by Damien Thorn

Citizens of the computer underground usually have no more substance than a name or handle at the bottom of a message, illuminated on the computer monitors we use for reading electronic mail, Usenet newsgroups, or topical forums on BBS systems and online services. With about 50 megabytes of public messages zipping through the more than 4,000 newsgroups on the Internet each and every day, most people don't spend much time thinking about the person or the face behind the ethereal words of glowing phosphor scrolling up the screen.

HACKING VEGAS

A Summer Conference for the Electronic Underground

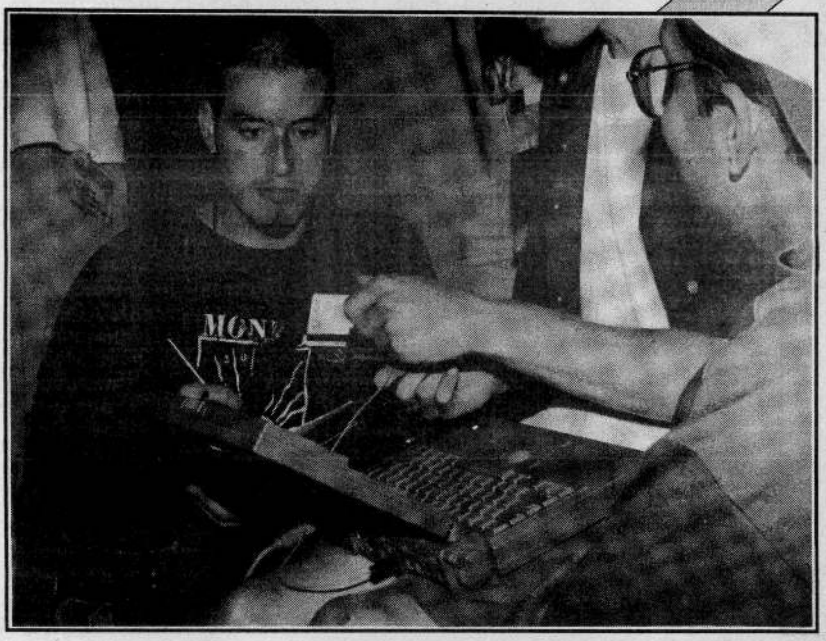
This desensitization toward the human element is typical, and comes as a result of both the quantity of online messages, and the rather cold, flat media itself. Whether it is a press release from the White House or a message from a user of America Online, everything looks the same. Content is the only thing that differentiates one posting from the next, and for people who regularly meet and exchange ideas and information online, this can often leave something to be desired in terms of getting to know people.

Since electronic communication has an impersonal feel by its very nature, some members of the online community have been working to change that in recent years.

The DefCon II conference in Las Vegas this last summer is one such event designed to bring together the media, online luminaries, hackers, and other members of the computer underground. DefCon is an opportunity for faces to be attached to online handles, and an opportunity to foster the growth of online friendships through off-line human interaction, which is especially important for those who spend a great deal of time communicating by modem.

This article essentially recounts my journey to the City of Lost Wages to attend DefCon and meet some of the many people I've read posts from or interacted with in the rushing bitstream of a community that has become known as "cyberspace."

Unfortunately, DefCon and related conferences have sometimes been perceived as nothing more than a group of hackers getting together to discuss new ways of sneaking past the security of computer systems, yet this image is far from the actual truth. Since the Internet makes electronic communication with the other side of the world as easy as talking over a fence to your neighbor, people involved in malicious or illegal activity simply don't come to public conventions to discuss the methods of their crimes. What drug dealer would attend a public conference on narcotics distribution? Digital criminals are probably more adept at using the existing communications infrastructure to disseminate information than the rest of us, and often go to elaborate lengths to conceal their location and identity.



The people attending DefCon II ranged from prominent writers and attorneys to those simply interested in both the cutting edge and the underside of technology. Aside from the social issues, the discussions at these "hacker conferences" are really about pushing technology to the edge.

The attendees want to know more about wireless modems and cellular phones than the manufacturer explains in the manual. They discover that one wireless network encrypts data packets sent over the air, and another network's packets can be "sniffed" from the ether and thus intercepted. These "hackers" have a burning need to understand how things work, just like the rest of us, but on a somewhat grander scale. Sometimes what they discover is more than a little disconcerting.

DEFCON II

DefCon II was the second annual conference held in Vegas to freely discuss technology and computers, and seems to be modeled after HoHoCon — a similar convention held every December in Texas (see "Rising from the Underground" *Nuts & Volts*, Mar. '94). Sponsored by a Washington college student named Jeff Moss who uses the handle "Dark Tangent" online, DefCon's electronic press releases promised to bring together many different factions of the online community, including those who tend to be at odds with one another.

Phil Zimmerman, author of the controversial and widely embraced encryption software known as "Pretty Good Privacy" (or simply "PGP") was scheduled to speak, as was Gail Thackeray — an attorney formerly with the State of Arizona who achieved fame as one of the driving forces behind "Operation Sundevil," a law enforcement effort to close down underground bulletin board systems across the nation.

It was hard to imagine the two of them in the same room: a rather tense-looking attorney general who believes that the government should have the capability to read electronic communications; and the man who developed secure encryption for the masses and gave it away to the world as free software. To say that Mr. Zimmerman is a thorn in the side of investigators like Ms. Thackeray is an understatement.

HEADING TO VEGAS

In a somewhat ironic twist, my guest at DefCon II was the sponsor of HoHoCon. Jesse (known online as "dfx") was in California on a break from touring with his band, so we made plans to meet and fly to Vegas. The opportunity to spend a few days with Jesse and pick his brain proved invaluable in my quest to understand a number of different things.

