenol incident did little to calm the paranoia.

With the right elements and access to the average college library, it is possible to make C4, nitroglycerin, napalm, nerve gas, phosgene, and even pure skunk scent. What a sad testament that there are those who would make it and put it to unspeakable ends.

The extreme Left and extreme Right have, through tacit custom—mutual assent, it sometimes seems—chosen contrasting ways to misbehave with chemicals. The Right has come to be linked with material we've just outlined: explosives, boomers, roman candles, and everything else Ted Kennedy would rather crap in his pants than let you get your grubby hands on. The Left, on the other hand, sees nothing wrong with whipping up a batch of amphetamines or blotter acid, even selling it in a twisted sort of capitalistic venture it normally abhors. The Left gets its explosives via roundabout routes from the Red Bloc: Why fool with flash powder when rocket-propelled grenades are yours for the asking? Ah, hypocrisy. Human nature won't let even political extremists sulk in peace.

The practical point behind it all says that people in the business of selling these goods and people in the government will presume that you plan fiendish deeds when you sign up to buy certain substances, whether that presumption be true or false. You will command more attention that you imagined just by ordering chemical catalogs. In today's grim environment, that's enough to get you checked out for criminal connections and political bent (if you are linked to the Klan, they will assume you're making explosives; if you belonged to the SDS or voted for McGovern, they will assume that you aim to synthesize angel dust).

Here the issues of alternative ID, mail drops, and so on begin to take on new meaning—but don't kid

yourself. Even the best of the fake IDs will not hide you if the feds decide in a serious way that they want to chat.

Chemicals listed in catalogs obtained in early summer, 1988, from firms that advertised in Popular Science showed a dreary lack of verve. Chemicals of the type and quality best suited to pyrotechnic use are simply not found openly. One must dig, tap into the old-boy network and such. Several firms will not sell chemicals to individuals, period. True, some chemical companies sell potassium nitrate and potassium perchlorate, but it is usually reagent grade, which makes it prohibitively expensive. Grades suited to pyro use are either "pure" or "technical."

We interviewed two individuals associated with Square Lake Enterprises, Inc., successor to the now-defunct WesTech Corporation, via telephone on 8/29/88. Square Lake, as far as we have been able to ascertain, is the only remaining source of pyro-grade chemicals—but several catches could hang you up. The firm operates under a consent decree in the wake of a legal onslaught from the muscle end of the Consumer Product Safety Commission. Sources at Square Lake indicated that their counsel advised them that the cost of fighting restrictions in court would prove astronomical; that even if they won, they would lose out of insupportable financial burden. To stay in business, the principals agreed to a consent decree that limited sales of finely powdered metal to half a pound per person per six months, except to licensed manufacturers of explosives, and to keeping records in such detail as to allow verification of compliance, as well as legitimate cooperation when some mutant decided to misbehave in a serious way and chose an explosion as his modus operandi. SLE does not sell potassium chlorate, and CPSC has forbidden them from selling barium chlorate. They do not presently carry ammonium perchlorate because the military and space agencies have seized control of the sole remaining source in the United States in the wake of an explosion at the only other NH4ClO4 plant. That second manufacturer is rebuilding, and SLE intends to resume sales when supply restrictions allow. They will not sell oxidizers and combustible materials ordered simultaneously; the customer must order them on separate forms, pay by separate, guaranteed funds or have materials shipped COD.

Their chemical inventory includes potassium perchlorate, potassium nitrate (with anti-caking material added), potassium permanganate, barium nitrate, strontium nitrate, antimony sulfide, titanium in either 10 mesh or 60 mesh; aluminum in bright, pyro, and Black German pyro (mesh claimed is an incredible 600). They sell syrupy sodium silicate and calcium carbonate, the ingredients of fabled professional pyrotechnic adhesive, as well as green and red safety fuse, glue, a few mortars suitable for making class C fireworks.

SLE does not offer tube salute casings, since one of CPSC's key attack-points held that simultaneous sales of chemicals and casings designed to produced banned report devices constituted sales of kits to make same. We have already shown the mindless futility of restricting sales of paper tubes. In fact, one might argue that CPSC's actions could backfire in the sense that experimenters might turn to PVC or metal cases.

Sadly, they offer literature that, while containing some timeless and useful information, may lead the novice straight down the route to ruin: Weingart's Pyrotechnics and Davis' Chemistry of Powder and Explosives, both 40 years out of date. They offer two apparently proprietary treatises we have not seen. We asked why they did not carry Ron Lancaster's Fireworks: Principles and Practice, and the reply was that it was not a hot seller at $35. Read carefully the cautions below regarding pyro literature.

They will not sell to anyone under the age of 21, and require a photocopy of your driver's license with the initial order. Fact is, they keep more info on file at Big Brother's behest than the local gun shop where you bought that last box of shotgun shells....

The author has not purchased pyro materials since 1973. Taking inflation into account, pyro-grade chemicals now sell for prices one can only describe as lethal.

We asked whether the principals at SLE suspected themselves or the company to be under surveillance, and neither felt that they were. Of course, if B.B. didn't want them to know, they wouldn't.... Write for their catalog c/o PO Box 3673, Logan, UT, 84321. Their order form asks "Where did you hear about Square Lake Enterprises?" It might be unwise to mention this dread text....

What if dedicated pyro suppliers dry up? Chemicals in proper grades and particle sizes would remain available. Otherwise, a domestic pyro industry would cease to exist. But companies that routinely sell 500 pounds of potassium perchlorate, technical, 200 mesh, to the Rozzazzo & Fong Fireworks Co., Ltd., do not want to hear from you. First, you probably want five pounds at most. Second, like every business in America, they have found it impossible to ignore the rising tide of product liability suits. All they need is to sell you a potent oxidizer, have you blow off your right hand, then have to defend themselves against a multimillion-dollar lawsuit brought by your parents, since you happened to be 15 years old....

In a practical sense, only one path offers access to whatever chemicals you wish to use, and without hassles or drawing heat. That means following the arduous steps toward becoming a serious pyro, properly licensed and such. It would not hurt to prepare some stationery and a set of purchase orders and a bank account with your business name. You would be surprised how many doors it opens. And, of course, when a chemical firm receives a significant order for hazardous materials, it helps to have it accompanied by a business check, a purchase order, a cover letter on the appropriate stationery, and a "true copy" of your explosives license. Without the license, forget it.

You will probably have to buy most chemicals in hundred-pound lots, but that is part of the price of dabbling in the occult. If you cannot pay the fare, get off the train. You will save a bundle over what pyro supply houses used to charge for a pound of anything, at least when pyro houses existed, and you won't have to buy again for a long time....

THE LITERATURE OF PYRO: CAUTION!

Available in reprint are George Washington Weingart's Pyrotechnics, Professor Tenney L. Davis' The Chemistry of Powder and Explosives (incorporated in The Poor Man's James Bond, Part II; apparently, Davis' book has passed into the public domain), and Britisher Ron Lancaster's Fireworks: Principles and Practice; along with a sampling of highly technical manuals such as Military and Civilian Pyrotechnics, by Herbert Ellern, and the translation of Schidlovsky's Russian treatise on the subject, complete with differential equations to keep you up into the wee hours....

These books make fine reading, but present definite hazards for the uninitiate, who haven't yet learned from theory or practice the breed of doomstruck compositions that guarantee an abrupt and explosive end to one's career.

The first two texts mentioned, The Chemistry of Powder and Explosives and Pyrotechnics, grew out of a very different era—circa 1943 and the early postwar years, respectively—a time that saw cherry bombs, torpedoes (a cherry bomb with no fuse that explodes when thrown against a hard surface), and cannon crackers sold openly (the #12 cracker measured 1-1/2" x 12" long, and came in boxes of 25). Worse, industry standards called for potassium chlorate as the oxidizer because it saved money over the perchlorate and gave a genuinely terrible bang. Those babies earned the name, cannon crackers. These texts tell exactly how the big crackers were made, and what compositions they used. The modern pyro, pro or amateur, gets the creeping Fear just dreaming that these formulas ever got mixed, much less placed in unenlightened hands.

And you can get those books from the same outre' tribe of dealer who stocked this grim rag.

The point is, read those older texts for interest, for historical intrigue if you wish. But under no circumstances entertain studies of whipping up a batch of Weingart's chlorate-based cannon cracker formula #3. Odds are, it will detonate while you're mixing it, and you can kiss your hands, eardrums, and eyes goodbye, then learn our probation system from the inside, since the judge won't have the heart to send up a first-offender, especially after your crippling accident....

8
ODDS & ENDS

"Vengeance is Mine," sayeth the Lord—and Mickey Spillane....

* * *

LIE DETECTORS?

Everyone knows the basics: Certain physiologic changes are believed to flag the subject who knowingly fibs. That assumption underlies the notion of lie detectors. Polygraphs and voice stress analyzers are the two most widely touted. The polygraph measures pulse, respiration, and galvanic skin response (a fancy way to say "sweating"). The VSA registers supposedly inaudible voice tremors.

But these tools post erratic track records. The media, in its rare fits of public service, has profiled horror stories of men and women denied employment, fired, incarcerated, or—worst of all—suffering bruised credit based on goofed-up lie detector tests.

One exercise proved particularly instructive to students of human physiology. The polygrapher was told that one of a series of subjects was suspected of thievery. The examiner tested all subjects. In every case, the machine found the marked suspect to be lying, yet that subject was utterly innocent. This was repeated with different subjects and different polygraphers three times in a row, with the same results. What could account for such consistent inaccuracy?

Simple. The human nervous system can, in fact, detect subliminal physiologic phenomena at an unconscious level. Our subconscious can hear the sounds the VSA uses, even though our hearing technically extends only to 20 Hz (though we damned well sense the 5 Hz rumble of an earthquake). The same applies to intonation, accent, and gestures. It probably applies to facial expression as well. You've heard the phrase, "guilt written all over his face"? This refers to a set of the features almost impossible to produce at will that we see on the faces of guilty persons—or those who <u>feel</u> guilty.

The human subconscious can integrate all this and come up with a fair estimate of whether someone is lying, probably because that ability had survival value millennia ago. Today we see the evolution of a new subspecies, those who can lie poker-faced, without tells. That ability seems to possess survival value, too. Lawyers and politicians bear it...just the breed we want to flourish and rule our world....

Now, get this: A subject's perception, conscious or subconscious, that <u>someone else</u> believes he is lying may induce, or at least heighten, those physiologic responses that polygraphers associate with deception. The fact of the examiner having been told that a certain subject was suspect becomes a self-fulfilling physiologic prophecy.

If guilt can be written all over the human visage, so can the belief that someone else is guilty. The human subconscious spots both looks. Trained persons, usually police, who live in a world of lies, come to hone this skill finely.

Think about it. Haven't you ever been wrongly accused of some bad deed? Remember your reaction? Flushing, rapid breathing and heart rate, sweaty palms, trembling voice. Just how does that differ physiologically from the deception response?

Of course, another possibility says that polygraphers in these grim studies didn't want to look bad by finding nothing. They have to earn a living. The polygrapher who reported zip might find his employer looking for a "better" polygrapher....

Agreeing to take a polygraph exam, or believing the results good or bad, both represent no more than a roll of the dice.

EVOKED RESPONSES: THE NEXT STEP?

The author once supervised a neurophysiology lab that routinely ran strange and venal tests called "evoked responses." This chat carries the weight of personal experience, even though the author has forsaken the horror of Hippocratic rot for the decadence of deep-fringe writing.

Back on track: Evoked responses are electrophysiologic phenomena elicited by any of a variety of stimuli and recorded, most often, from the brain. The commonest examples are visual, brainstem auditory, and somatosensory evoked responses. Their corresponding stimuli are a black-and-white video monitor displaying a checkerboard pattern that reverses black-for-white about once a second; rarefaction clicks (the speaker diaphragm moves only backward with each click) delivered through an incredibly expensive set of headphones; and subliminal shocks applied to various nerves. The characteristic waveforms seen in response to these stimuli and recorded from the head are known as evoked responses. The diagram shows examples from the author's lab.

What end do they serve? They rank as the most sensitive means of detecting subtle dysfunction of otherwise inaccessible neural pathways. A patient may show a perfectly normal physical exam, only to have visual evoked responses detect clear-cut abnormalities that identify multiple sclerosis. Brainstem auditory responses may become abnormal years before the appearance of a tiny tumor of the nerve that goes to the ear.

Recording evoked responses compares with plucking a 1-watt radio transmission from Australia out of the air. The responses sometimes measure a fraction of a millionth of a volt in size. Only computerized averaging of series of a hundred to several thousand stimuli, which attenuates the noise component, lets us view the raw evoked response in its naked splendor.

The most important aspect of an evoked response waveform is its latency: the time between the stimulus and the appearance of the response. This ranges from about 1.5 milliseconds in the case of brainstem auditory evoked responses, to several hundred milliseconds in other types—so-called "late" responses. Early responses correlate clearly with known anatomy and disease.

But there is something mysterious, almost spooky, about these late responses. We don't yet know exactly what they are or what they mean or how the brain generates them. But we have learned enough to put us onto them as potential truthsayers with a 99 percent accuracy rate, this compared with 20 to 80 percent for the polygraph or VSA, depending upon whom you choose to believe.

In a chilling series of experiments, subjects were given a word and told to remember it. Then they were hooked up to the fiendish recording apparatus. A video monitor displayed a series of words, and the brain waves were checked for an evoked response after each word. What a kick when the only word to trigger a late evoked response was the one they had been asked to recall.

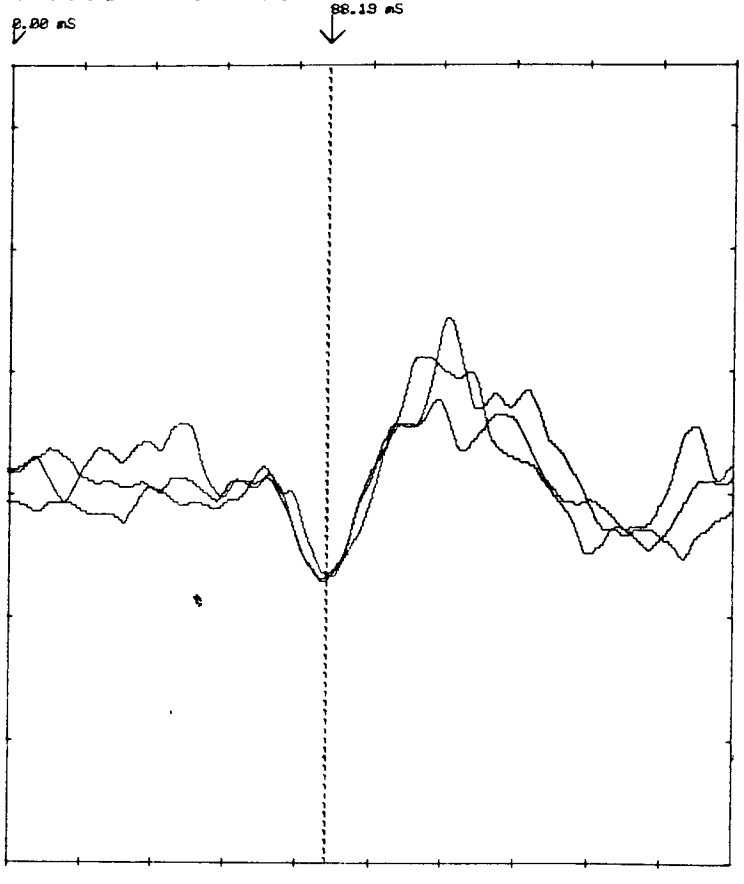
Note that evoked responses are involuntary. In fact, brainstem auditory and somatosensory evoked responses record with exceptional clarity from subjects who are asleep, even under general anesthesia. Thus, they have shown the capability to bypass conscious sentries that jinx the VSA and polygraph, and at least potentially would find application in totally uncooperative subjects.

[redacted]

7/31/86
VEP1
G= 20 H= 70 L= 10.0
S=20.00 RR= 2.11
AVE= -1/100 SC= 10

OS

T=88.19 0.00 DELTA=88.19



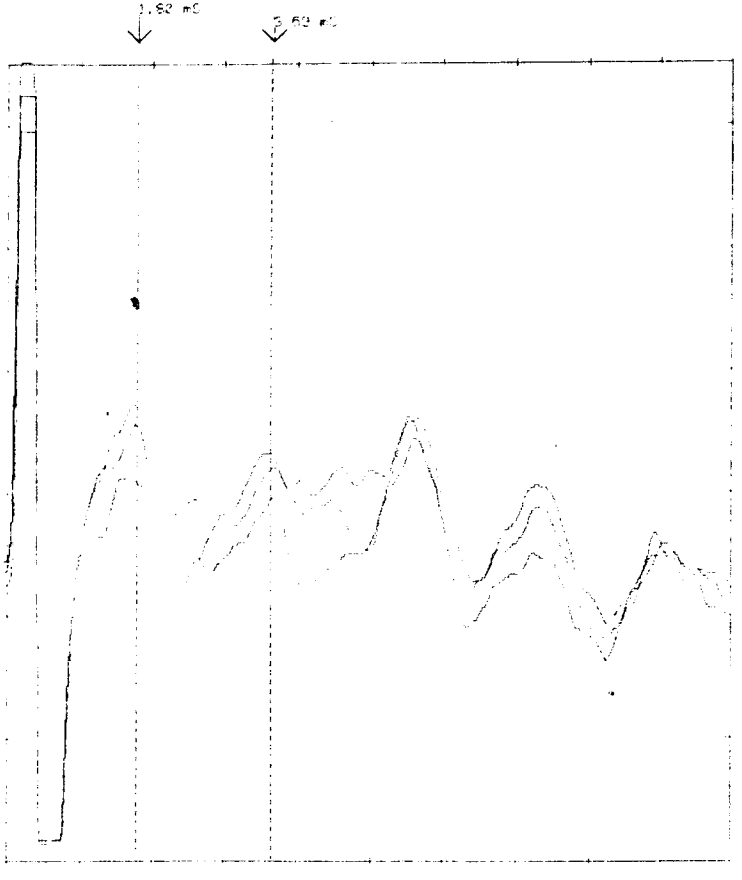
[redacted]

G= 10 H=3000 L=100.0
PW=100 S= 1.00 RR=11.10
AVE=1005/2000 SC= 30

CLICK RARE
THRESHOLD R= 25 L= 25
INTENSITY R= 70 L= 70
MASK R= 50 L= 0

10/30/86
AS

T= 1.88 3.69 DELTA= 1.80



LEFT: Visual evoked response, left eye, normal. Response elicited while subject watched video monitor displaying checkerboard pattern that reversed black/white. Result is computer average of 100 reversals. RIGHT: Brainstem auditory evoked response. Amplitude measures on the order of a microvolt, series of peaks easily reproducible, but demand 1000 or more clicks per series to average out noise. Normal series of peaks.