Although I've learned to loathe the overbooking policies of many airlines, once we actually squeezed on the plane, the flight was uneventful. After a short van ride we picked up our rental car and

headed for the Sahara Hotel, home to DefCon this year. Driving up the strip served as a reminder that Sin City is the convention hot spot of the world, including events of such magnitude as the Consumer Electronics Show and Comdex in the fall.

After stowing our gear, we headed out in search of the convention area. Not coincidentally, it was located at the opposite end of the hotel from the lodging area. This meant a half-mile trek past every eatery, slot machine, and casino area in the hotel. Finally reaching the convention rooms, we noted that there were no rowdy youngsters or people hunched over computers. This was not a good omen, and I began to wonder if the conference had been cancelled.

As we wandered around, I noticed a large sign on a stand near the hallway leading to a conference room. It announced the National Laparoscopists Association was holding a meeting. Brow furrowed, trying to remember what a laparoscope was, I noticed a much smaller sign attached to the wall. One of those black felt-type with little white letters that can be pressed in to place. This one bore the cryptic message "NO MO FEDS." Paydirt. This was the place.

Entering the conference room, we saw a number of people milling around in DefCon II T-shirts, wearing the official clip-on conference badges. A slightly overweight young man sat behind the registration desk with a clipboard and laptop computer. As we introduced ourselves, his eyes widened a bit and he began searching the registration database for our names. Nothing came up, so he had us fill out a form and Dark Tangent came over to explain that some of the registration information had been left in Seattle, but would be faxed over in the morning.

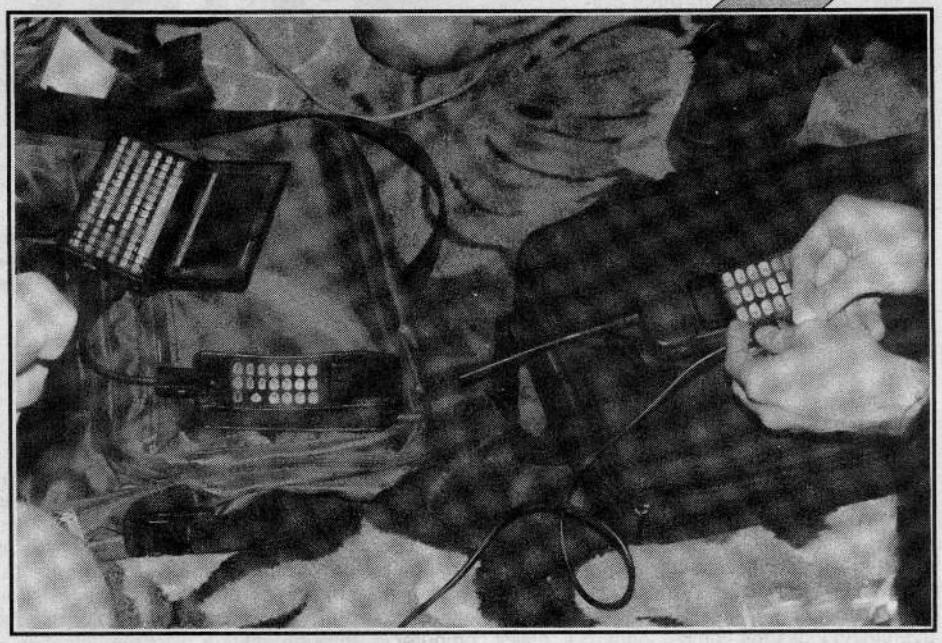
We were given our badges, and noted with amusement that mine had the word "press" superimposed over the multicolor logo under the plastic. Interestingly, you had to use a permanent marker to fill out your own name and organization information on the badges. There was also a blank space for you to write down your E-Mail address.

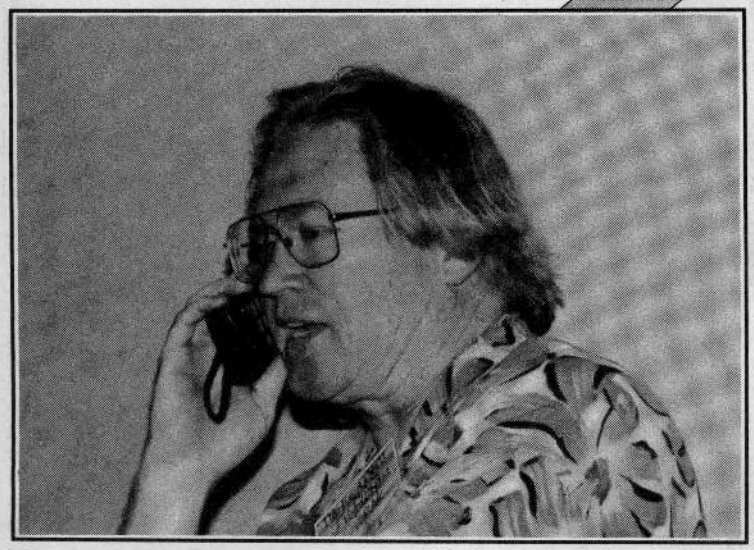
Looking through the convention program, I was amused to note that the convention included an ongoing "Spot the Fed Contest." The basic contest rules were outlined as follows:

"If you see some shady MIB (Men in Black) earphone penny loafer sunglass wearing Clint Eastwood to live and die in L.A. type lurking about, point him out. Just get my attention and claim out loud that you think you've spotted a fed. The people around at the time will then start to discuss the possibility of whether or not a fed has been located. Once enough people decide that there has been an I.F. (Identified Fed) and the I.F. has had a chance to say whatever, an informal vote will be held. If enough people agree, shirts will be passed out."