Two background scenarios: 1) A manufacturer of evoked response instruments told the author several years ago that his firm was close to a breakthrough in recording electrodes that did not have to touch the head. (This is not the same as reports of reading single words in a person's mind from a distance, using vaguely described apparatus, but the real thing with immediate medical applications.) Conventional electrodes must be applied with conductive paste or a pure evil glue called collodion. Marks who would never sit still for the wires could be maneuvered into position near a sensor, then questioned. 2) Texts on hypnosis infer that the unconscious mind continues to hear all that goes on around us even while we sleep, including sleep induced by general anesthetics. The author witnessed something that bore this out during a horrible stint in medical school. A surgeon had just removed the gallbladder of a chronically complaining woman. Wishing to rid himself of her, now that the cholecystectomy fee was in the bag, he told her, somewhat playfully, while she was still under the gas, "Mrs. Gide, tomorrow you're going to have trouble with your female organs!" Sure enough, next day her complaints shifted to the appropriate area.

If it turns out that we can record late evoked responses from sleeping persons, the scheme reduces to slipping the mark a mickie, wiring him up, and "asking" questions in a special form, for example, "You did steal the missing drugs." This, if all panned out, would elicit the late evoked response. "Check questions" might resemble "You did not crash your car on the way to work this morning," and so on.

It is quite a leap from that doomstruck experiment to truth-saying through evoked potentials, at least so far as the mainstream medical literature reflects. Frightening enough that a start has been made. The CIA has probably been gnawing at it for ten years....

* * *

...YES—BUT DO THEY KNOW?

As part of research for this book we had the publisher mail questionnaires to the Motor Vehicle Bureaus in all 50 states. Rather than waste several pages reprinting their addresses, phone numbers, available info and fees, since that essential but dreary data has seen space in no less than 4 other books, we'll throw in a question that might not have occurred to those who would tap the MVB for information: Does the Motor Vehicle Bureau keep records of parties who request information? If so, will they give that data to the subject of the query? In other words, can the mark pick up your trail by checking with the MVB to see who's been snooping?

In many cases the answer was yes.

If spooklore has taught us anything, it's the frightening extent to which we may do unto others...and they unto us. This dictates discretion, perhaps use of a mail drop and an alias, when digging up the goods on someone likely to take it personally, and who probably owns 6 volumes on tactical revenge. Pay by money order, not personal check.

ALABAMA

Stated only that requests for info must appear on a special form containing the requester's notarized signature.

ALASKA

Maintains no records of requests for info.

ARIZONA

Required to keep copy of request for at least 6 months, but that info for internal or law enforcement use only.

ARKANSAS

Stated that they do keep records of requests for info, then went on to note that "When a traffic violation report is sent to any requester other than the licensee, the licensee also receives a copy of the traffic violation report. Requests for information on records are kept by the department. Although requester

information is available to the public, individuals on whom the request for information was made is not public information." You figure out the syntax.

FLORIDA
Excludes personal info on active or former law enforcement officers (address, phone number, photos, employment of person or family, "confidential/fictitious registration records"). Law requires them to record the name of anyone other than law enforcement personnel who requests info about anyone else, the name of the subject asked about, and to keep the info for a minimum of 6 months. They sell photographs of the subject, up to 20" x 24" B&W enlargement, for $3.75.

HAWAII
Requires that persons other than those having a clear-cut need to know driver info sign an affidavit, and in some cases post a bond before being given info. They did not answer our question as to length of time such info would be kept, but we infer from material they sent that a request would generate a significant paper trail leading to the inquirer.

IDAHO
"Records of requests for information are maintained for 3 years, but volume alone prohibits providing this information, if requests were made."

INDIANA
Keeps records of requests, but did not specify their fate or accessibility.

IOWA
"Some requests for record information may be kept for a limited period of time and would not be considered confidential."

MAINE
Keeps requests for info on file for 1 year; requests deemed public information.

MINNESOTA
Retains records of requests for information "for accounting purposes only."

MISSOURI
Did not address issue; however, maintains one of the most comprehensive databases we reviewed, high prices; on an intuitive basis we suspect that they keep records of requests for info.

MARYLAND
Keeps records of requests, which can be released to anyone.

MONTANA
Keeps requests of motor vehicle info for 3 years.

NEVADA
Maintains records of requests "for audit purposes only."

NORTH CAROLINA
Did not specifically state, but request must be submitted on form that asks for requester's name, address, phone number, and DL number, and reason for request.

NORTH DAKOTA
Law requires them to notify the subject when someone requests a copy of his driving record, and to identify the requester.

OREGON
Keeps requests for info for 3 years, they are public records.

PENNSYLVANIA
Retains copies of requests for info for 3 years, and will reveal to the subject that he has been asked about; however, source stated over the phone that such records were not computerized, were stored and would have to be dug up manually, such that it might be possible to miss the fact that a request was fulfilled.

TENNESSEE
Does not keep records "...in a manner in which they could be located. These records are kept only for auditing purposes."

VERMONT
Does not maintain copies of requests for info.

VIRGINIA
Retains all requests for driver's records for 3 years and will disclose date and to whom furnished upon written request from the subject asked about.

WISCONSIN
"Varies—call if you want details."

Replies from the following states did not address the question of keeping records of requests: CA, DE, GA, MA, MI, SC, SD, TX, UT. The rest of the states didn't answer the letter, printed on the publisher's expensive bond stationery....

* * *

CREDIT, ALTERNATIVE ID, AND RELATED MATTERS
Let's skip the waltz and get straight to the tango.

1. Perfectly innocent men and women have legitimate need for alternative ID.

2. The only paper worth getting is genuine paper. Phony paper burns with felonious smoke.

3. In many states possession of alternative ID is not a crime. In some states it is.

4. None can deny that some use alternative ID for crime, but the same holds for use of guns, cars, and common tools for crime.

As a rule, American citizens can call themselves anything they wish, and change the name at will, so long as foul deeds or intent to commit them don't taint the scene. You can live under an alias if you wish. The alias, this name other than your given name, becomes your legal name after a period in some jurisdictions.

Which holds fine in principle; but few interest/power groups will let you interface with them under a name other than the one by which they have come to know you. Banks, credit institutions, vehicle registries, police, and the tax folks don't care what you call yourself, so long as you fly straight and ante up, come payout time. They have taken a dim view of alternative names since some persons have used them to escape valid burdens. If that name fails to tally with records you have created under a different name, they will want to know why; or, worse, will refuse to interface with you, in effect locking you out of the system.

And you do need to be part of the system, no matter what name you choose. To own and operate a car, insure it, marry, parent, run a business, sue someone (or, more likely, be sued)—all this becomes awkward or impossible without a name that resonates in the downtown files.

Though America requires no national identity cards in the internal-passport sense the Soviet Union or France do, identity cards by any other name are a fact of life just to stay out of jail. If the Authorities stop you on

the street and ask for "ID" and you don't materialize the right plastic, they can impound you without further cause, on the presumption that you are a wanted criminal. So, for all intents, possession of some form of bonded identity card is a must to travel freely in this free land of ours.

But conditions may arise that make it foolish to retain your link with a certain name. A legal change of name will do for some situations, gigs that don't make it profitable to track you down. For others you will have to get new, valid ID under a name that liberates you utterly from a bad past.

This need for freedom spawned an underground in the techniques of obtaining new ID. Its seamy reputation may have arisen in part from early connections with domestic freak/hippie/drug/terror groups. At least 4 established and authoritative books detail the technique of getting new, valid ID—and it must be valid, the real thing, issued by the proper government agency. It's the only kind that will stand scrutiny. ID nowadays always tags to several computer files. If the number on your identity card doesn't beep the right bell on the computer, it means a trip downtown for questioning.

NEW ID BY MAIL?

The fake-ID mailorder business must be making money, but the product fools only those who purchase it. Nobody in a position to ask for ID is likely to buy fake plastic as genuine. Attempting to fake a driver's license or state-issued ID is good for an automatic bust that your attorney will plea-bargain guilty as a means to keep you from doing a stretch, at least if you have a clean record going in and the DA is in a tender mood....

The only ID worth having is that which will withstand the type of scrutiny it is designed to protect you against. Not only must it appear physically impeccable, replete with the laser grating or hologram that shows up under the light or whatever, but your name, address, and license number must come up on the central screen when they run a make on you. The only way to get one with your name and picture on it is to have a genuine false name under which to get it.

The new-identity business has legitimate uses in a moral sense, if not a legal one. This society thrusts unjust obligations on men and women as a matter of course. Male victims of divorce actions that leave the wife 90 percent of assets and half his income have reasonable complaint and should suffer no pangs at skipping out. Likewise, having to support kids one never gets to see may be a bit much. And what about ladies who have been around the track too often and wish to marry up, so to speak, but who cannot otherwise escape a bad rep? No, when burdens passeth the point of human understanding, it becomes no sin to leave them behind.

It seems, in these grim times, that most grammar-schoolers in certain hip/felonious sections of the country know how to get false ID.

Many areas now cross reference birth and death info. The lack of a connection between those two once formed the basis for assuming the identity of someone born about the time you were, but who died early in childhood, preferably in another county and preferably in another state. With that avenue now blocked, more sophisticated ruses are required.

People looking for you in a serious way know all about false ID, as well as means to backtrack it. If you got your false ID in a neighboring county then skipped out on a million-dollar obligation you could, in fact, have paid (nobody will bother if you cannot pay), the investigator will concentrate his efforts close to home and find you quickly. On the other hand, if you had the foresight to get your ID in a state in which you have never resided, and saved it for just the right situation, you may be very difficult to find.

RULES

Before closing in for the kill, a scene at which you must present yourself for inspection by some career civil servant, gear up for the event. Attention to detail will save some embarrassing and potentially costly gaffes.

1. Dress the part. Wear neat, inconspicuous clothing. A modest wristwatch and medium-priced pen, rather than a ten-cent throwaway. Men should wear ties and be clean-shaven and generally neat in appearance. A

recent haircut would not hurt if you lean toward the long-haired-weirdo-hippie-freak cult. Shined shoes. Women should not look like off-duty whores. A dress or fashionable slacks, understated makeup, no stick-on nails. In short, do not look like a "criminal type" on the make for new ID.

2. Act the part. Be polite, soft-spoken. Remain calm no matter what happens. That includes long waits for which bureaucracies are rightly famous.

3. Procure "supportive documents" in advance. Bogus SS card, insurance card, blood donor card (give blood and do it under a false name; who would dare challenge a goddamn blood donor...?). Documents should not look fresh, obviously. Monogrammed wallet, shirt; wedding ring if your cover calls for you to be married, pictures of pets, kids, etc.

4. Have on your person enough cash for bail and have memorized your attorney's phone number, both home and office, just in case something genuinely ugly goes down....

5. Park your car well away from the facility, where it will not be tagged if left overnight. In fact, you might take a cab to the facility. If the authorities get called, the quickest way to tie you to another name is simply to run a make on your vehicle plate number.

6. If you anticipate being asked for a cover story as to place of employment and so forth, have it down pat before you go in. If you are to be asked for a business phone number, memorize it. The best number will be an unlisted one belonging to a trusted comrade who will answer with "Acme Transistor Company. May I help you?" and will praise you as one of their most talented design engineers.

7. If they don't buy your pitch, calmly leave the premises with whatever documents you brought with you. Hundreds of other places are waiting for you.

Major cities harbor large criminal populations, many of whose members seek new ID. For that reason, their ID-related bureaus are likely to be hip to ruses that succeed with no trouble out in Sparse County. So don't make a trip to the big city because you live in a small town.

OPTIONS FOR VIRGINS

The lord of one of America's grandest credit data banks reportedly opined that every American should be given a permanent personal identity number. Until that comes to pass, options remain. Those who have not yet established a paper trail might invoke options that compartmentalize aspects of one's life. For example, when starting with a clean slate, obtain as many credit instruments as possible, but use different names, addresses, social security numbers, dates of birth, occupations, and so on. The genuinely far-sighted operative will establish accounts at different banks in different towns (you have heard of gossip, no?) to enhance the separation. In this way, damage to one identity will not taint the others—or their credit profiles.

When paying bills remember that they note your bank account number. Whatever you told the bank about yourself, the creditor knows. Whatever you told the creditor about yourself, the bank knows. Both get suspicious when facts fail to jibe. Paying by money order puts added distance between you and the snoopers.

It is foolish to let on about your system—to anyone. (Especially your new bride. You will dump her, or she you, within 10 years. A jilted spouse blabs everything to the most damaging ears.)

Post office boxes offer some insulation, but beware the hazards. In small towns the nature of your mail will shortly become common knowledge. And anytime the feds want to know all, the postal service will hand them your mail before passing it to you. The post office denies all responsibility in these cases. The guys who get the mail open it. The post office maintains credible deniability....

Another vital point is, even after you get new ID, pay taxes. Normal people do it, and no agency is willing to put more manpower on your trail, and has the muscle to tap otherwise sealed sources, to collect on a penny-ante tax-evader than the IRS. It does not care about your new name and lifestyle, as long as it gets its cut of your take. (Beware the fact that the IRS files are open to the Justice Department.) Call it cheap

insurance, as well as the patriotic thing to do, at least for those unfamiliar with Senator Fullbright's Golden Fleece file.

What is good ID worth in the wrong situation? Ask a survivor of Germany in the thirties what he would have given for the proper set of papers when the roundup squad swept through town. "Your papers are in order, Mein Herr. You may board the ship. Have a pleasant voyage to America." And as Frank assured us on the Mothers' first LP, it sure can't happen here....

MAIL DROPS

A mail drop is an address other than your own which will receive letters and parcels on your behalf, then forward them to you. Most will also post letters and such for you, so that they bear a postmark of a town other than yours.

Using mail drops for genuinely touchy business may not be wise. There are just too many ways to trace it. First of all, every private eye and police agency in the country keeps a list of mail drops and receiving/forwarding services. They simply punch in the address and run a search of their database, and up it pops that "your" address is a mail drop. From there, all they have to do is present a subpoena, or warrant, which in the case of the more aggressive PIs may be totally bogus, and the service will hand over a complete record of all your mail transactions. ("Would you tell us, Ma'am, where the packages came from that you forwarded to the subject?" "Yessir. They were from 'Gay Stallion Films' in Covina, California." "Thank you for your cooperation, Ma'am.") At the trial, that tidbit will discredit you utterly in the eyes of the jury—and that is exactly how the game works nowadays.

Conduct your affairs in anticipation of a hostile future probe. Using aliases, mail drops, semi-anonymous money orders, and so on can help. But be aware of their limitations in the face of a truly determined investigation.

Most of this can be garnered from fiction sources (The Day of the Jackal) and a library of new-ID books that have seen print since the early seventies. In fact, 1971's Paper Trip I remains in print as this book comes out.

SOCIAL SECURITY NUMBERS: THE BASICS

The scene is a job interview. The interviewer riffles off a series of seemingly harmless questions, then pops "What is your social security number?"

Wellsir, there is much more to ad libbing an SSN than choosing 3-2-4 digits at random, at least if they are to blend with the rest of your cover.

Those who wish to fabricate an SSN for whatever reason have to understand features which the informed can spot instantly as queer. The number tells the state of birth of the holder. If your employment application says you were born in Nevada, and the SSN you give comes from North Carolina, well, it puts the personnel manager hip to your ruse.

Federal law demands that you give your SSN when filing tax returns, but, at least on the surface, IRS seems stingy about giving that number out. But it has been known to use it to track down special categories of misfits. For example, fathers (it's always the father....) who fail to pay child support. It was reported that a female employee of a section of the government with access to the SSN computer was jailed for tracking down a man based on his SSN. The reason? He had made the Mafia's hit list. It used his SSN to track him down, then waxed him. That's one way they find you, and one reason the federal witness protection program assigns new SSNs (the film, F/X, suggested that they gave them out sequentially, rather than randomly, a seemingly stupid move one hopes does not mirror real life).

A working knowledge of states and their corresponding SSNs will serve well when it comes to coughing up one that jibes with the state of birth you just gave the employment officer. Since so many other texts have printed the data, our wisdom simply advises memorizing what three-digit prefixes tag what states.

CREDIT

Some spook texts devote chunks of space to means to establish credit or patch wounded credit. Readers who seek those ends find that information invaluable. But those who have yet to interface with the system in a serious way might choose the ounce of prevention to awful pounds of cure: DON'T USE CREDIT.

Pathetic credit junkies—the author has been there—might laugh aloud at that insane advice, yet it springs as a sensible offshoot of credit and its terrible ills. Credit encircles too many aspects of your personal life. It digs a permanent hole, becomes part of your identity profile. Once established, it defines your scope of action, pegs your place in society—which might be OK if all credit info were accurate. Sadly, it isn't. For that reason, consider these options:

1. Never reveal your correct social security number to anyone except the IRS and other agencies empowered by law to know it. Warnings on credit card applications that giving false information is a crime hold true if you give bad info as a prelude to fraud. As long as you pay, prosecution probably won't enter the picture.

2. Never reveal your correct date of birth to any agency not empowered by law to know it. Ditto the comments above re: SSNs.

3. Avoid forming a self-trapping matrix by using different SSNs, DOBs, names, and other personal information when getting phone service, buying electricity or cable TV service. Nothing illegal curses this as long as you do not commit fraud or intend to commit fraud or other crime. Pay your bills and nobody cares. Be aware that a single bit of info revealed to two sources can trash the entire scheme, simply because certain data is supposed to be unique to an individual, such as the SSN or a phone number. If two people give the same phone number, and neither has a roommate, one of them is lying. Computers look for these cross-links.

4. Choose one identity for the IRS and stick to it. The same holds for your driver's license, the name under which you keep a phone, and so forth.

5. Meet all financial obligations promptly.

6. Establish bank accounts under different identities and use checks that fit the scene.

7. Pay by anonymous money order when needed.

8. Do obtain at least one major credit card, unless you are prepared to live with the inconvenience of never being able to rent a car. (Alternatively, you may apply to a car-rental company to become "cash qualified," which subjects you to exactly the type of credit check as applying for a card; if you have created the proper paper person, "his" credit should check good.)