Basically, the "spotter" received an "I spotted the Fed" DefCon T-shirt, and the "spotee" received an "I am the Fed" T-shirt. Although all done in fun, the contest actually produced results. Whether they're looking for someone, or like the rest of us, are there simply to learn more about the ways technology is being used, there are representatives of various law enforcement agencies in attendance at almost all computer-related events. Most of them choose not to announce it on their conference badges, because people tend not to want to be seen talking to them.

InfoWorld columnist Robert X. Cringley later wrote of the contest, "Silly? Nope. The kids of DefCon smoked-out four flunkies from the super-secret National Security Agency . . . [who] paid their $30.00 registration fee with a check from some bogus veterans organization . . . it was their fanatical support for the Clipper encryption chip and general lack of computer knowledge that really set them apart."





HACKING THE HACKERS

One of the major differences between Summer's DefCon and Winter's HoHoCon is that DefCon's sessions took place on both Saturday and Sunday, with the conference area remaining open virtually 24 hours a day. HoHoCon has a more structured program, with the conference itself taking up only one day. By about 2:00 am on Saturday morning, more people were just arriving to register for the conference.

Standing near the registration desk, I overheard Dark Tangent explaining to a few new arrivals that someone else on the Internet had been posting fake pre-registration announcements. The individual had defrauded a number of people, and Tangent remarked, "They were more professional than me. They actually sent back receipts to the people who had sent money, confirming their registration!"

I was surprised to learn that the mailing address posted in the announcements was located in Merced, CA. Located less than 60 miles from my home town of Stockton, I informed Tangent that this small community was hardly known as any kind of computing hot spot.

At that point, a man in his early forties who had been standing near the registration desk approached me and said, "Excuse me, but I heard you mention that you lived in Stockton. You wouldn't happen to be Damien Thorn?" Not recognizing the man, I somewhat warily confirmed my identity. With a smile, he extended his hand and introduced himself as John Markoff with the New York Times.

Excitement replaced concern as I was finally meeting the writer I had first spoken to some 13 years ago. As a teenager, Markoff had interviewed me and a few other people for one of the first articles on "computer hackers" to ever be published. Coauthor of the book, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Markoff is a journalist I hold in high esteem, yet had never met in person until this point. Our infrequent communications had always been via phone or electronic mail. [For those interested, Markoff's *Cellular Phreaks and Code Dudes — Hacking Chips on Cellular Phones is the Latest Thing in the Underground* appears as a companion article to "Secrets of the Oki 900" in the Dec. '93 issue of *Nuts & Volts*.]

Markoff introduced me to a vaguely familiar looking man who was in the process of filling out his convention badge. It was John Davorak, *PC World* columnist and author of several books. He wasn't immediately recognizable due to his casual dress and the lack of a secret service-like entourage of suited men that normally monopolize his attention and escort him

around industry trade shows where he is paid to speak.

With no activity scheduled to take place in the conference room until the following morning, Davorak decided that he wanted to ride the indoor roller coaster at the MGM Grand Hotel. While I thought it was a bit unconventional, Davorak tends to be like that. His dry sense of humor, lack of egotism, and blunt candor are probably just as important as his insight and knowledge in making him one of the PC industry's leading writers and speakers.

We hit the road and after taking a shortcut that actually seemed to be the long way there, we piled out of Davorak's rental car near the MGM Grand and began the mile-long trek through the casino and food service areas toward the arcade and indoor rides. A pattern was beginning to develop here, and it was opined that the Las Vegas building code contained a floor plan provision that managed to force hotel patrons to walk through every casino and past the entrance to each restaurant in order to get from one place to another.

Arriving at the roller coaster, we found that it had closed several hours earlier. Disappointment best describes my feelings at discovering the falsehood of the urban myth claiming Vegas is the city that never sleeps. Even in the city's largest hotel, attractions and eateries do close down for the evening.

Wandering around the hotel on the way back to the car, conversation turned to the local area network (LAN) that seemed to interconnect all the slot machines and other gaming devices. As gamblers pumped coins into the one-armed bandits, LED billboards displayed an ever-increasing amount of money as potential jackpots grew. It was interesting to speculate about the possibilities when several hundred techno-savvy DefCon attendees would be running around a hotel literally wired for cash. Of course, the casinos were even more abundantly wired with closed circuit video cable which dissuaded any hands-on investigation of the gaming network.

Not having been to Vegas for quite some time, I was impressed by the awesome array of monitors that were a part of the wall in the sports wagering area. What seemed like 50 screens were keeping track of a huge array of sports scores and race results. Wondering how they could possibly gather so much data at once, I asked Davorak where he thought it all came from.

"Probably from an AS/400 minicomputer in the basement," was his flip reply.

THE CONFERENCE

As the conference got underway on the following day, what actually held more of my attention than the scheduled speakers were the small groups of people tinkering with technology around the edges of the room.

Despite being one of the older hotels on the Vegas strip, the Sahara was sufficiently high-tech to have replaced the standard locks on the guest room doors with an electromechanical unit that used a "card key" as an access device. These units, manufactured by Sargent, actually contained a code on a magnetic stripe that electrically unlocked the door when swiped through the card reader on the lock.

As depicted in Photo 1, a group of people decided to explore the technology used by these room key credit cards for the benefit of a writer with *Mondo 2000* magazine. Using a surplus credit card reader that had been interfaced to the serial port of a lap top computer, the group obtained inconsistent results. It appeared that the data was encoded on the magnetic stripe in a format that was not related to standard credit cards.

Meanwhile, the parade of speakers got underway at the front of the conference room. Included was Ray Kaplan, principal of the Arizona-based consulting firm Kaplan, Kovara & Associates which specializes in system and network security in the DEC environment. In addition to being a prolific writer for major computer journals and magazines, Kaplan is regarded as the "grand-daddy of all convention speakers."