9. When confronted with forms to fill in, always give misleading or incomplete information, except where doing so violates law (with private concerns that chance approaches nil).

10. Do not fall into the credit trap. Live beneath your means. Want a new car? Save until you can pay cash. You'll get a sweeter deal and save interest payments, in addition to eliminating the credit issue altogether.

11. Anticipate hassles because you lack a credit history. Those who apply to live in apartments routinely get run through Retail Credit, Inc., or a similar databank. No record can close as many doors as a bad one. Be prepared to offer, say, 6 months' rent in cash in advance as the levy of being an unknown.

12. Decide your priorities before you enter any situation that may demand release of personal data. If you may be denied rental, decide beforehand whether you will put up with the hassle of living elsewhere, or surrender and reveal all that personal data needed for the credit check.

CONSUMER INFORMATION REPORTS

Consumer Information reports magically transform bums, geeks, and winos into irrefutable sources whose pronouncements become final.

The CI industry has created a job—and a huge income—for itself by fostering the notion that its reports are necessary, desirable, and reliable. As to reliability, fantasize this:

You apply for a job with a company that routinely obtains pre-employment consumer investigative reports. The agency asks you for the names of everyone on your street, at least 2 houses down. Then it chooses one at random to interview. It invites that person in to be interviewed about you:

Q What do you think of Mr. Walsh?
A He seems odd to me. He comes and goes at such strange hours.
Q Have you ever observed any deviant behavior on Walsh's part?
A I think he uses cocaine or marry-wanna.
Q Does he throw loud parties?
A Oh, you bet.
Q Do you believe he drinks to excess?
A He probably keeps more liquor in that house than Seagram's distillery.
Q How does he get along with his wife?
A They fight all the time. I think she's getting ready to leave him.
Q Any other evidence of domestic strife?
A His two kids are always in trouble at school.

Since this is a fantasy, pretend that the source will tell the truth about anything he is asked about himself:

Q Now, sir, if I may ask you a few questions to help establish your reliability and qualifications to serve as a witness in the case of Mr. Walsh?
A Of course.
Q Fine. Have you checked to see whether his job might demand that he keep odd hours?
A No.
Q When was the last loud party Mr. Walsh threw?
A I can't recall.
Q On what do you base your impression that Mrs. Walsh is about to decamp?
A Huh?
Q Let's try another question. Have you personally viewed the vast stores of booze you stated Mr. Walsh kept?
A No.
Q Have you personally observed him to be drunk or to use illegal drugs?
A No.
Q Have you, yourself, ever been drunk?
A I'm an alcoholic, but I've cut back to a half-pint a day.
Q Where are you currently employed?
A I was fired six months ago for habitual drunkenness on the job.
Q What is—er, was—your line of work?
A I was an engineer on a railroad that hauls toxic waste and nerve gas weapons.
Q Have you, yourself, had any trouble with the law?
A I'm on parole for embezzlement.
Q Thank you, Mr. Vagabonde. That will be all. I'll have your comments about Mr. Walsh typed up for you to proofread before they become part of his permanent file....

The scene is prima facie absurd; not what the witness said about the subject of the investigation. Other works have documented that such comments are all too common. What's absurd is the investigator making the vaguest attempt to establish the reliability of the witness, or his moral right to judge another person, prior to embalming his comments about a defenseless third party.

Exaggeration has a point. What happens in this scenario is exactly what the information bureau and those

who use it are doing, only they insist upon fooling themselves and the public about it (they fooled Congress, or perhaps lobbied it into abject submission, when they gilded the Fair Credit Reporting Act heavily enough to counterbalance the idea of fair play).

LOW PROFILE

Several authorities in this field of privacy feel that one of the most effective means of shielding one's personal life from scrutiny is not to do things that trigger a probe. For example, flaunting the symbols of success, living in a neighborhood where the guest houses start at $60,000, flashing one of the golden credit cards, and so on make others give you that second look that whets the appetite to know more. Now, be frank in admitting that symbols serve that very end in this symbol-oriented society. Keeping a low profile may fail to draw the caliber of mate you've set your sights on, for example.

Make a choice: you have seen how much of your existence can be an open book to those with nothing more than the desire to know. Erasing that desire wraps another layer of insulation between you and loss of privacy. But if those symbols are a part of your scene, necessary for some social strata, then accept their burdens...but keep some things private.

SAFE DEPOSIT BOXES

...aren't safe from bank burglaries, open to just about any agency, especially the IRS, with nothing more than administrative authorization. This means looking hard at alternative caches for those truly personal documents—your alternative ID—and computer files (encrypted, then copied onto bulk-erased and freshly formatted diskettes, with the decoding programs and passwords securely stored elsewhere; do have the presence of mind to rename files that might otherwise give you away; change FRAUD.TAX to, say, GAME1.BAS).

Be aware that the bank creates a record every time you access the box, and that this record could prove damning. If you were served papers suing you for ten million dollars, and the next day went to your safe deposit box, then lost the suit to the tune of the full amount, you will have a hard time convincing the judge that you did not remove assets from the box that the court would otherwise have attached to pay your monumental if mundane judgment.

In the heyday of the survival cult, the notion of burying one's goods became hip. Several texts gave advice on the mechanics involved, mostly relating to sealing 4" PVC pipe correctly and including a packet of desiccator to keep the stuff dry, how to avoid metal detectors, and so on. Dunno. Seems like creative use of above-ground locales, with their instant-access feature, offer the more flexible choice in these changing times.

DATABASES & DATASORTS: DAT'S AWRIGHT....

To use a well known firm as an example, take Radio Shack. Notice the mechanics of buying at that fine chain of stores. The salesperson writes each part-number on the sales slip, and almost always asks for your name and address. And if you pay by credit card, your own, you can hang it up...banish all fantasies of privacy.

Now, why do Radio Shack and hundreds of other companies gather this information?

1) Inventory control. It tells them daily, even hourly, what products move and what they need to jettison. 2) Buying patterns in response to ad campaigns, sales, and the like. 3) Names of buyers offer added value in that mailing list companies want them. Not just that, but matching the name with the product(s) bought offers greater worth. Many advertisers pay extra to reach persons who regularly buy high-ticket items at Radio Shack, or any other store.

But what if a party wanted to know the names and addresses and any other info of any person anywhere in the land who had bought the parts, or most of them, that suggested he was building bugging gear? Big Brother is no stranger to what goes on in the private sector. He might tap into Tandy's main computer without Tandy's permission or knowledge, and ask it who had bought, within a space of a day or a year, the

parts to make, say, a phone-tap FM transmitter. Or the voice scrambler whose plans appeared in Radio Electronics. Would your name surface along with the other dissidents tagged for surveillance?

COUNTERMEASURES

When you buy materials from which the wrong—or right—inferences could be made, automatically, arbitrarily, and at the flip of a switch, doesn't it make sense to throw up a bit of a screen? Buy some parts at one store, the rest at another, order the remainder through the mails, all under different names and addresses. (But even here we hit snags. The government's computer contains every telephone number, voter registration, address, social security number, date of birth, and name in the land. The program can be told to zero in on alias-users—buyers whose names fail to match with known local names, people whose names and addresses do not appear in the phone book, or which do not match with real names and addresses, and so forth.)

* * *

COMPUTERS REVISITED

One fascinating revelation—perhaps we should pull up short and call it an inference—arising from the hydrogen bomb story held that work hung up almost two years out of physicists' hopeless belief that it would take that long to solve mathematical equations involved, a necessary prelude to building a device costing millions of dollars. In those days that meant money.

The hydrogen bomb ushered in a leap of destructive power that paralleled the jump in information-handling power afforded by the personal computer. Though modern-day nuke designers still rely on supercomputers, or at least a VAX, how long in theory would it take to repeat those 1950 H-bomb equations on a desktop machine running an Intel 80386 and its 80387 math coprocessor? A day? An hour? Mere seconds?

The information has always been there, patiently awaiting those with the time and temperament to unearth it, collate it, and synthesize something from it. More than anything else, the personal computer can let the average citizen of the Western Bloc access it, manipulate it, control it, harness it. The computer has proven to be the proverbial lever long enough to move the Earth.

The government and big private concerns have held such vast power because of computers. They alone could pay to maintain instantly accessible files on literally anyone.

But that's changed. Trouble is, the populace has yet to make a unified, organized effort to keep tabs on the government the way it does on you and—ulp—me.

Right now, there exist desktop computer systems capable of maintaining files on every elected representative, for example (let's start with that singular breed). Want to see Senator Bullmoose's voting record on screen in graphic form for his entire career? Punch a few keys and up it pops. Compare it with a graph of his campaign contributions and their sources, then ask for a correlation. Hmmm. The big blip from RipOff Cigarettes coincided with his No-votes to cut tobacco subsidies.... Want to know who's registered to lobby for whom in Washington? Again, it should be at your fingertips. Party-attendance, guest lists, public bank balances, the percentage of IRS screw-ups compared with taxpayer screwups. Commercial software that leans in this direction surfaced in the summer of 1988. "Congressional Toolkit" from B. J. Toolkit (Croton-On-Hudson, NY) offers a database of sorts on Congress, along with the power to generate form-letters for mass mailings. The company sells also databases on selected state governments.

When they first became available to personal computer users, Winchester hard disks that held a helpless 5 megabytes sold at about a thousand dollars a meg. Today the entry-level norm has pushed past 20 to 30 meg, with one company upping the ante to 60 meg, this on a sluggish XT-class machine. The 80286 and 80386 machines take hundreds of megabytes of storage in stride, along with the ability to manage megabytes of random access memory (RAM). The optical storage disk effectively places unlimited desktop mass storage in the hands of anyone who owns a personal computer. That should lead to—

THE PEOPLE'S DATABASE

Any phrase containing "the people's" usually means that Karl Marx, Nick Lenin, and Jane Fonda endorse it. Let's be straight and say that, with due regard to those legendary freedom-fighters—whatever that vague phrase means—"the people" as a concept belongs neither to the left nor the right. Rather, it distinguishes the general population from its government and from non-governmental groups that exercise power not accessible to the average citizen. Of all elements that define these several groups, the one that has proven decisive over the years is the ability to store and retrieve information about other persons.

That power now lies within the grasp of "the people," and they couldn't act more oblivious to it.

Truly powerful private databases would of necessity have to restrict access by those they profiled: police, politicians, lawyers, businesses, private investigators, etc. Only the little guy and his family could join the club.

Easier said than done. Once the system proved itself in a handful of cases, the reigning powers would plant moles in the system, pass restrictive laws—even sabotage would follow.

The "underground" concept holds nothing, for not only does that breed dwell powerless, except as to annoyance value, but its outcast status makes it easy prey for all marauders. No one will come to its rescue in the event of a "crackdown." The easiest method has been a civil suit. Simply defending a suit costs hundreds of thousands of dollars. No insurance exists to cover this twilight-zone sort of activity. When faced with a suit, they would usually forfeit or lose, or capitulate by dismantling their data network.

Describing the mechanics of intelligence-gathering, retrieval, and storage is easy. Implementing it in ways that achieve the desired clout won't be.

Present computer bulletin boards allow dialog, which is fine if you wish to hash over obscure and mundane dreck. Start talking about deeds that muscle in on Big Brother, private or governmental, and watch how quickly the feds show up to confiscate your computer—and you.

At a minimum, these subjects need to be in the public database:

The media.
Local IRS contingent; most info about auditors, supervisors.
IRS errors and resultant damage to taxpayers.
Nearest FBI contingent.
Local police records of disciplinary action, unnecessary use of force, officers' history of alcoholism, etc.
Location of speed traps, etc.
Local politicians.
State legislators.
Employees of local offices of credit agencies ('specially those lovable field-reps).
Local private investigators.
The Phone Company, in whatever guise.
Editorial staffs of local newspapers—with whom are they chummy?
Apartment complex managers.
Apartment complex owners.
Lawyers.
The Consumer Product Safety Commission.
Physicians.
Insurance brokers.
List of who has sued whom, why, for how much, who won.
Local district attorney.
Judges (start with all who have handled scrapes of the Kennedy clan).
The Bureau of Alcohol, Tobacco, and Firearms.
Powerful, i.e., wealthy, people who have shown an interest in shaping local policy, whether it be zoning, taxes, easements, water and sewer, etc.

Use optical scanners to input data from books such as the phone directory (the computer should be able to generate its own reverse phone directory). Some sources may be willing to cooperate and put the data on optical disks or rent it via modem. (The phone company will monitor these data transfers; better go back and move the phone company and its policy makers to the top of the surveillance list....)

One of the most important systems would be a "counter-credit" computer file: a file that held mistakes contained in credit or consumer files, one that devoted its space to the subject's side of things. Create a file on merchants and so on who gave this info consideration and those who did not. Boycott those who did not. Note the potential for blacklisting employers, apartment complex managers, and others who abused credit/consumer investigative reports.

Learn whom the FBI had investigated, its findings, and to whom it had released them.

Use computers to automate requests for info under FOIA.

A great deal of work for an individual. It would take a network to assemble this. We have to start someplace.

Wouldn't it feel great, being able to run a "make" on the creeps who just yesterday put you through a degrading credit check that got your name right but missed the part about that civil suit being settled in your favor?

How do you dig out dirt on these people and agencies? Check the references at the end of the book. There is no point to reprinting investigative technique; it's last week's news. Observation, bugging, running down license plates, staking out the residence, checking on the deed—it's all an open book. The point underscores the power of massed data instantly on tap.

It's been said that the personal computer is a tool of capitalism. True, but one that will never reach its potential without an organized effort on the part of citizens to stand up for their rights, or make their own.

Wouldn't terrorists and criminal types like to get their filthy hands on this data? Yes. And for that reason we do have to keep certain aspects of government and enforcement off limits, both for society's benefit and to protect the lives of our legitimate operatives. But clearly the days of impunity from investigation simply because a man or woman totes a badge or wears a uniform are over.

Hookup networks present a gilded opportunity for B.B. to tune in on you, unless you use a genuinely difficult encryption algorithm. And, despite what you have heard, despite what the NSA says you cannot do, it is possible to maintain relative privacy with the right encryption; but don't think those encoded bits will remain secret forever. The NSA stores them, and as computers evolve, will decode them.

Picture one scenario: you have been tooling along at a comfy 35 when an urgent blue light starts to pulse in the rear-view mirror. The heat wants you for something. Submissively, you pull over.

"May I see your license and registration, sir?" asks the patrolman, as he burns his 35,000 candle-power sealed-beam flashlight straight in your face.

"Certainly, Officer. And may I have your name and badge number?"

"Yes, sir. My name's Friday—Moe Friday. Badge number 714."

"Thank you."

While he puts in a call on your license and registration, you put in a call to the civilian database on him: Has this cop ever been charged with use of excessive force? What does his psych profile say he usually stops people for? Does he use radar? Is he qualified to use it? When was his last radar refresher? Is he prone to jolt you with his shock-stunner for mouthing off? A psycho, perhaps, to pull his piece and wave it for show?

Just as the officer has a legitimate interest in knowing whether a speeder or bad driver has outstanding warrants or a history of DUI, so civilians maintain rightful interest in the officer's past behavior.

Stop and look at the concept of Special Privileges and the reasoning behind it. We empower select members of society with rights and authority denied the rest, ostensibly to serve the common good. In the case of police, we have given them power to arrest, to carry firearms, to have their commands obeyed under penalty of incarceration (disobeying a police officer). As a given, courts take the word of a police officer over that of the unsworn citizen if it comes to a trial.

It just makes sense to subject those with this terrible and discretionary leeway to tighter surveillance as the price of expanded powers. True, they already undergo semi-probing background checks just to get their jobs; but these checks and the results are conducted and held largely in-house. Better to get some of it out where all can see it.

J. Edgar Hoover's stint at the helm of the FBI left us with a grim legacy of illegal government snooping unequaled in modern times. And it became common knowledge that intelligence units of many police departments bugged premises and phone lines without authorization. But who's to say it isn't still going on? Get lists of the agents, make their personnel files public knowledge. It's a reasonable price for special privileges.

Re-reading those artless words evokes a dreadful sense of naivete. A unified "people's database" could snag on regional, factional, racial, economic, and political differences. Each social stratum must have its own idea of what a non-governmental database should be and how it should be used. Cooperation vital to an effective setup might not materialize. Pipe dreams....

* * *

DESKTOP PUBLISHING AND ITS IMPLICATIONS FOR FALSE DOCUMENTS

Personal computers can design fake birth certificates that, if printed on a phototypesetter, will fool anyone because a photocopy would look as if it had been minted from the real thing. The same design fed through a laser printer easily betrays itself as phony because of the low resolution of current lasers, about 300 dots per inch.

But times change. Rumors of 650 dpi laser printers for consumers are circulating already. We expect the evolution of printing technology to shave the gap between laser printers and true phototypesetters, with their 3000 dpi resolution. They should be available to anyone with a computer soon. What an irony that the coming flood of fake documents will undermine the Authorities' faith in paper, edging us further toward a completely digitized society and negating a newfound power to produce genuine-looking papers.

* * *

LIPSTICK...AND OTHER TRACES

Fingerprints and tire tracks are macrotraces: visible to the naked eye, and so obvious that all but the most amateurish felon obscures them or avoids leaving them. But forensic science has identified a wealth of trails that are not obvious when they get left. These microtraces and the fresh generation of of lab apparatus that detects them have opened up a world of new and reliable sources of evidence.

Forensic science's power to identify even microscopic traces of material or flesh and match it with samples gathered later amazes no one so much as those who have gone to the big house because they overlooked that flaw in their plans. Recently, forensics began talking about extracting the DNA (deoxyribonucleic acid) from a tiny piece of skin to match it with that of the perpetrator as surely as a fingerprint. That means that, if they found the spot from which a sniper cooled his target, they would also be able to recover microscopic

traces of shed skin (you shed skin all the time, but don't see most of it). A trip to the lab, and a sample of your own (which they can get from the carpet in the motel room you rented for the job) and you are as good as convicted.

* * *

ALARMS & RELATED LORE

Forewarned is forearmed, and from that simple maxim sprung the alarm trade. Alarms possess three key elements: 1) sensors, 2) the control station, and 3) the "means of notification."

SENSORS

"Captain, sensors indicate...."

So began Mr. Spock's report to the Captain of the USS Enterprise, whose five-year mission never seemed to plunge it into back-streets and alleys of burglar country where most Americans live and work.

Intrusion alarms must possess means of sensing the intruder, and so they do. A dazzling array of sensors, from mundane to outlandish, have evolved in parallel with security needs. To understand a sensor is to grasp its strengths and limitations, whether your end be to defeat it or trust your valuables or your life to it.