Also gracing the convention with his presence was Winn Schwartau, who is considered one of the country's leading experts on information security and electronic privacy. His professional affiliations and accomplishments are far too numerous to list, but can be summed up by saying that when Schwartau speaks, everybody listens. Of particular interest to the audience was Schwartau's discussion of HERF (High Energy Radio Frequncy) guns and EMP/T (Electromagnetic Pulse Transformer) bombs.

These forms of non-lethal magnetic weaponry could conceivably be used to destroy the computer and communications infrastructure of a city, state, or country without the physical destruction and loss of life that accompany traditional methods of sabotage or warfare. In addition to consulting with government and congress regarding these issues, Schwartau has just authored a book that includes a discussion of high-tech warfare. Appropriately entitled, *Information Warfare — Chaos on the Electronic Superhighway*, the volume "outlines almost every kind of informational disaster imaginable leaving the reader to think there may be no way out of the quagmire that is the new information age," according to the book's dust jacket. Further information is in the "Resources" sidebar.

Paradoxically, Schwartau became the victim of a low-tech nightmare during the conference. He awoke early one morning to the sound of an exploding toilet. Although the hotel manager thought he was kidding at first, the maintenance people dispatched to his room did indeed find Schwartau experiencing "the sight and sound of Lake Meade in room 1487" as he so eloquently described the plumbing catastrophe that provided him with his own little tidal wave. In Phrack #46, he colorfully describes the efforts of three maintenance people using wet vacs to "suck up

RESOURCES

Sources of Additional Information

The following contact information is provided to empower and encourage you to seek out more information on the topics and products mentioned in the accompanying article, and do a little exploring of technology on your own.

BACK ISSUES

We made reference to several articles that have previously appeared in *Nuts & Volts* on related topics. These were mentioned to help you obtain more detailed information on those subjects, and allow me to avoid covering the same ground again. Back issues can be ordered directly from the publisher for $5.00 each which includes postage. Subscribing might be a good idea if you don't already . . . then you'll never miss an issue.

Nuts & Volts Magazine
430 Princeland Court, Corona, CA 91719; 909-371-8497

PRETTY GOOD PRIVACY

The freeware public key encryption program authored by Phil Zimmerman is available from numerous online sources. Using gopher on the Internet will show you dozens of sites from which you can transfer the program. Many commercial online service providers also have the program available for download. If you would like to donate funds or equipment to Zimmerman's real-time voice encryption software efforts, he can be reached at prz@acm.org via Internet E-Mail.

UNDERSTANDING COMPUTER VIRUSES

American Eagle Publications offers several books and newsletters about computer viruses, and a CD-ROM containing a large collection of virus samples, mutation engines, and source code. For more information or a catalog, contact:

American Eagle Publications, Inc.
P.O. Box 41401-A Tucson, AZ 85717

CELLULAR TELEPHONE EXPERIMENTER'S KIT

The CTEK interface is available for two Oki phones and their AT&T equivalents. The basic interface kit runs $100.00 and requires a $25.00 adapter cable, depending upon the particular phone with which it is to be used. Supported models are the Oki-900 (AT&T 3730) and the Oki-1150 (AT&T 3760). E-Mail can be sent to info@nw.com via Internet, or write:

Network Wizards, P.O. Box 343, Menlo Park, CA 94026
(415) 326-2060 • (415) 326-4672 FAX

CELLULAR SURVEILLANCE SYSTEMS

Law enforcement agencies can obtain a complete surveillance kit comprised of the Oki-900, CTEK interface, H. P. Palmtop computer and the software mentioned in the article from Tech Support Systems. They also manufacture a briefcase system complete with DTMF decoder and Marantz cassette recorder. A multiple cell unit has just been introduced. Sales of these devices are restricted by federal law.

Tech Support Systems
1040 Hamilton Court, Menlo Park, CA 94025; (415) 325-6691

CONFERENCE INFORMATION

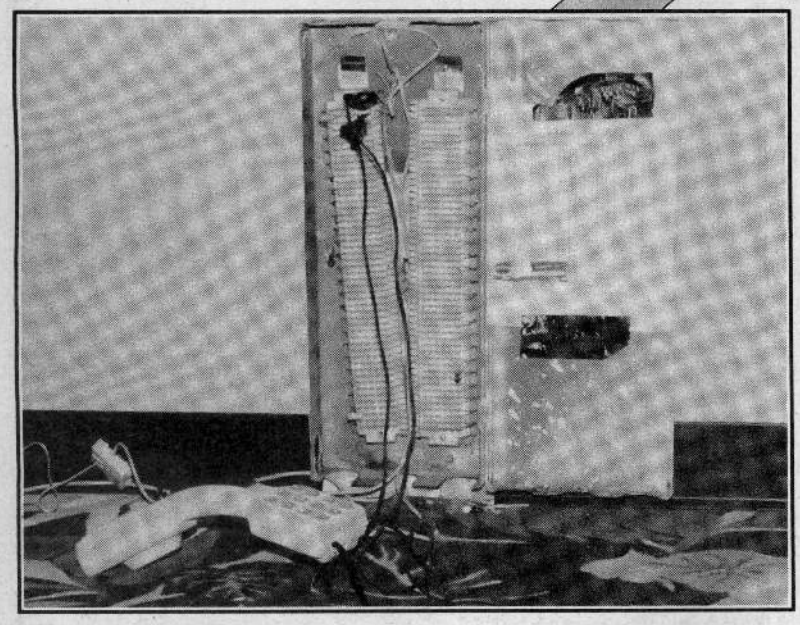
This year's DefCon is already in the planning stages, and organizers are hoping for better Internet connections, A/V live feeds, and virtual reality (VR) demos. If you'd like to attend, obtain more information, or even consider speaking at the convention, send E-Mail to dtangent@defcon.org or write:

DefCon, 2709 E. Madison Avenue #102, Seattle, WA 98112

the Nile River" from his room and the 14th floor hallway.

ENCRYPTION AND SOFTWARE PIRACY

A few new faces turned up at this conference, including Philip R. Zimmerman, a software consultant specializing in cryptography, authentication, and data security.



Mr. Zimmerman is most well known for his role as a leading advocate for public access to strong encryption. He authored "Pretty Good Privacy" (PGP), a free public key encryption software package that has become the world-wide de facto standard for the encryption of electronic mail.

The publication and wide dispersion of this software and its extensive use on the Internet outside of the United States has led to export control problems and conflict with the National Security Agency's desire to restrict the general use of high-quality encryption. Since encryption based on the Digital Encryption Standard (DES) algorithm is illegal to export except under special conditions, Zimmerman is the subject of an ongoing criminal investigation by U.S. Customs.

Zimmerman excited the crowd by announcing that his current project is working towards enabling encrypted voice communications in real-time with consumer-grade equipment such as a SoundBlaster compatible sound card.

Another popular speaker was Peter Beruk, the litigation manager for the Software Publishers Association (SPA). For those unfamiliar with the SPA, this is the anti-piracy group responsible for the "Don't Copy That Floppy" and related advertising campaigns. The Washington, DC based group represents over 1,100 software publishers, developers, and distributors.

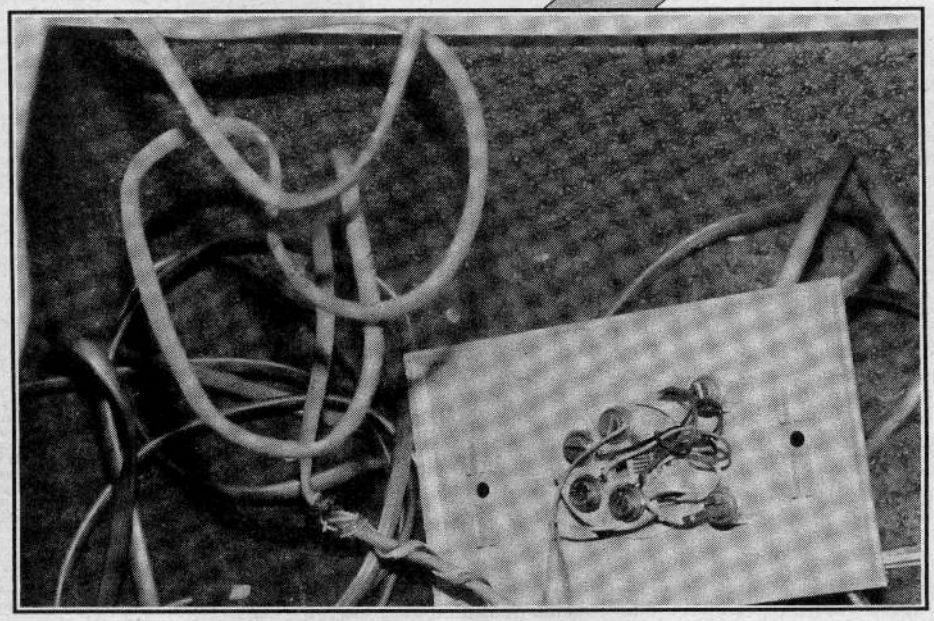
Mr. Beruk withstood a fair amount of derision from the audience, but got the attention of a number of BBS sysops by mentioning that the SPA has a full-time employee that does nothing but call Bulletin Board systems looking for illegal copies of software online. While he would not discuss specific investigative techniques, Beruk did say that the SPA has authorization from various software publishers to upload copies of their software to "pirate" boards in order to gain higher access to the so-called "warez" sections where commercial programs are available for download.

RADIO FREE BERKELEY

Although unrelated to computers, Stephen Dunifer of Radio Free Berkeley attended the conference and spoke about pirate media, fitting in perfectly with his discussion of the controversial topic. Many hams and others interested in radio are probably familiar with Mr. Dunifer. In a nutshell, Dunifer's Radio Free Berkeley is part of a growing movement advocating micropower broadcasting.

Micropower broadcasting refers to the use of low power, inexpensive transmitters to reach local communities on unused broadcast frequencies. It's the "voice of the people," says Dunifer. "In an era of multinational controlled mass media, micropower broadcasting is the voice of the community."

Since DefCon, the FCC has heightened its battle against Dunifer by filing a federal injunction to stop him from broadcasting. With this action occurring last October, Dunifer has vowed to fight the FCC, saying they are infringing his First Amendment right to freedom of speech. Dunifer and his attorney contend that the FCC has created a regulatory process that prevents people without hundreds of thousands of dollars from becoming broadcasters and serving the community. He states, "If a person has money, his voice can be heard everywhere. If a person doesn't have money, he can be heard on the street corner."



Luke Hiken, Dunifer's attorney from the National Lawyers Guild was quoted in *Radio World* on November 16th, 1994 as saying, "You can't even think about [broadcasting] without $150,000.00. The FCC should be facilitating communication between people, not handing it out to the rich." Hiken agrees with Dunifer, contending that the licensing process and minimum requirement of a 100 watt transmitter takes radio ownership away from the people and places it in the hands of a corporate broadcast elite. "Communication is controlled by a small number of billionaires. The American people . . . have no voice on the radio spectrum," states Hiken in the article.