MAGNETIC CONTACTS

One of the oldest, most durable and reliable sensors is the magnetic contact. In its commonest form, it is a magnetic switch—one whose on/off state is determined by the presence of a nearby magnetic field—and a small magnet to supply that field. The nearness of the magnet can either open or close the switch connected to an alarm circuit. Switches open in the presence of a field are said to be "NO" or "normally open." Those normally closed are said to be "NC."

Most magnetic switches are visible and easily bypassed, assuming the burglar/intruder knows whether they are open or closed. Since most are NC, a wire clipped across the exposed terminals will bypass them. Despite these drawbacks, magnetic switches are cost-effective, durable, resistant to false alarms if installed properly, and deter all but determined vermin.

The hidden ones can be detected often with a good compass. The photo shows that even the compass out of a Cracker-Jack box will detect the typical alarm sensor magnet from 5 inches. Pros doing serious work use a magnetometer....

But sometimes it isn't practical to bypass with clips. Perhaps the window is guarded with foil or a shatter sensor. Some switches have been defeated by a strong, externally applied magnetic field. Where to get a magnet to supply that field? Expensive woofers often use ceramic magnets weighing 60 ounces or more. Edmund Scientific and several industrial supply houses also sell big magnets. Now, as to how to orient the magnet. This ploy has been mentioned, but the author has not seen specific instructions given as to proximity, polarity, and so forth. As a rule, you want the second magnet to take the place of the first as its holder is jimmied away. This may be a two-felon job.

The author used the 60-ounce magnet, part of an 11-pound structure, from a Gold Sound model 1260 woofer and a set of normally closed magnetic contacts to test distance over which the big magnet could keep the switch closed. The results were unimpressive, perhaps out of the circular shape of the field produced by the platter-like magnet. The cheap compass followed the field at a distance of 3 feet, give or take.

Clearly, those who would use magnets in this fashion need to do careful advance work: know whether the switch is NO/NC, its location, material used in door, then buy the stuff and do a dry run. Like picking locks, and before doing it for serious stakes (like three to five in the pen) you must know all the angles. An accomplice must case the place (pretend to be cleaning service; if they hire you you're in!).

The magnet fails on steel doors for obvious reasons: the iron content of steel makes it a magnetic conductor. It "captures" the magnetic flux and makes it flow along the lines of the substance, reducing its impact at the switch. Magnetic contacts mounted on steel doors usually employ spacers or special shielding to avoid having the door neutralize them.

And, just because you made it inside doesn't mean you have made it to the boiler room. Most professional alarm installers and many do-it-yourselfers put in traps. Even they understand how easily the magnetic contact can be bypassed. For example, cut a hole in the door and walk in.

So-called high-security magnetic contacts use a pair of switches sensitive to the direction of a local magnetic field and oriented at right angles to one another. Imposition of a new magnetic filed may hold one switch, but makes the second switch open, and the jig is up.

FOIL

Foil refers to metal strips, usually lead, lacquered over exposed outside glass surfaces such that it forms part of a closed alarm loop. Window shatters, foil breaks, alarm triggers. Simple.

But foil foils mainly smash-and-grab operations. Being visible, and with the existence of glass cutters with a sharp bite, it takes little imagination to see how to defeat foil: Cut a circle out of a window where there is no foil, bypass the closed loop. In sections at which the foil must bridge a raised surface, it often requires use of screw terminals. Here a simple alligator-clip jumper will suffice.

Use of foil seems to be waning, judging from the appearance of storefront glass nowadays. It remains a durable, reliable countermeasure with deterrent potential, since burglars understand that foil is almost never installed alone, that traps inside will confound the caper.

GLASS-BREAK DETECTORS

The vulnerability of foil led to development of a sonic sensor that mounts directly to glass, particularly large expanses it would be unsightly to foil fully. It is said to be "tuned" to the frequencies of breaking glass and glass cutters.

Anyone who has used these handy gems will tell what a pain they can be. The cheap ones require connection to some manner of "pulse stretcher," since the signal sent out by the sensor itself will not trigger the alarm. Many demand sensitivity adjustment. Too much, and a passing truck calls the police. Too little, and the glass cutter goes undetected. Adjustment requires that the amateur purchase a special meter and a custom striker to simulate breaking glass, which is nothing to the professional installer who will use and depreciate the gear, but a hefty outlay for the do-it-yourselfer.

Then there is the adhesive. It doesn't last forever, and substituting your own may alter the response characteristics of the sensor.

Still, like foil, would-be burglars know window sensors when they see them. They probably do deter many B&Es.

The best protective combination for large expanses of clear material is polycarbonate, either alone and with a scratch-resistant coating, or sandwiched between layers of glass, like an automobile windshield; and fit it with alarm sensors. That way, an attempt to break in A) lets everybody know, and B) thwarts all but a prolonged attack with a saber saw.

ULTRASONIC MOTION SENSORS AND THE CURSE OF FALSE ALARMS

A train sounds its horn as it approaches. Though you know intuitively that the pitch of the horn is constant, you hear a droning scream that drops in pitch as the train hurtles past. This results from the Doppler effect. Electronic instruments can "hear" tones, both audible and inaudible to humans, as well as shifts in the pitch of those tones, like the droop in the whistle of a passing train. This forms the basis of ultrasonic intrusion sensors.

An ultrasonic sensor consists of a source of sound in the range of 25 KHz to 40 KHz. This lies above the audible range of humans since lower-pitched tones might be irritating or tip off crooks (alarms using audible tones do exist).

The second crucial element is a receiver capable of detecting a change in pitch of the tone. What would change the pitch of the reflected sound? Movement of the object it bounced off. It would show the same type of Doppler shift as a train whistle. Here the moving object is assumed to be a prowler.

The problem with ultrasonic sensors, at least the early models and even some still sold, is their proclivity to sense non-intruders. Moving air currents can set them off. Ultrasonic sound created by water heaters can do it, too. Expanses of glass rattled by gusts of wind. The list of things that move when no one is around is too long to print. Most of them have been culprits in false alarms sensed by ultrasonics.

But the principle of the system is, uh, sound, and the electronics inexpensive (indeed, the works have been reduced to a chip). Ultrasonic sensors found credibility in verification circuits made so the unit would not trip with the first, or even the second or third, pulse. This added circuitry breathed new life into an inexpensive but effective sensor, which had seemed doomed out of its shortfalls. Today's high-end ultrasonic motion detectors incorporate sophisticated discrimination circuitry that has all but eliminated false alarms, keeping the ultrasonic alarm a viable choice.

How do you know that an ultrasonic device protects the premises? Assuming you can tour the locale beforehand, simply inspect it. Most units are clearly visible, and many sport "walk lights"—LEDs that glow when the sensor trips. This will give you a reading on the sensitivity of the alarm. Without the ability to case the joint, an ultrasonic sniffer may be of use. This devices senses ultrasonics, then cuts the frequency by half to one quarter, making it clearly audible through a set of headphones. These devices are fun to play with in their own right: animals and insects use the ultrasonic band for plenty of business we known nothing of. Tuning in is like using a scanner. Information Unlimited sells plans for an ultrasonic sniffer.

MICROWAVE SENSORS: SON OF FALSE ALARMS

Microwaves are electromagnetic radiation, but the behavior of this energy conforms in many ways to that of sound, and we can harness those properties to give us indication of movement. Police radar is the most widely known application. As with ultrasonics, it's the change in pitch of reflected microwaves that provides the indication of movement and speed.

Microwaves exhibit special properties. They bounce off metallic objects; but water, as in water contained in the human body, absorbs them. They pass through most non-metallic, dry materials, such as wood and plastics. Thus, a human body moving in a microwave field can alter the returning waves either by soaking them up, or by reflecting them off metallic objects carried or worn on the person.

A basic microwave sensor consists of a transmitter and a receiver, just as with the ultrasonic detector. The receiver is made to detect changes in the quantity of reflected energy, rate of change, or to employ the Doppler effect to discern movement.

The advantages of microwave sensors are high sensitivity, the ability to cover vast spaces, both open and enclosed, with a single sensor.

But microwave sensors suffer problems which have proven among the most vexing in the alarm trade. First, though absorbed by water and reflected by metal, they pass unimpeded through wood and many plastics, which means that the microwave sensor will pick up not just the felon in the office, but the rats in the walls and the dog trotting by outside the office, or the pedestrians and cars parading innocently past.

Remember that water absorbs microwave energy, and that much modern plumbing consists of microwave-transparent plastic. Flushing the commode on the fifth floor can trip the alarm down in the lobby because plastic pipe runs in the walls.

Beyond that, microwave sensors may be set off by radio interference from other sources, such as microwave ovens and deadly police radar—even radar emissions given off by some extremely cheap brands of radar detectors.

With all these drawbacks, there are still situations for which microwave sensors offer the most sensitive, reliable, and cost-effective coverage. Outdoor alarms covering thousands of feet, consisting of a transmitter at one end, receiver at the other. Police radar detectors may pick this up and warn us of the threat.

And as with ultrasonic motion sensors, microwave has been mated successfully with circuitry to screen out false alarms.

INFRARED SENSORS

Formerly one of the most exotic and expensive alarm technologies, infrared has surfaced on the shelf at your local discount house at a fraction of the price it commanded 10 years ago.

Infrared refers to electromagnetic energy whose frequency places it in the range of heat, as in heat of the human body compared with its surroundings. Infrared alarms employ two configurations, active and passive.

The active type is easy to figure out based on knowledge of ultrasonic and microwave units. One unit sends out infrared signals, a sensor detects direct or reflected energy. The combined gimmick works by sensing changes in the pattern received. The simplest is a full interruption, as with a single beam sent down a hallway or across a doorway. A body passing through would disrupt it fully. This crude type of circuit has been used with visible light as well, often as an "announcer" placed in front of the door in stores. The whole works—transmitter and receiver—can be had on a single chip.

More sophisticated devices add nuances to the pattern, and may detect changes short of interruption, a la microwave.

IR viewers and night-vision goggles can see IR beams, though not as spectacularly as portrayed in the movies.

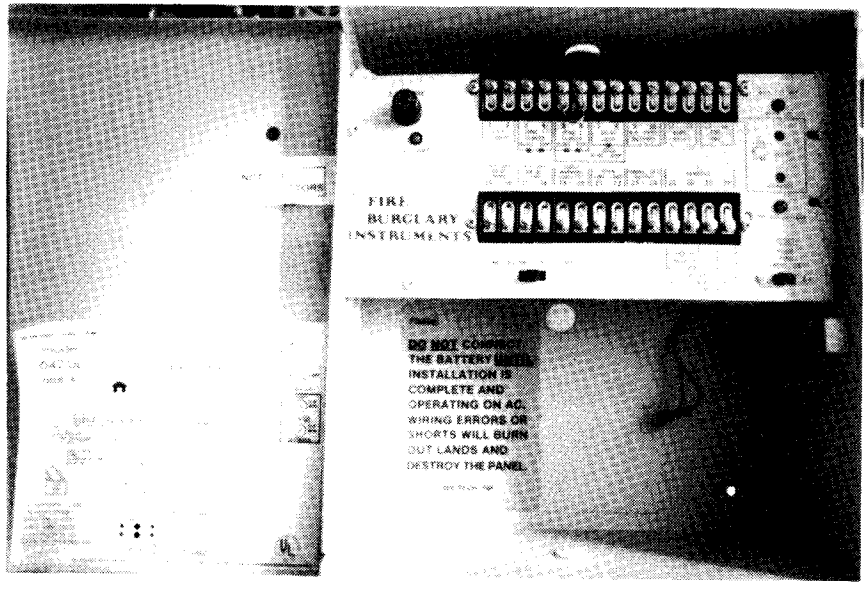
Passive infrared sensors adapt to the existing background infrared radiation, then detect changes in it produced by the shielding effect of a moving body, as well as heat from the body itself.

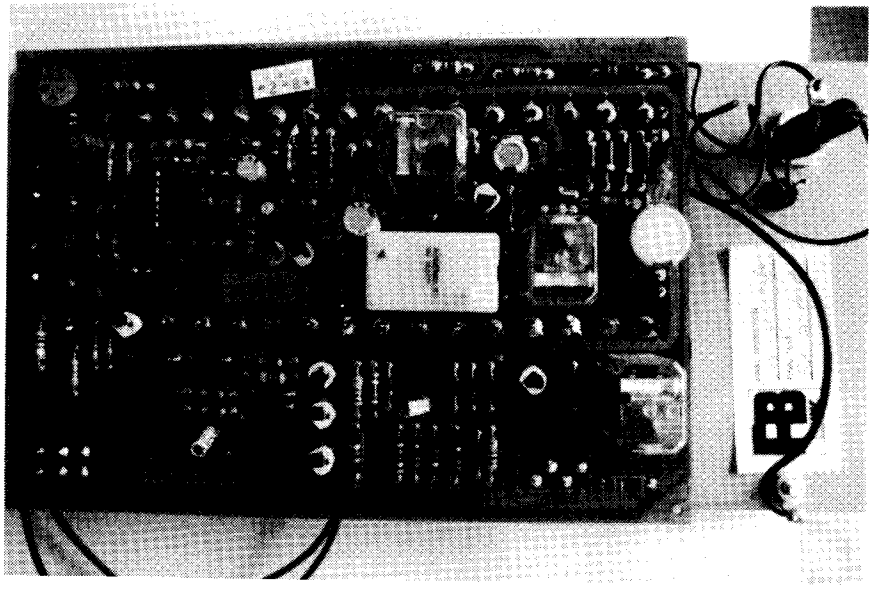
Early infrared devices had their share of false alarms. Many were too sensitive, so that the beam of headlights shining through the window could trip them; or movement of the walls caused by a passing truck, the changes in temperature produced by heating and cooling systems. And as electronic devices, some found themselves triggered by two-way radios and other sources of stray energy.

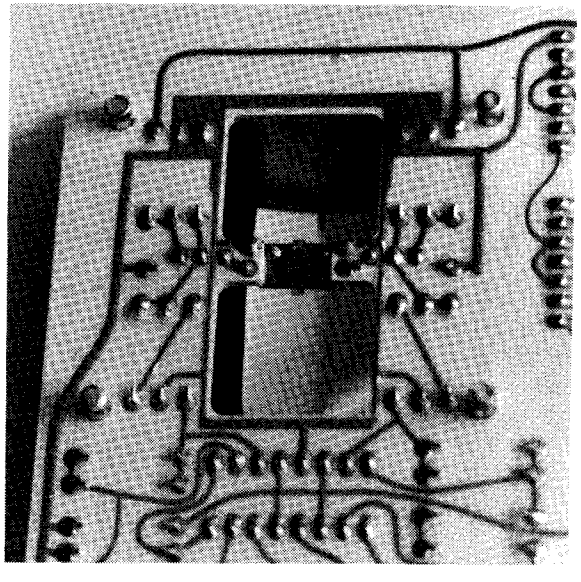
But the devices which have been around since the late 1970s cut up the sensor field of each unit into multiple adjacent zones. They include circuitry—sort of a built-in verifier—that require two adjacent zones to fire in succession within a set period or the sensor will not trigger.

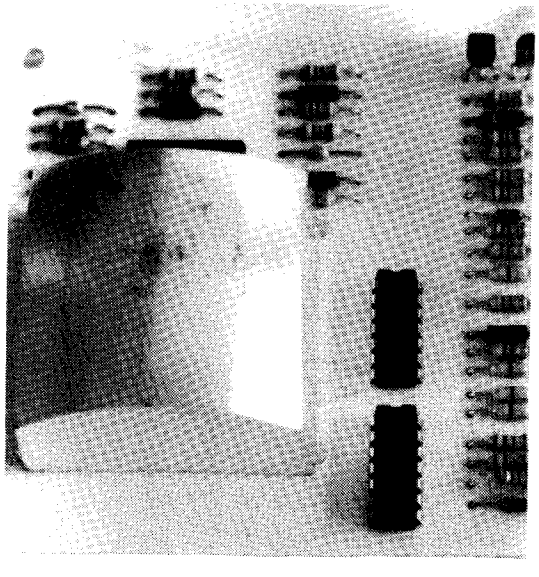
Ultrasonic, microwave, and infrared sensors require power. That usually means another pair of wires going to each sensor, and explains why most users of these sensors were institutional, at least until recently. Some passive infrared sensors use built-in, long-shelf-life lithium batteries as the sole power source, with a claimed active life of more than ten years. The author has used this type of sensor in an office and found it reliable and resistant to false alarm. Initial cost was high: $40 per single-zone sensor, $60 per multiple zone sensor (1984); but the cost and trouble savings of not having to wire external power to each sensor more than made up for this cost (which fell short of other IR sensors in any case....).

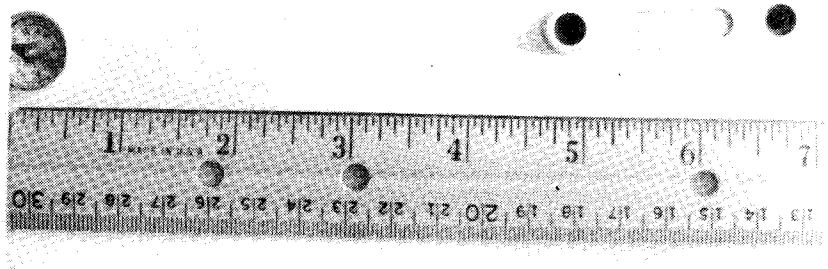
Just for kicks, the author sought to defeat his own alarm. Instructions that come with the IR units told to set the sensors at face-height, since the face is usually warmer than the rest of the body. He found that he could defeat the alarm by crawling, which took him out of its sensor zone, or by walking v-e-r-y s-l-o-w-l-y, since the device would not trip unless two adjacent sensor zones triggered in succession and within a set period. Do not rely on IR alone. A sturdy combination consists of magnetic sensors, IR, and internal traps, such as pressure sensors under the carpet, proximity sensors, and so forth.











TOP LEFT: Inside a common alarm control box. TOP RIGHT: Panel itself uses electronics that date to the early seventies. BOTTOM LEFT: multi-zone self-powered passive infrared sensor w/cover removed. BOTTOM CENTER: Back of same unit, illustrating use of reflector to let one IR sensor-pair cover multiple zones. BOTTOM RIGHT: Even compass out of Cracker-Jack box picks up field of magnet used in alarm contact at 5". Use better compass or magnetometer for serious work.