CELLULAR TECHNOLOGY

Plenty of other speakers took the podium and either educated or held a dialogue with the audience about their organizations or specific areas of expertise. The presentations included a demonstration of electronic countermeasures equipment, and Dr. Mark Ludwig of American Eagle Publications, Inc., handed out his award for a much publicized virus writing contest. Although I did not recognize him at the time, Dr. Ludwig's controversial books and virus CD-ROM are apparently quite popular and even advertised in this publication.

Despite the variety of information presented at the conference, my feeling (although biased perhaps) was that the most sought-after knowledge at the convention came late at night, long after the camera crew from a Los Angeles television station had gone home: Cellular communications.

Cellular technology has been gaining large numbers of aficionados, and the Oki 900 has become one of the most popular phones among cellular hackers and experimenters. Evidence of this trend appeared early on. Knapsacks and computer cases were opened up and Oki cellular phones were interfaced to everything from full-size lap top computers to the tiny Hewlitt-Packard palm top systems as shown in Photo 2.

Although street rumor indicates the Oki 900 is no longer manufactured, the popularity of the small phone stems largely from the Cellular Telephone Experimenter's Kit (CTEK) developed by Mark at Network Wizards of Menlo Park, CA. The CTEK is a small box and cable that allow the phone to be controlled by software through the serial port of any PC [see review in the Dec. '93 issue of *Nuts & Volts*].

The CTEK essentially converts standard EIA-232D serial data to the proprietary format required to communicate with the Oki via the

data port on the bottom of the phone. Included in the package is a source code library so that programmers can create their own custom software to control many of the phone's functions. The most popular software being created for the phone are scanning programs which cause the phone to decode the cellular phone numbers and other information from the cellular network's forward control channels.

In addition to being able to display particular mobile numbers, the software can also cause the phone to change frequencies, thus following conversations through handoffs from cell tower to cell tower. A Bay Area company has actually developed a commercial cellular surveillance package that centers around the CTEK interface and an Oki 900 phone, and is sold to law enforcement agencies through distributors such as Tech Support Systems of Menlo Park.

Despite what amounted to a rather large collection of cellular equipment owned by many of the conference attendees, John Davorak opted to use his phone right in the hotel conference room (Photo 3). Although Davorak escaped any problems during his call, others in Las Vegas weren't quite so fortunate.

It seems that a group of people assembled in a hotel room and used test mode commands to not only monitor cellular conversations, but to participate in them as well. As discussed in "Cellular Test Mode Secrets — The Scanner Within Your Phone" (*Nuts & Volts*, June '94), most cell phones can contain diagnostic routines that can be invoked by anyone who knows how to access them. These commands allow the phone to be switched to any given channel, and the conversation on that frequency to be heard through the phone. In addition, the transmitter can be turned on as well.

If a phone is tuned to a cellular channel where a conversation is in progress, and the command is given to turn on the transmitter, then that phone can become an "extension" — allowing communication with the people involved in the original conversation. For various technical reasons, the cellular network will summarily drop the call if the third phone transmits for more than a few seconds.

According to information published after the convention, the assembled group illegally used test mode commands to interject their comments into a number of conversations occurring in the city near the hotel. The targeted conversations included those being held by prostitutes and drug dealers. Several criminal transactions were called off based on the confusion caused by these unwanted participants in what were supposed to be private phone calls.

Although monitoring cellular conversations is a violation of the Electronic Communications Privacy Act (ECPA), and the FCC would no doubt frown on such activity, it's almost enough to make you wonder if cellular hobbyists could unite in order to take a bite out of crime.

PHONES AND PHREAKING

The hotel phone system (PBX) had problems interfacing with the omnipresent computer modems at the conference. In a surprising display of cooperation, the hotel staff allowed a guest-provided terminal block to be patched into a cable running through the conference room (Photo 4) to accommodate dial-up communication. The management simply requested that everything be put back in order at the end of the conference.

Although everyone was generally respectful and well-behaved, the hotel phone wiring was too large a temptation for at least one person. Jesse and I had left the hotel to visit a regular *Nuts & Volts* reader who lived in the area, and upon our return turned on the television.

Because the Sahara has video server technology that allows guests to view their bills on the television, we saw that we owed the hotel more than $20 for phone calls. Not having made any toll calls, we stormed the front desk and obtained a summary of the charges. In the call detail we found entries claiming we had called 801-943-6825 at 10:42 PM for a total of $8.89, 801-575-3845 at 11:17 PM for $7.30, and 619-674-4630 at 11:22 PM at a cost of $5.69.

Since we had left the hotel at 10:00 PM and not returned until after midnight, the calls weren't made by us. Although I found it amusing, Jesse was not happy with the situation and the manager quickly removed the charges from our bill. Returning to our room, we removed the phone jack from the wall and confirmed our suspicion that the cable within each room actually contained several pairs (Photo 5).

We surmised that somewhere in the hotel, our phone line was accessible on one of these extra pairs. Simply rewiring the jack would allow calls to be placed from our extension without requiring physical access to our room or phone.

In a sense, it was a fitting end to another conference dedicated to exploring and experimenting with technology.

There's always someone who wants to exploit technology in order to get something for nothing, and in doing so manages to tarnish the reputation of these conferences for those that attend simply to learn and exchange thoughts and ideas.
NV

TOP SECRET

CONSUMERTRONICS
2011 Crescent, P.O. Drawer 537
Alamogordo, NM 88310
Voice: (505) 434-0234, 434-1778, 439-1776 (orders only) 8AM - 6PM MST, Mon - Sat
Fax: (505) 434-0234 (orders only; if you get voice, enter "#11 #11" any time) 24-hour, 7 days/wk
Free Tech Support: (relates directly to your order or prospective order): Tues. and Thurs. only
10% Off on orders $100+
15% Off on orders $200+
Add $5 total S-H (US, Canada). All items in stock. VISA, MCard OK. No CODs or "bill me"s. New Catalog (150+ offers) $2 w/order, $4 w/o (check or MO) - NO free catalog. NO dealers. Since 1971.