SEISMIC SENSORS

Passive in the sense that they send out no signal to betray their presence, seismic sensors get into sophisticated technology in their discrimination circuits. These must tell the difference between human footfalls and thunder, passing cars, animals, and a host of low-frequency vibration sources that otherwise would trigger them.

The breed encountered most commonly in civilian use hides underground; several above-ground species saw use in Vietnam, including one disguised as a rock.

Early models had to be dug up yearly to replace their batteries, inconvenient, to say the least, and expensive to maintain; and many had to be hard-wired. Later models powered their sensors by relying on the piezoelectric effect, but still faced the conundrum of processing the signal and getting it to the monitoring station. Either hard-wire, or rely on radio transmissions.

Whichever avenue you choose, seismic sensors are expensive, so much so that their use is limited to genuinely high security installations—it is rumored in certain circles that this type of sensor rings the NSA complex in West Virginia at a radius of one mile—working with limitless funds. That describes Uncle Sugar, all right.

PROXIMITY SENSORS

Know what a theremin is? Let's rephrase the question: Did you see the film, The Day The Earth Stood Still? Creepy outer-space music swelled in the background whenever the robot, Gort, sprang into action. A musical instrument known as a theremin conjured those tones. If you have never heard the name, chances are you've never seen one played. The musician's hands never touch the instrument, which consists of two flat metallic plates about a foot apart.

Placing a hand some inches above one plate activates the sound. Moving the hand closer turns up the volume. Move the other hand nearer or further from a second plate to alter pitch.

The theremin works on the principle of altered capacitance. Now, we all know about the Leyden jar, at least we did back when most of the population had attained a degree of literacy commensurate with eighth grade earth science. The Leyden jar is a capacitor, something that stores electrical energy. The mere proximity of two conductive objects creates capacitance, often so small as to be immeasurable. A theremin senses altered capacitance produced by nearness of human hands, and converts those changes into audible tones.

But the combination of a metal object, or a whole string of them for that matter—usually with the provision that they be isolated from ground—and a nearby human body sets the scene for a measurable change in capacitance when the body nears the wired objects. Proximity detectors function on this basis.

PDs have proven an inexpensive means of securing large numbers of metal objects that might otherwise sprout legs and walk off, such as desktop computers, personal copiers, and the like. Sometimes whole lots of cars or aircraft have been secured this way, and all by a control box no larger than a 35 mm camera.

The units are quite flexible. Simply wire together whatever you wish to protect, then adjust or "null" the unit, set the sensitivity (it can be set for actual contact, or variable proximity), and forget it. Gloves will not defeat the system, since capacitance changes despite them.

Professional units sell for hundreds of dollars; yet you can make use of the same principle in those hand-on-the-doorknob alarms: a hand on the outer knob is detected by a crude proximity sensor, one that lacks the sophistication or flexibility of the larger units. Less than $30 at Wal Mart.

HYBRID SENSORS

Alarm designers capitalized on the strengths of various sensors by using them in combination, which remedied their respective weaknesses. One sensor cross-checks the other. For example, water flowing through plastic pipes might send the microwave into a dither, but the passive infrared would ignore it. An intruder crawling slowly on the floor might escape the IR, but the microwave would tag him. These designs provide that no alarm signal fires unless both sensors give the OK. This built-in double-check has been implemented successfully, if not inexpensively.

SENSORS YOU AREN'T LIKELY TO USE

Bank vault doors contain temperature sensors for burn-jobs, as the torch attack is known in the trade. The interior may hold an air-pressure sensor to detect that slight drop/rise, depending on conditions, when the door swings open. Vibration sensors may line the interior vault walls, just in case the baddies have decided on the sledge-hammer attack through the side wall. Naturally, the floor will contain pressure pads that trip when stepped on, and the interior of the vault will contain in addition active and passive IR, microwave, and ultrasonic sensors.

And big-time safe crackers have defeated that and more....

THE CONTROL UNIT

Sensors merely send out some type of blip to claim that intrusion is underway. To perform some useful task, such as sounding an alarm or notifying the police, a control unit must process the blip.

Blips tend to measure low-voltage and low current, incapable of switching high-wattage loads that perform useful work. The control panel takes the blip and converts it into a change in a second or third circuit that does have the capability to switch heavy electrical loads.

In addition to this fundamental function, the panel decides when the system is armed and when not, and allows selection of alarm loops and zones, time delays for entries and exits, and so forth.

In addition to the sensor loop, the most vital input to the control panel is its arm/disarm switch. In the vast majority of cases, arming and disarming involve momentary closure of a switch that trips a latching relay inside the panel (a latching relay moves to either the on or off position each time it trips, and stays there until tripped again).

Now, if the arm/disarm switch were a button, anyone could press it. For that reason, alarm switches require either a key—most often a tubular one, given the ease with which pin tumblers fall to picks—or an electronic switch activated by a numeric code. Both types momentarily close a pair of contacts to enable/disable the panel.

DEFEATING ARM/DISARM SWITCHES

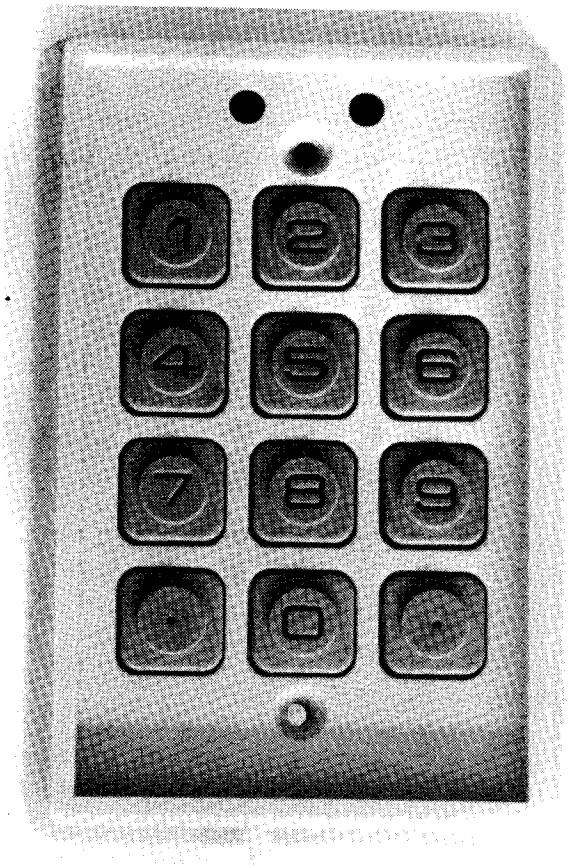
The author installed his first alarm system in 1979, two more in 1984. These were commercial-quality units of the type guarding many homes and businesses, and they cost a bundle. He has used tubular keyswitches, magnetic contacts, infrared sensors, foil, leased alarm lines and police-notification relays, electronic code switches, bells, backup batteries, and traps—and in the course of doing so picked some small knowledge of their quirks and workings.

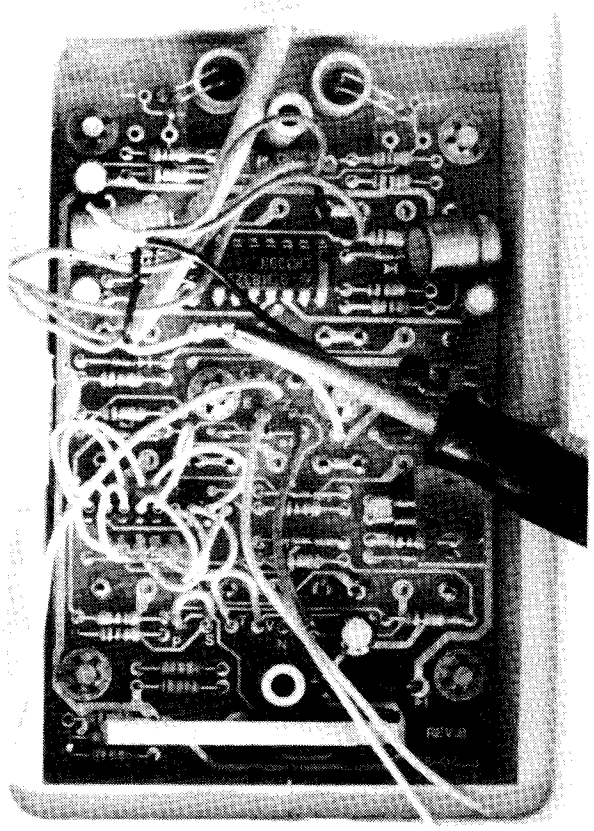
Of several methods to defeat an alarm, one involves turning it off. We review pointers here not to train fledgling felons, but to demonstrate the weaknesses in most low-to-moderate cost security systems.

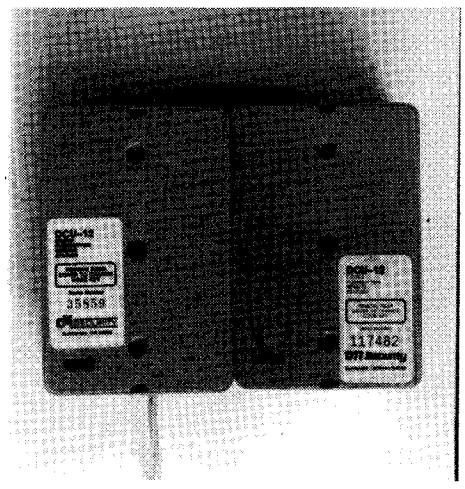
We all lose keys. Losing the tubular key to your alarm system usually means waking the neighborhood before you can rush in and kill the siren. Keyless electronic switches evolved as a convenience, but they work in an electrical sense the same as the mechanical breed. When discussing means to defeat them, we find no remarkable difference in approach.

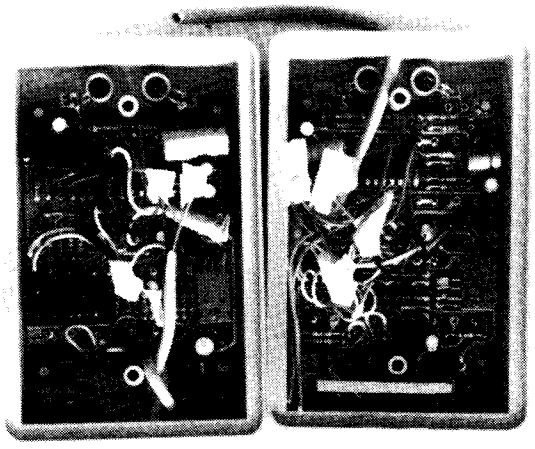
Virtually all residential and most commercial arm/disarm switches rely on momentary closure of a pair of contacts. That tubular keyswitch you see flagging the existence of some alarms (and some scams) is meant to be turned and held for about 0.5 seconds, long enough to trigger a latching relay inside the concealed control panel that A) arms the system, and B) turns on the red LED to tell you that it's armed. Code switches do this electronically, but a mechanical attack can let you defeat the system if you can get to the connecting cable.

These modules link to the panel via multi-wire cable, often ordinary telephone cable, 4- or 6-wire. Now, if you know which pair controls the alarm, you needn't bother with the box at all. Simply strip into the









TOP LEFT: Typical alarm code-key switch. Unit that has been in service some time w/o change in code may show wear or dirt on most frequently pressed keys. TOP RIGHT: Inside the box. Screwdriver tip between the pair that should be shorted for half a second to disable system. BOTTOM LEFT: Rear view of two code boxes made about four years apart by same company. Normally open tamper switch bottom left of both. BOTTOM RIGHT: Little change in circuitry over the years. Left tamper switch is no more than a piece of spring steel held away from a contact when box is screwed to wall. Unit on right uses true switch, requires much less pressure to hold, is more easily defeated. Also, right unit has capability to change code by moving jumper wires. Obvious from photos that, once you get inside the box, identifying the correct pair to short is a cinch.

multicable wire, and momentarily short the pair. (This assumes either that the box is mounted outdoors, or that you can access it without tripping the alarm.) You should see the red indicator light go off and the green come on if you have done it right.

What a pity no one uses the same color pair of wires consistently to tell which powers the LEDs and which controls the box. To learn that, you may have to open the control box. Be aware that all professionally installed and most amateur boxes hide a normally open tamper switch on the back that will trip the alarm as soon as you unscrew it from its mount. One pair of wires in the bundle serves that switch, and if you short them the alarm will sound.

The more expensive and more secure the system, the more likely you are to encounter switches mounted in the box, with a protruding plunger, plus one or more in the mount. That takes an awful lot of hands to hold unless you have partners, or can isolate the cable, know what wires terminate where, and can bypass them.

Is it possible to defeat them? Of course, and quite easily once we note their construction. The most useful tool to learn the status of wires feeding an electronic keyswitch is a digital multimeter. These meters sport extremely high impedances, usually 10 megohms or more, such that you could put the leads across the normally open tamper pair without tripping that sector. The red LED pair will be carrying either 6 or 12 volts, depending on the design of the system, and the green LED should be dead (if the green light is on, it means the system's off). The pair will be carrying low-level control voltage, since it trips a relay inside the panel. That is the pair to short for a half a second. If you identified the pair correctly, the green light will come on, and the system will be off. You may hear a relay click somewhere in the building as this happens.

Due to differences in design among brands, as well as the evolving nature of circuits, the professional approach means buying a panel, rigging it with the same type of keyswitch or electronic switch you have seen on the premises, and reading each pair with a DMM. You should be able to identify a unique voltage/polarity pair that tells you it's the one to short momentarily. You could do it in the field, but leaving so simple a matter to chance would be folly.

A direct attack on an electronic keybox is best done as a two-man job. Have one operative hold the box firmly in place while the other removes the mounting screws. Then slide a slim but firm shim up behind the box before you take it off the wall (of course, if it is mounted inside a socket in which the tamper switch is mounted, you must dig out the cable, since you probably won't be able to shim the switch if the works are recessed). Once freed, turn the box over. Carefully slide the shim to reveal the position of the tamper switch, usually the bottom. Depress the switch as you remove the shim fully. This exposes the back, which may then be pried off (two practiced pair of hands makes this easy). Now, you want nothing to do with the leads to the indicator diodes. By inspection and process of elimination, identify the prospective shorting pair. Take a jumper and short them to see if that disarms the circuit, as evidenced by the green on/red off change. (Make certain you do not short the tamper pair, which will trigger the alarm instantly; in fact, to facilitate handling, you might cut that pair, one wire at a time to avoid accidental shorting).

If one combination does not work, try others until the alarm is off. Then re-secure the box (screw it back on the wall, tape it to a board, lay a brick on it, whatever) and you are home free.

These boxes sell for so little that, in the process of casing the joint, to coin a phrase, you can ascertain the brand. Buy a system yourself and open it up, see how it works, put the meter on it. Pros work this way. It's one reason crime pays.

UNDERSTANDING THE CONTROL PANEL

Both users and would-be attackers of alarm systems should appreciate the differences between UL-approved and non-UL-approved units. There are effectively no rules for non-UL units. Those that meet UL standards are equipped with features that could prove decisive in special encounters. First, they must be equipped with battery backup. Cutting the AC power won't disable the system. Second, they must have a "secondary loop." This loop independent of one or more "main" loops remains active even after the automatic cutoff has silenced the main alarm tripped earlier. Many control units, UL-approved or not, automatically rearm themselves after being tripped if the alarm loop has been restored and before the automatic bell cutoff. That is, if a burglar forced open the door, tripped the alarm, then shut it as he fled when the bell sounded, the

unit would ring for 15 seconds to half an hour, depending on its configuration, then return to duty. If, however, the door had been propped ajar, or some other point in the loop left broken, the unit would shut itself off, leaving the premises defenseless.

Hardly surprising that an effective tactic calls for the burglar to trip the alarm intentionally, and in a few seconds cut an inconspicuous wire or shim a door open such that, though the unit will draw attention, its automatic cutoff will silence the alarm permanently since the alarm loop remains broken. The baddies return a few hours later to gut the premises at their leisure. (Cops know this ruse, and tend to keep an eye on premises whose alarm tripped earlier in the evening.)

UL-qualified units must contain a loop to guard against this attack. That loop remains armed whatever the status of the main loop, and will again sound the claxon should the baddies return. Of course, the backup loop must have its own independent sensor, usually a "trap" inside the building.

A third UL measure, one genuinely handy in light of known tactics to defeat combination switches, demands that entering the code, turning the key, or shorting the proper contacts will not silence the alarm once it has been tripped. It will do so with most non-UL units. That means that to defeat a UL unit, the alarm cannot be tripped even momentarily, or it rings until programmed to shut off, or until the owner or alarm company arrives.

Be careful hooking up the backup battery. Install it polarity reversed and kiss the panel goodbye. The author bought two $300 control panels in 1984, identical save that one was UL-approved, the other not. Only the approved unit bore an orange warning sticker that told of of deadly results of reversed polarity. (The author would have bought but one unit, but he had destroyed one by accidentally reversing the polarity, which was not marked all that clearly on the backup battery....) Given the stiff prices of alarm control units, and the simplicity of incorporating protective circuitry into them, one has to wonder why it had not been done. Who knows...maybe some companies do a fair business replacing burned-out boxes...certainly not the maker of the author's prize panels....

COST

Buying from an alarm company, even by mailorder, usually means a near-fatal price markup. Twenty dollars worth of electronics, and not very sophisticated stuff at that, becomes the $299 Deluxe Special when mounted in a $2 metal box. Sensors, wire, installation, and so forth cost extra, and bear the curse of that same awful markup.

What a pleasant surprise that you can buy units of equal performance at the local Radio Shack for half the cost. Radio Shack, at least in the opinion of some, has earned no renown for rock-bottom prices, which makes its prices on alarm gear—the equal of "professional" models in most respects—surprising and attractive. Comparison shopping is a must for amateur installers.

Before McGee Radio decided to change its image and its inventory, it carried the Cal-Rad line of products, among which some genuine alarm bargains could be found. We haven't been able to run down a discount Cal-Rad dealer. Perhaps McGee will rethink its marketing strategy.

WINDOW STICKERS

"Warning! These premises protected by electronic intrusion system!"

Now, everybody, criminals most of all, knows that some stickers are fakes. Experienced burglars know genuine stickers from phony, and real outdoor switches from bogus.

In general, window stickers will deter the unmotivated amateur, at least send him to the house next door, rather than call your bluff. Stickers and hard evidence of an alarm, such as a genuine outdoor disarm switch or obvious glass-break sensors could prove more effective in combination with warning stickers.

ILLUSIONS

The alarm business props up an illusion of security. Genuine security starts with attitudes and awareness patterns. Physical aids serve as extensions of those postures, rather than the bastions of security some would have us believe.

As a rule, NEVER discuss your security measures with anyone except as they need to know. This applies to your most trusted employee. If s/he must have the disarm combination, you must divulge the numbers; but you needn't reveal that the code is fixed, or the location of tamper switches, or where all the sensors are hidden, or that there is a backup loop, and so forth.

When you change employees, change the code, re-key your locks. Consider adding or moving your interior traps if the employee left under unpleasant circumstances, or if there was a taint of dishonesty.

THE "MEANS OF NOTIFICATION"

The alarm process distills to infinitesimal currents controlling the shifting of progressively larger ones. The detector circuit runs on milliamps or even microamps, but it trips a mechanical relay (which are being phased out as high-power semiconductors come to the fore) that will handle the power to drive an alarm bell. Some will trip a relay that will take the full 120 volts/20 amps from the wall circuit. Some fiendish defenders have made use of that very property to fashion potentially lethal traps, but that is illegal....

Suitable alarms can trigger most any device you care to name. Therein lies the key to their flexibility. Ringing a bell will not rattle most experienced burglars, especially ones who know your setup is not connected to an alarm station. It takes less than a minute to lift your thousand-dollar VCR along with a few other goodies, then be off and away, home free. What you seek is for your alarm not only to sound the siren, but to do something that makes the felon want to leave NOW, and the Devil can keep your damned VCR.

For many years, an acceptable means was a device that, after a set interval, released a cloud of CN or CS tear gas—which rendered the place inhospitable, but took about a week with the windows open to clear out so you could move back in. (And some owners "forgot" to disarm the bugger when they entered their own premises. What price security....)

And alternative might be an electric fence charger wired to selected objects; do not wire house current to anything. It killed in one case that got nationwide publicity. The jury ruled in favor of the crime victim and acquitted him of manslaughter.

Another option gets more exotic, but holds promise. This is the ultrasonic pain field generator sold by Information Unlimited. They sell completed units with sensor and everything; or you may configure your own alarm panel to activate the sound generator.

ALARM CONTROL CENTERS

In some locales, you may lease a line from the phone company and have it surface at the local police station or an alarm company. That way, when your alarm trips, the cops know it an instant after the crooks (or maybe first, if it is silent).

The leased pair reverses polarity. The monitor can tell if it is cut, but that gives a different signal than triggering the alarm. This is easy for someone with a knowledge of electronics to defeat. And the phone company couldn't be more helpful in showing where to access the line. It's right in the surface box on the outside of your building, where the bad guys can put the meter on it. Phone lines run 48 volts. The dedicated alarm pair usually does not; or, if it does, out of some limp attempt to foil burglars, they will attach a lineman's handset to each pair and key in on the pair with no dial tone. In the discussion of bugging you met the punch-down block. The phone company used that same punch-down block for the author's leased alarm-line pair; $17 a month in 1984.

Bigger game, such as banks, have turned to special pulsed signals to keep the central unit happy, but sophisticated vault specialists have mimicked even this complex signal.

The latest units send a digital bitstream seemingly random to someone monitoring it and trying to decipher it. But it's only a matter of time before it falls to decryption software.

* * *

A BRIEF LOOK AT SPOOK BOOKS

The publication in 1972 of Kurt Saxon's Poor Man's James Bond defined a genre—the "big" spook book—that was continued and refined by later authors and has grown to more than a dozen volumes, all feeding an insatiable hunger for this dread lore. In case the reader has not scanned them, we offer sketches of selected works.

THE ANARCHIST'S COOKBOOK

Badly out of date but still selling for $20 in some outlets, William Powell's early (circa 1972) effort has become an interesting period piece with strong political overtones, one that reflects a naivete of both the enforcers and their victims, as seen in better if more turbulent days. Its tech advice has succumbed to the passage of time, as do we all in the end. An interesting read from a historical perspective.

THE POOR MAN'S JAMES BOND

Now a cult figure in the realm of spook literature, and lately a guru in the survival camp that peaked in the late 1970s, Kurt Saxon shook the world with his new twist in 1972. TPMJB rambled through everything from tear gas to interesting uses for shotgun shells.

In those early days it was great fun to read, a great kick to show off to your friends. It made you feel as if you knew so much that nobody else did. Saxon's approach emphasized a self-sufficiency that has proven unnecessary, if only temporarily. For example, most folks can buy all the professionally produced tear gas they want today, and needn't resort to synthesis.

TPMJB now appears in a Part II edition that consists of a compendium of previously published material, including Tenney L. Davis' The Chemistry of Powder and Explosives. A worthwhile read for those who have not seen it.

THE BIG BROTHER GAME

Author Scott French, under the firm tutelage of publisher Lyle Stuart, produced The Big Brother Game in 1976. It has shown amazing stamina in the spook field, despite its necessarily dated technology, though many of its lessons hold firm. French's canny/witty insights into the private detective and big brother arenas ring true even today. A whimsical, post-60s innocence made it novel in its day, a warm, welcome glow that has faded from other works in the cold reality of these grim times.

A landmark book that upped the ante for authors looking to break into the field, TBBG remains on the recommended list.

THE COMPLETE SPY

McGarvey and Caitlin produced this compilation of hardware from various catalogs, complete with pix and prices, and shored up the list with slick filler to flesh out their uses. At 8-1/2 x 11, it is a true big spook book, perhaps the softest of the breed in terms of exposing the reader to genuinely tricky material. Superior section on physical disguise.

SPY-TECH

Conspicuous mainly for its journalistic excellence and the you-are-there feel it breathes into spyplane flights and spy satellite tests, Graham Yost's Spy-Tech leans top-heavy with spy satellites and aircraft, light on detail about field gear. The book covers in a single sentence what we would like to read several pages about. Still a good read and probably the most professionally flavored of the breed.

HOW TO GET ANYTHING ON ANYBODY

Lee Lapin's entry, one of the costliest of the bunch, going for $30 most places and as high as $34.95 in past Edmund Scientific catalogs, employs a Consumer Reports style in hands-on tests of selected spook gear. We see mainly medium-priced merch in profile. The heavy stuff rates mention, but we do not get to play with it through author Lapin's hands.

One of the meatiest of the group, HTGAOA wastes little space and belongs in the library of all serious students of investigation.

SPY GAME

A collaboration of Scott French and Lee Lapin, the work presently perches in the spook hutch but proves difficult to define. The premise seems to have been, What would a pair of spook-types do if they had unlimited resources? The authors bought or borrowed enough gear to keep them under government surveillance for the rest of their lives, then lit out on a road-trip for Africa, conducted field-tests, took pictures, and reported the results. In addition to providing worthwhile data unavailable elsewhere, the book takes us on a safari of vicarious indulgence like nothing else in print. Through the authors, we get to shoot body armor, peer through the best in night-vision scopes, handle the top directional mics, track cars equipped with the latest infrared beacons...the list goes on for more than 500 pages.

Spy Game offers expert advice from other contributors, most notably new-ID czar Barry Reid and defensive driving expert J. D. Aranha.

The book is big and expensive. It measures 8-1/2 x 11 and weighs several pounds, even in softcover. No price printed on the cover. We got our copy for $35 plus shipping, only to see it listed elsewhere for $30. Recommended.

Each of these books embraces a broad spectrum. For each subject they mention, there exist at least 5 dedicated texts. For example, silencers command a groupie-like following, as does credit, new ID, skip-tracing, and another favorite, lock-picking. Though ceding depth compared to dedicated texts, the spook genre offers a global perspective essential to effective use of its lore. For instance, no operative would master lock-picking and learn nothing of alarms and police behavior...or silencers, should the pit of the gig call for that grim recourse....

* * *

A PHILOSOPHY OF PERSONAL SECURITY

So what practical use arises from this dread and sinister lore? What other than passing interest has the average Jane for lock-picking and raw steel bullets?

First, it is a cult just to get information, a philosophy that there is nothing about anyone or any topic you cannot learn if you truly wish to do so; no place you cannot enter, nothing forbidden to those willing to pay the fare in terms of work and risk. Information confers power; power bestows freedom.

By the same token, recognize that there is much about you, often more than you imagined, available to others, most of it both detrimental and inaccurate—and those others usually harbor you ill will. Spooklore tells how to protect your own privacy, your own security.

In this age that won't rent you a car unless you flash a major credit card, or get "prior credit approval," which amounts to the same credit check the card companies run, few can afford to ignore this technology, this philosophy.

Did you buy this book through the mails? How did you pay for it? Having examined it, is there anyone whom you would wish not to know that you had bought it? Has the fact of its purchase put you on secret government surveillance lists?

If you paid by check, be aware that the law requires your bank to keep a photocopy of your checks for at least five years. Technically, they are required to copy only checks over $100, but many banks copy them all to avoid the labor cost of screening. The check need not mention the book title. The government and private snoopers know what companies sell what off-the-wall books. They have ways of pressuring them.

Did you know that some mailorder companies sell lists of their customers to mail solicitation agencies? (Hell, even SOF does it, but will remove your name if you so request.) Did you ask that your name be left off the bookseller's personal list? Did you use an alias?

If not, then count on the fact of this purchase being known. (The police reportedly found a copy of Hit Man, by "Rex Feral," in the closet of the man ultimately convicted in the so-called "billion dollar boy's club" case. Would any books in your closet give the wrong impression, should your house be searched for other reasons? This book, maybe....?)

9
SOURCES, RESOURCES, & REFERENCES

For those unfamiliar with the abbreviation, "ISBN" stands for "International Standard Book Number," a unique number assigned to most books published in the free world. You needn't know author, title, or publisher, only that number, to order a book from any bookstore, or to have the library check their stacks for it or get it on interlibrary loan. References listed here are worth reading, many are worth buying if you get involved in spookdom in a serious way. Catalogs listed are worth a look, too.

* * *

Microphones 3rd Edition, by Martin Clifford. 1986; ISBN 0-8306-0475-8

Digital Audio Signal Processing: An Anthology, edited by John Strawn. ISBN 0-86576-082-9

Digital Image Processing, by Gary Baxes. 0-13-214064-0, Prentice Hall

Digital Picture Processing, by L.P. Yaroslavsky. Springer Verlag 0-387-11934-5

Digital Processing of Analog Signals, by Thomas Young. Prentice Hall. These last four "digital" books will interest mainly those who already understand basic digital technology.

Code Breaking and Signals Intelligence, edited by Christopher Andrew. 0-7146-3299-6

Cryptography: A New Dimension in Computer Data Security, by Carl Meyer and Steven Matayas. 0-471-04892-5; Wiley. Do you have a PhD in mathematics? This is your book.

Private Investigator's Basic Manual, by Richard H. Akin 0-398-03520-2, Charles C. Thomas

Fireworks, by George Plimpton. 0-385-15414-3, Doubleday. The pyro underground seen through the eyes of the Times. An interesting read, but strictly soft-core.

Tungsten: Sources, Metallurgy, Properties, and Applications, by Yihe and Wang. 0-306-31144-5, Plenum Press

Intrusion Detection Systems, by Robert L. Barnard. Butterworth. 0-409-95025-2, 1981. Dry reading, but comprehensive and all meat.

Alarm Systems and Theft Prevention, by Thad Weber. Butterworth, 1973. 0-913708-11-9. Chatty; dated in a technological sense, but conveys much more in the way of the criminal mind-set and attack modes than Barnard's book.

Confidential Information Sources, Public and Private, by John M. Carroll. Butterworth. 0-913708-19-4, 1975. Solid basic reference, along with data on the Canadian systems.

Metalworking, by T. Gardner Boyd. 0-87006-396-0; Good Art Publishing

Metallurgy Basics, by Donald V. Brown. 0-442-21434-0, Van Nostrand Reinhold, 1983

Special Circuits Ready Reference, by John Markus. ISBN 0-07-040461-5, McGraw-Hill. One of a series of electronic circuit compendia compiled by Mr. Markus, this volume zeros in on compressors, limiters, automatic level controls, and frequency-shapers. Mere days before this book went to press we breadboarded the automatic level control circuit at the top of page 3 (referenced to 73 Magazine, June, 1976, pp 52-54). Using the old workhorse 741 op amp and a common FET stocked by Radio Shack (2N3819), this unit beat every ALC we had tested up to that point, including the 570/571 series of dedicated chips. We substituted the new J-FET input version of the 741 with some reduction in noise; mated easily to passband filter (cut hiss at the ALC by placing a 100 to 1000 picofarad cap across pins 2 and 6; the higher the cap value, the greater the treble/hiss cut; use the output pot of the ALC as your "volume control;" audio taper works best). As matters stand, we would use this design in lieu of the uPC1571 in Ultra-Amp, at least for the ALC. The circuit would not replace a true compressor.

Audio IC Op-Amp Applications, Third Edition, by Walter G. Jung. 0-672-22452-6, Howard W. Sams & Co., Indianapolis, 1986. Order by phone 800-428-SAMS. Also get Mr. Jung's Op Amp Cookbook, which deals with compressors and limiters.

Active Filter Cookbook, by Don Lancaster. Sticky reading at first, but the more filters you build, the more sense it makes. Get from Sams Co.

Understanding Operational Amplifiers, by Melen & Garland, from Sams. These last 5 books, along with chip-makers' data sheets and a few months at the breadboard, will enable the novice to design and build his own custom "Ultra Amp."

Amplification for the Hearing-Impaired, Ed by Michael C. Pollack, PhD. Grune & Stratton, 1988, 0-8089-1886-9. Main value lies in its vast reference list of audiology journal articles that detail signal processing techniques to maximize intelligibility of speech. Get it on interlibrary loan.

Cryptology and the Personal Computer, by Karl Andreassen. Aegean Park Press, 0-89412-145-8, 1986

Satellite and Cable TV Scrambling and Descrambling, by Brent Gale and Frank Baylin. 0-917893-07-7. Good discussion of theory, no hard descrambler circuits.

National Semiconductor Linear Databooks, #1, 2, 3. Offer info varying in depth from minimal to detailed external schematics & applications for their own & pin-compatible chips. Available from Digi-Key. #2 & 3 $10 each; #1 $15. #3 deals with audio amps and preamps. National and other chip-makers will, on request, send you application notes concerning their various chips, essential to understanding their uses. The books on op amps noted above contain manufacturers' names & addresses.

Parts Express, 340 East First St, Dayton, OH, 45402; 800-322-3525; best prices we've seen on piezo horn tweeters; general electronic parts.

Nuts & Volts magazine, Box 1111, Placentia, CA, 92670; $12/yr, $60 lifetime subscription; wide range of display and classified ads for all manner of electronic parts & finished gear.

J&M Country Store, RR1, Box 59, Alexander, IL, 62601. Mailorder dealer of Estes Industries rocket products. Good prices compared w/retail hobby stores.

Flight Systems, Inc. 9300 E 68th St, Raytown, MO, 64133. Source of F-class short-burn/high-thrust rocket engines. Catalog $2.

North Coast Rocketry, Box 240017, Mayfield Hts, OH, 44124. Catalog $1.50. Sells kits for rockets that dwarf Sidewinder missiles and the engines to power them. Their products aimed at advanced rocketeers. Run by genuine pros. 'Nuff said....

Fertik's Electronics, 5400 Elle St, Philadelphia, PA, 19120. Electronic parts, some surplus, many hard-to-find, bargains in some categories.

McGee Radio, 1901 McGee St, Kansas City, MO, 64108. Catalog $2. Formerly broad-spectrum electronics, now emphasizing raw loudspeakers, mics, PA gear. Carries piezo tweeters.

Fair Radio Sales, Box 1105, Lima, OH, 45802. Mainly surplus electronics, some of it pre-WW II. Best bargain: thin PC board $2.25 a sheet #VTC-SS 18" x 24", cut it w/scissors for quickie boards. 419-223-2196.

Mouser Electronics; has 3 distribution centers. 1-800-346-6873 for free catalog updated several times a year. Along with Digi-Key, one of the largest parts houses in the country. Fast, but usually has to back-order a few parts.

Digi-Key, 1-800-344-4539 for free catalog, ditto updates. Similar to Mouser, greater emphasis on connectors, different emphasis on semiconductors. The two firms' inventories complement each other. Fast, rarely has to back-order. These two catalogs essential if you get into electronics.

Gernsback Publications, Inc. Publishes Radio-Electronics and Hands-On Electronics. Back-issues of both are available. Write them at 500-B Bi-County Rd, Farmingdale, NY, 11735 for price and availability. They offer a photocopying service for individual articles. If you plan to build projects whose schematics Gernsback kindly granted us permission to reprint, you may want to get the whole article in which it originally appeared.

Crypt, version 3.1, was released just as this book went to the printer. Price $25, rather than $20 quoted earlier. Write Mr. Maniscalco for details on this vastly improved version of the program detailed in the Security chapter.

The Puzzle Palace, by James Bamford. 0-395-31286-8, Houghton Mifflin. Definitive work to date on the National Security Agency.

Will: The Autobiography of G. Gordon Liddy. For spiritual guidance.

Fear and Loathing in Las Vegas: A Savage Journey to the Heart of the American Dream, by Hunter S. Thompson. Ditto....

ERRATA

P7, last para: element inside credit card mic is not a WM62-A; P33, para 2, line 2: RC = LC; P42: caption Popular Science = Popular Electronics, which has been resurrected since The Spook Book was published; P42: schematic positive side of 47uF cap does connect to the left side of S1; P44, para 6, L2: you ears = your ears; P45 schematic: pin 4 of LM386 is grounded; P55 middle schematic 1uF NP cap should come off pin 10 rather than ground; P69, line 3, para 4: CCS = the CCS; P70, para 7, line 2: profession = professional; P103 diagram: U20 = U30 (generally, U20 = U30 in VC discussion); P110, para 2, line 3: delete "detectors;" P110, para 6, line 6: $11 = $8; P116, para 8, line 3: an = a; P129, para 9, line 3: M16A1 = M16A2; P130, para 4, line 1: alter = altar; P143, para 4, line 2: delete "with the axis;" P144, para 8, line 1: suppresser = suppressor; P144, para 11, line 1 speak = peak; P145, para 11; line 1: passed = passes; P226, para 6, line 4: offer = offers; P 240, para 5, line 3: of of = of; Mario Maniscalco's new mailing address: Box 110082, Cleveland, 44111.