As seen on CBS "60 Minutes," Forbes, etc. By John Williams - former Lockheed Senior Engineer, NMSU Computer Science Professor, NIH Health Physicist.

Wanted: 9 MAC IIci, PC386, portable or better; software; modem electronic test equipment; small parts. Buy or trade.

*All software supports all IBM-PC compatible x86 systems (8086 - Pentium)

Off-the-Shelf Hardware
Van Eck System, Data Card Reader/Writer, ATM2, KX Radar Emitter, Street Sweeper (radar), Lidare, Kidnap/Carjack Foiler, Voice Disguiser, Hearing Assistor, Shriek Module, EM Lab & Countermeasure, TENS, 6th Sense Communicator, Phone Color Box, Lineman's Handset, DTMF Decoder, Bug & Tap Detector/Blaster, Subliminal Mixer/Amp, Levitator, Vortex Generator, Neurophone/Rife/Hieronymus/Resonant Crystal Radionic, Magnetometer, RF & Microwave, Ultrasonic Jammer & Receiver, Infrared Detector, Electronic Dowser, Long-Range Eavesdropper, Noise Cancelling System, Unknown Presence Detector - many more devices. See Catalog.

SPECIAL PROJECTS
We design, build, repair, modify, maintain and-or consult on any device, system, process or project - electrical, electronic, computer, phone, mechanical, optical, automotive. Invention prototyping. Confidentiality guaranteed. Describe and include $25 pre-engineering fee (does not obligate you). Time and cost estimates in 7-10 days.

TECHNICAL RESEARCH SERVICES
Unique 58+K electronic and computer design article database accessed by title and subject: Digital, µP, µC, analog, hybrid, monograph, software. Many hacker, In-house, non-published articles. Provide us upto 25 keys (OK to combine topics), we return list, you select articles. $25 search fee + $1/selection + .25/page + $5 S-H.

AUTOMATIC TELLER MACHINES
ATM crimes, abuses, vulnerabilities and defeats exposed! 100+ methods detailed, include: Physical, Reg. E, cipher, PIN compromise, card counterfeiting, magnetic stripe, false front, TEMPEST, Van Eck, tapping, spoofing, inside job, super-cool, vibration, pulse, high voltage - others. Case histories, law, countermeasures, detailed security checklist, labeled internal photos, figures. ATMs contain up to $250,000 in cash! Recent $350,000 ATM crime spree still unsolved! $39.

CREDIT CARD SCAMS
Cardholders, merchants, banks suffer $ Billions in losses annually because of credit card fraud. Describes every known means of credit card fraud and scams. Protect yourself! $29.

CONS, SCAMS & RELATED SWINDLES
Cons, scams and related swindles fleece Americans of $100+ Billion per year! The most comprehensive survival manual on cons & scams of all kinds - from the classic to hi-tech. Details 100s, their many variations, and countermeasures. Protect yourself! $39.

Beyond VAN ECK PHREAKING
Eavesdropping on VDT and TV video signals using an ordinary TV! Documented in security industry literature. Range up to 1 KM. Plans include both the Consumertronics and the original Top Secret Van Eck designs! $29.

VORTEX GENERATOR
Heat and cool with amazing, simple 3-port device. Uses no moving parts, electricity, fossil fuel, liquid or freon. Guaranteed scientifically sound! Plans. $9.

Order Today! - 439-1776

CELLULAR/CORDLESS PHREAKING
How cellphones operate and are modified. Vulnerabilities to hack attack and countermeasures. Comprehensive info on reprogramming NAMs, ESNs, etc (cloning), control data formats, computing encoded MINs, ESNs, SIDHs, operating systems, PROMs and their programming, forcing ACK, test mode and resets, scanning, tracking, scanner restorations, freq and channel allocations, roaming, ESN and SIDH tables, parts/equipment sources, attendant stations, non-USA bands, health concerns, and the ECPA and critique. Step-by-step descriptions to keypad-reprogram 100+ popular cellphones. Plus complete section on phreaking cordless phones! Much more. Comprehensive, invaluable - 10 times more info than our competitor's $79 manual! $69. (Do Special Projects (above) for up-to-date hardware-software).

PBX HACKING
1000s of PBXs are hacked to the tune of about $8 Billion/yr! While our "VOICE MAIL HACKING" (below) details how VMSs are hacked for "phun" and profit - including VMS methods for hacking PBXs themselves - "PBX HACKING" addresses all other issues relating to PBX hacking, including countermeasures. Can your business or agency afford a $90,000 phone fraud loss (average loss due to hacked PBXs)? As described in Forbes Magazine article. $39.

VOICE MAIL HACKING
How Voice Mail Box systems are used and the specific ways they are hacked. Includes ASPEN, MESSAGE CENTER, BIX, GENESIS, RSVP, SYDNEY, PHONE MAIL, AUDIX, CINDY, CENTAGRAM, SPERRY LINK, EZ, etc. Absolutely required for all users, sysops and security personnel! $29.

PHREAKING CALLER ID & ANI
Details on how they work and dozens of effective ways of defeating Caller ID, ANI, *69, *57, and Call Blocking and *67. Also describes Caller ID, Orange, Beige, Cheese and CF Boxes, ESS, SS7, E-911, various CLASS services, CNA, NON PUB DA, CAMA, DNR, 800-ECR, Diverters, LD Extenders, Centrex - more. $29.