Form Approved: OMB No. 1512-0042 (3/31/86)

DEPARTMENT OF THE TREASURY
BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

APPLICATION FOR LICENSE
UNDER 18 U.S.C. CHAPTER 44, FIREARMS

FOR ATF USE ONLY

1. NAME OF OWNER OR CORPORATION (If partnership, include name of each partner)

2. TRADE OR BUSINESS NAME, IF ANY

3. EMPLOYER IDENTIFICATION NUMBER OR SOCIAL SECURITY NUMBER

4. NAME OF COUNTY IN WHICH BUSINESS IS LOCATED

5. BUSINESS ADDRESS (RFD or street no., city, State, ZIP Code)

6. BUSINESS LOCATION (If no street address in item 5, show directions and distance from nearest P.O. or city limits)

7. TELEPHONE NUMBER (Include Area Code.)
BUSINESS _____
RESIDENCE _____

8. APPLICANT'S BUSINESS IS
☐ INDIVIDUALLY OWNED ☐ A CORPORATION
☐ A PARTNERSHIP ☐ OTHER (Specify) _____

9. IS ANY BUSINESS OTHER THAN THAT FOR WHICH THE LICENSE APPLICATION IS BEING MADE CONDUCTED ON THE BUSINESS PREMISES? (If "Yes," give the general nature of that business)
☐ YES ☐ NO

10. APPLICATION IS MADE FOR A LICENSE UNDER 18 U.S.C CHAPTER 44 AS A: (Place an "X" in column (b) of the appropriate line. Submit the fee shown in column (c) with the application.)

TYPE*	DESCRIPTION OF LICENSE TYPE (a)	"X" (b)	FEE (c)
01	DEALER IN FIREARMS OTHER THAN DESTRUCTIVE DEVICES OR AMMUNITION FOR OTHER THAN DESTRUCTIVE DEVICES (INCLUDES: Rifles, Shotguns, Pistols, Revolvers, Ammunition only, Gunsmith activities and National Firearms Act (NFA) Weapons)		$30
02	PAWNBROKER DEALING IN FIREARMS OTHER THAN DESTRUCTIVE DEVICES OR AMMUNITION FOR FIREARMS OTHER THAN DESTRUCTIVE DEVICES		$75
03	COLLECTOR OF CURIOS AND RELICS (Note: Omit items 11 and 12 if checked here and no other licenses are applied for.)		$30
06	MANUFACTURER OF AMMUNITION FOR FIREARMS OTHER THAN DESTRUCTIVE DEVICES		$30
07	MANUFACTURER OF FIREARMS OTHER THAN DESTRUCTIVE DEVICES		$150
08	IMPORTER OF FIREARMS OTHER THAN DESTRUCTIVE DEVICES OR AMMUNITION FOR FIREARMS OTHER THAN DESTRUCTIVE DEVICES		$150
09	DEALER IN DESTRUCTIVE DEVICES OR AMMUNITION FOR DESTRUCTIVE DEVICES		$3000
10	MANUFACTURER OF DESTRUCTIVE DEVICES OR AMMUNITION FOR DESTRUCTIVE DEVICES		$3000
11	IMPORTER OF DESTRUCTIVE DEVICES OR AMMUNITION FOR DESTRUCTIVE DEVICES		$3000

MAKE CHECK OR MONEY ORDER PAYABLE TO THE BUREAU OF ALCOHOL, TOBACCO AND FIREARMS TOTAL FEES $

*NOTE: Applicants intending to engage in business relating to NFA weapons (including destructive devices and ammunition for destructive devices) are required to pay a special (occupational) tax before commencing business (26 U.S.C. 5801). for information, contact the NFA Branch, Bureau of Alcohol, Tobacco and Firearms, Washington, DC 20226.

11. HOURS OF OPERATION OF APPLICANT'S BUSINESS

Time	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Open							
Close							

12. ARE THE APPLICANT'S BUSINESS PREMISES OPEN TO THE GENERAL PUBLIC DURING THESE HOURS?
☐ YES
☐ NO (If "No," give explanation on separate sheet.)

13. IS APPLICANT PRESENTLY ENGAGED IN A BUSINESS REQUIRING A FEDERAL FIREARMS LICENSE? (If "Yes," answer 14.)
☐ YES ☐ NO

14. PRESENT LICENSE NUMBER

15. DESCRIBE SPECIFIC ACTIVITY APPLICANT IS ENGAGED IN, OR INTENDS TO ENGAGE IN, WHICH WILL REQUIRE A FEDERAL FIREARMS LICENSE (e.g., dealer in rifles, shotguns, revolvers and ammunition, dealer in ammunition only, gunsmith, dealer in machine guns, etc.)

IF BUSINESS OBTAINED FROM SOMEONE ELSE GIVE

16. NAME

17. LICENSE NUMBER

18. LIST BELOW THE INFORMATION REQUIRED FOR EACH INDIVIDUAL OWNER, (sole owners must include themselves), PARTNER, AND OTHER RESPONSIBLE PERSONS (see Instruction 7) IN THE APPLICANT BUSINESS. IF A FEMALE, LIST GIVEN NAMES AND MAIDEN, IF MARRIED, e.g., "MARY ALICE (SMITH) JONES," NOT "MRS. JOHN JONES." (If additional space is needed, use a separate sheet.)

FULL NAME	POSITION AND SOCIAL SECURITY NO.	HOME ADDRESS (Include ZIP Code)	PLACE OF BIRTH	DATE OF BIRTH

19. HAS APPLICANT OR ANY PERSON LISTED ABOVE: (If "Yes," place an (*) by the name and show city and State at right.)	YES	NO
A. HELD A FEDERAL FIREARMS LICENSE		
B. BEEN DENIED A FEDERAL FIREARMS LICENSE		
C. BEEN AN OFFICER IN A CORPORATION HOLDING A FEDERAL FIREARMS LICENSE		
D. BEEN AN EMPLOYEE RESPONSIBLE FOR FIREARMS ACTIVITIES OF A FEDERAL FIREARMS LICENSEE		

CITY

STATE

GIVE FULL DETAILS ON SEPARATE SHEET FOR ALL "Yes" ANSWERS IN ITEMS 20 & 21.		YES	NO
20. IS APPLICANT OR ANY PERSON NAMED IN ITEM 18 ABOVE:	A. CHARGED BY INFORMATION OR UNDER INDICTMENT IN ANY COURT FOR A CRIME PUNISHABLE BY IMPRISONMENT FOR A TERM EXCEEDING ONE YEAR[1]		
	B. A FUGITIVE FROM JUSTICE		
	C. AN ALIEN WHO IS ILLEGALLY OR UNLAWFULLY IN THE UNITED STATES		
	D. UNDER 21 YEARS OF AGE		
	E. AN UNLAWFUL USER OF OR ADDICTED TO MARIJUANA OR ANY DEPRESSANT, STIMULANT OR NARCOTIC DRUG		
21. HAS APPLICANT OR ANY PERSON NAMED IN ITEM 18 EVER:	A. BEEN CONVICTED IN ANY COURT OF A CRIME PUNISHABLE BY IMPRISONMENT FOR A TERM EXCEEDING ONE YEAR[2]		
	B. BEEN DISCHARGED FROM THE ARMED FORCES UNDER DISHONORABLE CONDITIONS		
	C. BEEN ADJUDICATED AS A MENTAL DEFECTIVE OR BEEN COMMITTED TO ANY MENTAL INSTITUTION		
	D. RENOUNCED HIS CITIZENSHIP HAVING BEEN A CITIZEN OF THE UNITED STATES		

22. **CERTIFICATION:** Under the penalties imposed by 18 U.S.C. 924, I declare that I have examined this application and the documents submitted in support thereof, and to the best of my knowledge and belief, they are true, correct and complete.

SIGN HERE ▶	TITLE	DATE

FOR ATF USE

23. APPLICATION IS

☐ APPROVED ☐ DISAPPROVED*

☐ TERMINATED*

*LICENSE FEE WILL BE REFUNDED BY THE BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

REASONS FOR TERMINATED OR DISAPPROVED APPLICATION

SIGNATURE OF REGIONAL DIRECTOR (COMPLIANCE)	250	DATE

[1]Information — A formal accusation of crime made by a prosecuting attorney, as distinguished from an indictment presented by a grand jury.

[2]The actual sentence given by the judge does not matter — a "yes" answer is necessary if the judge could have given a sentence of more than one year. Also, a "yes" answer is required even if a conviction has been discharged, set aside, or dismissed pursuant to an expungement or rehabilitation statute. However, a crime punishable by imprisonment for a term exceeding 1 year does not include a conviction which has been set aside under the Federal Youth Correction Act.

Form Approved: OMB No. 1512-0027 (10/31/89)

DEPARTMENT OF THE TREASURY—BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

APPLICATION FOR TAX PAID TRANSFER AND REGISTRATION OF FIREARM

SEE INSTRUCTIONS ATTACHED.
TO BE SUBMITTED IN DUPLICATE
TO: National Firearms Act Branch
Bureau of Alcohol, Tobacco and Firearms
Washington, DC 20226

2a. TRANSFEREE'S NAME AND ADDRESS (If transferee is a Special (Occupational) Taxpayer who is acquiring firearm for personal use, rather than as part of his business inventory, show personal name below and check here: ☐)

2b. TRADE NAME *(See instruction 2e)*

3a. TRANSFEROR'S NAME AND MAILING ADDRESS (If the firearm is registered under your trade name, enter your trade name. EXECUTORS: See instruction 2f.)

3c. IF APPLICABLE: DECEDENT'S NAME, ADDRESS, AND DATE OF DEATH

1. TYPE OF TRANSFER *(Check one)*
(See instructions 1 and 6)

☐ $5 ☐ $200

Submit with your application a check or money order for the appropriate amount made payable to the Department of the Treasury. Upon approval of this application, this office will acquire, affix and cancel the required "National Firearms Act" stamp for you. *(See Instruction 6)*

3b. NUMBER, STREET, CITY, STATE AND ZIP CODE IF DIFFERENT FROM ITEM 3a.

The above-named and undersigned transferor hereby makes application as required by Section 5812 of the National Firearms Act to transfer and register the firearm described below to the transferee.

4. DESCRIPTION OF FIREARM *(Complete items a through h)*

a. NAME AND ADDRESS OF MANUFACTURER AND/OR IMPORTER OF FIREARM	b. TYPE OF FIREARM *(Short-barreled rifle, machine gun, destructive device, any other weapon, etc.)*	c. CALIBER, GAUGE OR SIZE *(Specify)*	d. MODEL LENGTH *(Inches)* e. OF BARREL: f. OVERALL: g. SERIAL NUMBER

h. ADDITIONAL DESCRIPTION OR DATA APPEARING ON FIREARM *(Attach additional sheet if necessary)*

5. TRANSFEREE'S FEDERAL FIREARMS LICENSE *(If any)* *(Give complete 15-digit number)*				6. TRANSFEREE'S SPECIAL (OCCUPATIONAL) TAX STATUS	
First 6 digits	2 digits	2 digits	5 digits	a. ATF IDENTIFICATION NUMBER	b. CLASS

7. TRANSFEROR'S FEDERAL FIREARMS LICENSE *(If any)* *(Give complete 15-digit number)*				8. TRANSFEROR'S SPECIAL (OCCUPATIONAL) TAX STATUS	
First 6 digits	2 digits	2 digits	5 digits	a. ATF IDENTIFICATION NUMBER	b. CLASS

UNDER PENALTIES OF PERJURY, I DECLARE that I have examined this application, and to the best of my knowledge and belief it is true, correct and complete, and that the transfer of the described firearm to the transferee and receipt and possession of it by the transferee are not prohibited by the provisions of Chapter 44, Title 18, United States Code; Chapter 53, Title 26, United States Code; or Title VII of the Omnibus Crime Control and Safe Streets Act, as amended; or any provisions of State or local law.

9. SIGNATURE OF TRANSFEROR *(Or authorized official)*	10. NAME AND TITLE OF AUTHORIZED OFFICIAL *(Print or type)*	11. DATE

THE SPACE BELOW IS FOR THE USE OF THE BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

BY AUTHORITY OF THE DIRECTOR, THIS APPLICATION HAS BEEN EXAMINED, AND THE TRANSFER AND REGISTRATION OF THE FIREARM DESCRIBED HEREIN AND THE INTERSTATE MOVEMENT OF THAT FIREARM, WHEN APPLICABLE, TO THE TRANSFEREE ARE:

STAMP NUMBER

☐ APPROVED *(With the following conditions, if any)*

☐ DISAPPROVED *(For the following reasons)*

SIGNATURE OF DIRECTOR, BUREAU OF ALCOHOL, TOBACCO AND FIREARMS	DATE

ATF Form 4 (5320.4) (10-83)

CERTIFICATIONS

If the transferor of a destructive device, machinegun, short-barreled shotgun or short-barreled rifle is a Federal firearms licensee, and the transferee is anyone other than a licensee qualified to deal in the firearm to be transferred, the transferee must sign the Applicant Certification (item 2 below) in the presence of the law enforcement officer signing item 3 below. The Law Enforcement Certification (item 3 below) must be completed for the transfer of any registered firearm to an individual other than a licensee qualified to deal in the firearm to be transferred. In addition, the individual transferee must affix a recent photograph (taken within the past year) in item 1 and submit, in duplicate (to the transferor) two completed copies of FBI Form FD-258, Fingerprint Card. (See Important note below.)

1. PHOTOGRAPH

AFFIX
RECENT PHOTOGRAPH HERE
(Approximately 2" x 2")

2. APPLICANT CERTIFICATION

I, _____, have a reasonable necessity to possess the device or
(Name of Transferee)

weapon described on this application for the following reason(s) _____

_____

and my possession of the device or weapon would be consistent with public safety (18 U.S.C. 922(b) (4) and 27 CFR 178.98).

UNDER PENALTIES OF PERJURY, I declare that I have examined this application, and to the best of my knowledge and belief it is true, correct and complete, and that receipt and possession of the firearm described on this form will not place me in violation of the provisions of Chapter 44, Title 18, U.S.C.; Chapter 53, Title 26, U.S.C.; or Title VII of the Omnibus Crime Control and Safe Streets Act, as amended, or any provisions of State or local law.

_____ _____
(Signature of Transferee or official authorized to sign for firm) (Date)

3. LAW ENFORCEMENT CERTIFICATION (See IMPORTANT note below)

I certify that I am the chief law enforcement officer of the organization named below having jurisdiction in the area

of residence of _____. I have no information indicating that the transferee will use the fire-
(Name of Transferee)

arm or device described on this application for other than lawful purposes. I have no information that the receipt and/or possession of the firearm described in item 4 of this form would place the transferee in violation of State or local law.

_____
(Signature and Title of Chief Law Enforcement Officer - See IMPORTANT note below)

_____ _____
(Date)

_____
(Organization and Street Address)

IMPORTANT: The chief law enforcement officer is considered to be the Chief of Police for the transferee's city or town of residence, the Sheriff for the transferee's county of residence; the Head of the State Police for the transferee's State of residence; a State or local district attorney or prosecutor having jurisdiction in the transferee's area of residence; or another person whose certification is acceptable to the Director, Bureau of Alcohol, Tobacco and Firearms. If someone has specific delegated authority to sign on behalf of the Chief of Police, Sheriff, etc., this fact must be noted by printing the Chief's, Sheriff's, or other authorized official's name and title, followed by the word "by" and the full signature and title of the delegated person.

Form Approved: OMB No. 1512-0024 (9/30/86)

DEPARTMENT OF THE TREASURY—BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

APPLICATION TO MAKE AND REGISTER A FIREARM

(Submit in duplicate. See Instructions attached.)

TO: National Firearms Act Branch, Bureau of Alcohol, Tobacco and Firearms, Washington, DC 20226

The undersigned hereby makes application, as required by Sections 5821 and 5822 of the National Firearms Act, Title 26 U.S.C., Chapter 53, to make and register the firearm described below.

1. TYPE OF APPLICATION *(Check one)*

☐ a. TAX PAID. Submit with your application a check or money order for $200 made payable to the Department of the Treasury. Upon approval of the application, this office will acquire, affix, and cancel the required "National Firearms Act" stamp for you.

☐ b. TAX EXEMPT because firearm is being made on behalf of the United States, or any department, independent establishment, or agency thereof.

☐ c. TAX EXEMPT because firearm is being made by or on behalf of any State or possession of the United States, or any political subdivision thereof, or any official police organization of such a government entity engaged in criminal investigations.

2. APPLICATION IS MADE BY:
☐ INDIVIDUAL
☐ BUSINESS FIRM ☐ GOVERNMENT ENTITY

TRADE NAME *(If any)*

3a. APPLICANT'S NAME AND MAILING ADDRESS *(Type or print below and between the dots)*

b. IF P.O. BOX IS SHOWN ABOVE, STREET ADDRESS MUST BE GIVEN HERE

c. COUNTY

IMPORTANT: COMPLETE THE REVERSE SIDE. INDIVIDUALS (INCLUDING LICENSED COLLECTORS) MUST ALSO SUBMIT, IN DUPLICATE, FBI FORM FD-258, FINGERPRINT CARD.

d. TELEPHONE AREA CODE AND NUMBER

4. DESCRIPTION OF FIREARM (Complete items a through i)

a. NAME AND LOCATION OF ORIGINAL MANUFACTURE OF FIREARM (RECEIVER) *(If prototype, furnish plans and specifications) (See Instruction 2f.)*	b. TYPE OF FIREARM TO BE MADE *(Shortbarreled rifle, machine gun, destructive device, etc.)*	c. CALIBER, GAUGE OR SIZE *(Specify)*

d. MODEL

LENGTH e. OF BARREL: *(inches)* f. OVERALL:

g. SERIAL NUMBER *(See Instruction 2g.)*

h. ADDITIONAL DESCRIPTION *(Include all numbers and other identifying data which will appear on the firearm)*

i. STATE WHY YOU INTEND TO MAKE FIREARM *(Use additional sheet if necessary)*

5. APPLICANT'S FEDERAL FIREARMS LICENSE *(If any)*
(Give complete 15-digit number)

First 6 digits	2 digits	2 digits	5 digits

6. SPECIAL (OCCUPATIONAL) TAX STATUS

a. ATF IDENTIFICATION NO. | b. CLASS

7. EMPLOYER'S IDENTIFICATION NUMBER *(If applicable)*

IMPORTANT: GIVE FULL DETAILS ON SEPARATE SHEET FOR ALL "YES" ANSWERS IN ITEMS 8 AND 9

8. IS APPLICENT	YES	NO
a. Charged by information or under indictment in any court for a crime punishable by imprisonment for a term exceeding one year?		
b. A fugitive from justice?		
c. An alien who is illegally or unlawfully in the United States?		
d. Under 21 years of age?		
e. An unlawful user of or addicted to marihuana or any depressant, stimulant or narcotic drug?		
10. A citizen of the United States		

9. HAS APPLICANT	YES	NO
a. Been convicted in any court of a crime punishable by imprisonment for a term exceeding one year?		
b. Been discharged from the armed forces under dishonorable conditions?		
c. Been adjudicated as a mental defective or been committed to any mental institution?		
d. Renounced his or her citizenship, having been a citizen of the United States?		

UNDER PENALTIES OF PERJURY, I DECLARE that I have examined this application, including accompanying documents, and to the best of my knowledge and belief it is true, accurate and complete and the making and possession of the firearm described above would not constitute a violation of Chapter 44, Title 18, U.S.C., Chapter 53, Title 26, U.S.C., Title VII of the Omnibus Crime Control and Safe Streets Act, as amended, or any provisions of State or local law.

11. SIGNATURE OF APPLICANT	12. NAME AND TITLE OF AUTHORIZED OFFICIAL OF FIRM OR CORPORATION *(If applicable)*	13. DATE

THE SPACE BELOW IS FOR THE USE OF THE BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

By authority of the Director, Bureau of Alcohol, Tobacco and Firearms, this application has been examined and the applicant's making and registration of the firearm described above is:

STAMP NUMBER

☐ APPROVED *(With the following conditions, if any)*

☐ DISAPPROVED *(For the following reasons)*

EXAMINER	DATE	AUTHORIZED ATF OFFICIAL	DATE
	253		

ADDITIONAL REQUIREMENTS

The Chief of Police, Sheriff, or other official acceptable to the Director must complete the "Law Enforcement Certification" below. If the applicant is an individual (including a licensed collector) a recent photograph must be attached in the space provided and FBI Form FD-258, Fingerprint Card, completed in duplicate, must be submitted.

1. PHOTOGRAPH

AFFIX
RECENT PHOTOGRAPH HERE
(Approximately 2" x 2")

2. LAW ENFORCEMENT CERTIFICATION (See IMPORTANT note below)

I certify that I am the chief law enforcement officer of the organization named below having jurisdiction in the area of residence of

_____
(Name of Maker)

I have no information indicating that the maker will use the firearm or device described on this application for other than lawful purposes. I have no information that POSSESSION OF THE FIREARM DESCRIBED IN ITEM 4 ON THE FRONT OF THIS FORM WOULD PLACE THE MAKER IN VIOLATION OF STATE OR LOCAL LAW.

_____
(Signature and Title of Chief Law Enforcement Officer–see IMPORTANT note below)

BY (See IMPORTANT NOTE BELOW)_____
(Signature and Title of Delegated Person)

_____
(Organization)

_____
(Street Address)

_____ _____
(City, State, and ZIP Code) (Date)

IMPORTANT: The chief law enforcement officer is considered to be the Chief of Police for the maker's city or town of residence, the Sheriff for the maker's county of residence; the Head of the State Police for the maker's State of residence; a State or local district attorney or prosecutor having jurisdiction in the maker's area of residence; or another person whose certification is acceptable to the Director, Bureau of Alcohol, Tobacco and Firearms. If someone has specific delegated authority to sign on behalf of the Chief of Police, Sheriff, etc., this fact must be noted by printing the Chief's, Sheriff's, or other authorized official's name and title, followed by the word "by" and the full signature and title of the delegated person.

Form Approved: OMB No. 1512-0025 (12/31/86)

DEPARTMENT OF THE TREASURY — BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

NOTICE OF FIREARMS MANUFACTURED OR IMPORTED

(Complete in duplicate – See Instructions on reverse)

TO: The Director, Bureau of Alcohol, Tobacco and Firearms, Washington, DC 20226

The undersigned hereby serves notice of the manufacture, remanufacture, reactivation, or importation of firearms as required by section 5841 of the National Firearms Act, Title 26, U.S.C. Chapter 53.

1. TYPE OF NOTICE

a. FIREARMS ON THIS NOTICE ARE: *(Check one)*

- ☐ MANUFACTURED
- ☐ REMANUFACTURED
- ☐ REACTIVATED
- ☐ IMPORTED *(If imported complete Items c and d)*

2. PRINT NAME AND TITLE OF PERSON AUTHORIZED TO SIGN FOR A BUSINESS OR FIRM

3. NAME AND ADDRESS *(Include trade name)*

b. NUMBER OF FIREARMS COVERED BY THIS NOTICE *(See Instruction 1.c.)*

FOR IMPORTED FIREARMS ONLY

c. IMPORTATION PERMIT NUMBER *(See Instruction 1.d. on reverse)*

3.a. TELEPHONE NUMBER *(Include area code)*

d. PERMIT EXPIRATION DATE

4. DESCRIPTION OF FIREARMS *(Complete all items)*

DATE OF MANUFACTURE OR REACTIVATION *(If imported, give date released from Customs custody & manufacturer's name) (If remanufactured or reactivated, indicate name of original manufacturer)* a	TYPE OF FIREARM *(Shortbarreled rifle, machine gun, destructive device, etc.)* b	CALIBER GAUGE OR SIZE c	MODEL d	LENGTH *(In.)* OF BARREL e	LENGTH *(In.)* OVERALL f	SERIAL NUMBER AND OTHER MARKS OF IDENTIFICATION *(See Instructions 1.e. and 1.g.)* g

h. ADDITIONAL DESCRIPTION *(Use additional sheets if necessary)*

i. WHERE ARE FIREARMS KEPT?

5. FEDERAL FIREARMS LICENSE

LICENSE NUMBER	TYPE OF BUSINESS	EXPIRATION DATE

6. SPECIAL (OCCUPATIONAL) TAX STAMP

ATF IDENTIFICATION NUMBER	CLASS

UNDER PENALTIES OF PERJURY, I DECLARE that I have examined this notice of firearms manufactured, remanufactured, reactivated or imported and, to the best of my knowledge and belief, it is true, correct and complete.

7. SIGNATURE OF MANUFACTURER OR IMPORTER *(Or authorized official shown in Item 2)*

8. DATE

ATF FORM 2 (5320.2) (3-85)

INSTRUCTIONS

1. Preparation of Notice of Firearms Manufactured or Imported.

a. This form is required to effect the registration of all firearms imported, manufactured, remanufactured or reactivated by qualified Federal firearms licensees who have paid the special (occupational) tax to import or manufacture firearms.

b. Firearms may not be described on attachment sheets. Each must be listed on ATF Form 2.

c. A separate Form 2 must be submitted for the four categories of manufacture, remanufacture, reactivation and importation of firearms.

d. If the importation involves more than one import permit, a separate Form 2 must be filed to report those firearms imported under each permit.

e. Serial numbers—Sections 178.92 and 179.102 of the regulations require that an individual serial number, *not duplicating any serial number placed by the manufacturer on any other firearm,* must be placed on the firearm.

f. Reactivation of an NFA firearm—Any NFA firearm (including the frame or receiver of such firearm) must be registered to the possessor in order to be lawfully possessed. A Form 2 to register a reactivated NFA firearm will not be accepted if the unserviceable firearm is not registered to the applicant. The firearm in that event, would be considered contraband and would be subject to the seizure and forfeiture provisions of the law.

g. If a firearm being remanufactured includes a previously identified NFA frame or receiver, the serial number must be the original serial number, followed by letters identifying the remanufacturer.

h. The signature required on both copies of this form must be entered in ink. Facsimile, photostatic or carbon signatures are not acceptable. Although typed forms are preferred, pen and ink may be used; forms completed in pencil will not be accepted.

i. If any questions arise concerning the preparation of this form, please contact the nearest ATF Office or the National Firearms Act Branch at (202) 566-7371.

2. Where to File Form—Submit completed forms to the National Firearms Act Branch, Bureau of Alcohol, Tobacco and Firearms, Washington, DC 20226.

3. When to File Forms—

a. All firearms manufactured, remanufactured or reactivated during a single day must be filed no later than the close of the next business day. (27 CFR 179.112).

4. Disposition of Form—The manufacturer or importer must prepare the form, in duplicate, file the original with the National Firearms Act Branch and keep the copy with the firearms records required to be retained at the premises covered by the required special (occupational) tax stamp.

5. Receipt of Form by the Bureau of Alcohol, Tobacco and Firearms—

a. The receipt of this form properly prepared and executed by a manufacturer will register the firearms listed on the form to the manufacturer, with the exception noted in item 1f. of these instructions.

b. Timely receipt by ATF of a properly prepared and executed form and timely receipt by the ATF Regional Director (Compliance) of a copy of ATF Form 6a (required by 27 CFR 178.112) covering the firearm(s) reported on the form by the importer, will register the listed firearms to the importer.

PAPERWORK REDUCTION ACT NOTICE

This request is in accordance with the Paperwork Reduction Act of 1980. The information you provide as a qualified licensed firearms manufacturer or importer is to register, as required by law, firearms within the jurisdiction of the National Firearms Act, which have been lawfully manufactured or imported. The data is used to determine applicant's eligibility to register the firearms described. The furnishing of this information is mandatory (26 U.S.C. 5841c).

ATF FORM 2 (5320.2) (3-85)
☆ U.S. GPO: 1985—461-843/36926

Form Approved: OMB No. 1512-0182 (1 31 86)

DEPARTMENT OF THE TREASURY
BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

APPLICATION FOR LICENSE OR PERMIT
UNDER 18 U.S.C. CHAPTER 40, EXPLOSIVES

FOR ATF USE ONLY

NOTE: PLEASE COMPLETE IN TRIPLICATE, USING TYPEWRITER OR BALL POINT PEN

SECTION A (Must be completed by all applicants)

1. NAME (If partnership, include name of each partner)

2. TRADE NAME, IF ANY

3. EMPLOYER IDENTIFICATION NO. OR SOCIAL SECURITY NO. (Voluntary—see instructions)

4. NAME OF COUNTY

5. ADDRESS (RFD or street no., city, State, ZIP Code)

6. LOCATION (If no street address in item 5, show direction and distance from nearest P.O. or city limits)

7. TELEPHONE NUMBER (Include Area Code)

Business ( )_____ Residence ( )_____

8. ARE YOU PRESENTLY ENGAGED IN A BUSINESS FOR WHICH A LICENSE OR PERMIT IS REQUIRED UNDER 18 U.S.C., CHAPTER 40, EXPLOSIVES? (If yes, show date business began)

☐ Yes/Date:_____ ☐ No

9. IS OR WILL YOUR BUSINESS BE: (Check appropriate box)

☐ Individually Owned ☐ A Partnership · ☐ A Corporation ☐ Other (Specify) _____

10. APPLICATION IS MADE FOR A LICENSE OR PERMIT UNDER 18 U.S.C., CHAPTER 40 AS A: (See instructions and check appropriate box)

TYPE CODE	EXPLOSIVES LICENSE	X	FEE
20 21 22	Manufacturer of High Explosives Manufacturer of Low Explosives Manufacturer of Blasting Agents		$50
23 24 25	Importer of High Explosives Importer of Low Explosives Importer of Blasting Agents		$50
26 27 28	Dealer in High Explosives Dealer in Low Explosives Dealer in Blasting Agents		$20
29	Dealer in Low Explosives — Black Powder Only		$20
30 31	Manufacturer (Limited) of High Explosives Manufacturer (Limited) of Low Explosives		$ 5
	EXPLOSIVES PERMIT		
33 34 35	User of High Explosives User of Low Explosives User of Blasting Agents		$20
36 37 38	User (Limited) of High Explosives User (Limited) of Low Explosives User (Limited) of Blasting Agents		$ 2
	PLEASE MAKE ☐ CHECK ☐ MONEY ORDER PAYABLE TO THE "BUREAU OF ALCOHOL, TOBACCO AND FIREARMS" TOTAL AMOUNT		$

11. DURING THE TERM OF THE LICENSE OR PERMIT, THE APPLICANT INTENDS TO MANUFACTURE, IMPORT, DEAL, OR USE:
(See instructions for definitions of classes of explosives)
(Check appropriate box)

☐ High Explosives ☐ Low Explosives (Including fireworks)

☐ Blasting Agents

12. LIST THE TYPES OF EXPLOSIVE MATERIALS YOU INTEND TO MANUFACTURE, IMPORT, DEAL OR USE (e.g., Dynamite, TNT, Black Powder, Fireworks, etc.)

13. IS STATE OR LOCAL LICENSE OR PERMIT REQUIRED FOR EXPLOSIVES OPERATIONS?
(If yes, give numbers, if not obtained, give date applied for)

☐ YES/Numbers or Date _____ ☐ NO

14. DATE OPERATIONS REQUIRING A LICENSE OR PERMIT ARE DESIRED TO COMMENCE:

STORAGE FACILITY DATA (Must be completed if explosive materials will be stored)

Section 842(j), 18 U.S.C. provides "It shall be unlawful for any person to store any explosive material in a manner not in conformity with regulations promulgated by the Secretary." Before applying for a license or permit, the applicant must read and be familiar with the requirements as set forth in 27 CFR Part 55, Subpart K — STORAGE. AN APPLICATION FOR A LICENSE WILL BE DENIED IF UPON AN INVESTIGATION IT IS FOUND THAT STORAGE FACILITIES ARE INADEQUATE.

15. ALL OF THE STORAGE FACILITIES LISTED ON ATTACHED SHEETS, IF ANY, MEET THE MINIMUM REQUIREMENTS AS SET FORTH IN 27 CFR PART 55, SUBPART K — STORAGE (If No, explain on separate sheet)

☐ YES ☐ NO

16. TYPE, LOCATION AND DESCRIPTION OF EACH PERMANENT STORAGE FACILITY (Attach separate sheet(s) — See instructions 1, 11 and 16)

17. TYPE AND DESCRIPTION OF EACH PORTABLE OR MOBILE FACILITY (Attach separate sheet(s) — See instructions 1, 11 and 16)

RESPONSIBLE PERSONS INFORMATION

18. LIST BELOW THE INFORMATION FOR EACH INDIVIDUAL OWNER, PARTNER, AND OTHER RESPONSIBLE PERSONS (See Instruction 9) IN THE APPLICANT BUSINESS. IF A FEMALE, LIST GIVEN NAMES AND MAIDEN, IF MARRIED, e.g., "MARY ALICE (SMITH) JONES", NOT "MRS. JOHN JONES." (If additional space is needed use a separate sheet.)

FULL NAME a	POSITION & SOCIAL SECURITY NO. (Voluntary—see last page) b	HOME ADDRESS (Include ZIP Code) c	PLACE OF BIRTH d	DATE OF BIRTH e

GIVE FULL DETAILS ON SEPARATE SHEET FOR ALL "Yes" ANSWERS IN ITEMS 19 AND 20		YES	NO
19. IS APPLICANT OR ANY PERSON NAMED IN ITEM 18 ABOVE	a. Charged by information or under indictment in any court for a crime punishable by imprisonment for a term exceeding one year		
	b. A fugitive from justice		
	c. Under 21 years of age		
	d. An unlawful user of or addicted to marihuana or any depressant, stimulant or narcotic drug		
20. HAS APPLICANT OR ANY PERSON NAMED IN ITEM 18 EVER:	a. Been convicted in any court of a crime punishable by imprisonment for a term exceeding one year **(Note: The actual sentence given by the judge does not matter — A "Yes" answer is necessary if the judge could have given a sentence of more than one year. Also a "Yes" answer is required if a conviction has been discharged, set aside, or dismissed pursuant to an expungement or a rehabilitation statute.)**		
	b. Been adjudicated as a mental defective or been committed to any mental institution.		

SECTION B (MUST BE COMPLETED AS NOTED)

21. HOURS OF OPERATION OF APPLICANT'S BUSINESS (N/A for user-limited)

TIME	SUNDAY	MONDAY	TUESDAY	WED.	THURS.	FRIDAY	SAT.
OPEN							
CLOSE							

22. ARE THE LICENSE APPLICANT'S BUSINESS PERMISES OPEN TO THE GENERAL PUBLIC DURING THESE HOURS?
☐ YES ☐ NO
(If no, give explanation on separate sheet)

23. LICENSE APPLICANT'S BUSINESS IS LOCATED IN:
☐ A Commercial Building ☐ A Residence
☐ Other (Specify)_____

24. PERMIT AND MANUFACTURER—LIMITED APPLICANTS: PURPOSE FOR WHICH EXPLOSIVE MATERIALS WILL BE USED
☐ Coal Mining (Including construction on coal mining property)
☐ Other Mining Or Quarrying ☐ Agriculture ☐ Construction
☐ Road Building ☐ Oil Drilling ☐ Fireworks Display
☐ Seismographic Research ☐ Other (Specify)_____

25. MANUFACTURER—LIMITED: LOCATION WHERE EXPLOSIVES MANUFACTURED

26. MANUFACTURER—LIMITED: LOCATION WHERE EXPLOSIVES USED.

27. USER—LIMITED: SPECIFY QUANTITY OF EXPLOSIVE MATERIALS NEEDED (Not applicable for fireworks display)

28. PERMIT APPLICANT INTENDS TO TRANSPORT EXPLOSIVE MATERIALS IN INTERSTATE OR FOREIGN COMMERCE?
(If yes, state where)
☐ NO ☐ YES _____

29. PERMIT APPLICANT INTENDS TO PURCHASE EXPLOSIVE MATERIALS IN INTERSTATE OR FOREIGN COMMERCE?
(If yes, state where)
☐ NO ☐ YES _____

30. TYPE 29 LICENSE APPLICANT: DO YOU HAVE A FEDERAL FIREARMS LICENSE? (If yes, show the Federal firearms license number)
☐ NO ☐ YES _____

SECTION C — CERTIFICATION (MUST BE COMPLETED BY ALL APPLICANTS)

31. Under the penalties imposed by 18 U.S.C. 844, I declare that I have examined this application and documents submitted in support thereof, and to the best of my knowledge and belief, they are true, correct, and complete. I also certify that I am familiar with all published State laws and local ordinances relating to explosive materials for the location in which I intend to do business.

APPLICANT'S SIGNATURE	TITLE	DATE

FOR USE OF BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

32. APPLICATION IS
☐ APPROVED ☐ TERMINATED*
☐ DISAPPROVED* *(Fee will be refunded)

REASON FOR DISAPPROVAL/TERMINATION

SIGNATURE OF REGIONAL DIRECTOR (COMPLIANCE)	DATE

$29.95
Printed in U.S.A.

ISBN 0-940401-72-X