The HACKER FILES
Compilation of 100s of the best articles written (in ASCII) by top hackers & phreakers. Covers every major topic in hackerdom! 3 HD Disks* $59.

Beyond PHONE COLOR BOXES
Dozens phone color boxes described - many circuits. Plus Call Forwarding, Conferencing, Phreak History, Glossary, Diverters, Extenders, Loops, REMOBS, Bridging Heads & Cans, Optocom, 3rd Party and many other non-box methods - more. $39.

ROBOFONE AUTODIALER
Powerful, versatile, menu-driven "Wargames" autodialer lets you dial any quantity (up to 10K) or mix of local-long distance phone #'s in any order, over any length of time, whether busy or answered (your choice) and log the times-commands-results to monitor-disk-printer. Quick-dial directory of up to 600 numbers. BUSY redial options. Direct modem command and control. All Result Codes, including VOICE and RINGING. Optional shell to terminal program upon CONNECT. Exit to menu or DOS (for patching). Manual + Disk* $29.

COMPUTER PHREAKING
Describes in detail how computers penetrate each other, and how VIRUSES, TROJAN HORSES, WORMS, etc are implemented. Dozens of computer crime and abuse methods and countermeasures. Includes disk filled with hacker text files and utilities, and the legendary FLUSHOT+ protection system (Ed. Choice, PC Magazine). BBS advice, password defeats, glossary - much more! Manual + Disks* $39.

SOFTWARE PROTECTION SYSTEM
Unique system that highly discourages costly software piracy while permitting legit archival copies. No known way to defeat. No special equipment required. Simple and automatic to install on your distributed software. Compatible with all other copy-prevention systems. Manual + Disk* $59.

CRYPTANALYSIS TECHNIQUES
Five powerful menu-driven crypto programs (in .COM and their .BAS sources) to analyze, decrypt "secure" ciphertexts. Worked-out examples. Recommended by prestigious "Computers & Security". Manual + Disk* $29.

ROCKET'S RED GLARE
Design and construction of solid-propellant amateur and survival rockets. Emphasis on formulation, manufacture, installation of propellants, motors, igniters, etc. Includes list of commonly available materials, and the design of launch pads and test beds (with schematics). $29. FIREWORKS: How firecrackers (M-80s, blockbusters, cherry bombs), small rockets, volcanos, fountains, sparklers and safety fuses are made and colored. Simple, cheap, common ingredients. $9. Both $36.

Sold for Educational Purposes Only

STOPPING POWER METERS
As reported on "60 MINUTES": How certain devices can slow down (even stop) watthour meters - while loads draw full power! Device plugs into one outlet and normal loads into other outlets. Also describes meter creep, overload droop, etc. Plans $29. THE I.Q. MANUAL: External magnetic ways (applied to meter itself) to slow down and stop watthour meters while drawing full loads. Plans. $19. KW-HR METERS: How watthour meters work, calibration, error modes (many), ANSI Standards, etc. Demand and Polyphase Meters. Other experimental results to slow and stop meters by others. $18. Any 2, $36. All 3, $59.

HIGH VOLTAGE DEVICES
HV device plans: Stun Gun, Taser, Prod, Cane, Flasher, Blaster, Zapper, Audio/RF/Radar Jammer, Jacob's Ladder, Plasma & Van de Graaff Gens., Fence Charger, Geiger Counter, Ozone Gen., Fish Stunner, Plant Stim., Kirlian, more! All plans for only $29.

UNDER ATTACK!
Electromagnetic Interference and Electronic Weapon Attacks cause: Cancer, birth defects, and profound psychological, neurological, cardiovascular and immune system disorders! Destructive to people, animals, plants, equipment! Includes ACTUAL CASES OF EM ATTACKS ON PEOPLE (we investigated)! Includes how to verify and pinpoint EMI and electronic attack sources, and specific countermeasures. $29. EM BRAINBLASTER: Tutorial and plans for powerful ELECTROMAGNETIC WEAPONS and LAB DEVICES. Optimum circuits, freqs, waveforms, duty cycles, intensities. Thorough. $29. Both $49.

RADIONICS MANUAL
Exciting electrical, electronic and electromagnetic therapeutic, diagnostic and preventive devices (mostly experimental). History, descriptions, plans (dozens), availabilities of Radionics Devices from early to modern. While drugs cost $ Hundreds, electricity costs pennies! $29. HEAL THYSELF: Plans for 3 major electronic therapeutic devices of types approved by FDA. $24. EMF & LIGHT THERAPIES: Systematic study of the germicidal properties of EMFs and lights *in vitro* and *in vivo*. Bands include µwaves, 4 IR, 6 visible and 3 UV, using continuous, single-pulse, strobe, random pulse rate and width exposures. $29. Any 2, $49. All 3, $69.

STEALTH TECHNOLOGY
Police radar is fascinating! It also has error rates of 10-20%! Every known error mode - stealth method and material used to minimize radar reflections - tactic and strategy to fight unjust radar tickets (that cost you $100s in insurance and risk cancellation) - methods to detect and jam signals - fully described! $29.

SECRET & SURVIVAL RADIO
Optimum survival and security radio equipment, methods, freq allocations and voice/data scrambling/encoding. Includes small receivers/transmitters, telemetry, antenna optimizations, remote monitoring and control, security, surveillance, and ultrasonic, fiber-optic and infrared commo. 70+ circuit plans, tables. $29.

By an ORDER of the MAGNITUDE
The most comprehensive, hard-hitting, hi-tech survival book ever written! Topics include electronic, computer, commo, chemistry, energy, weaponry, cryptography, concealment, revenge, alarm, disguise & ID change, etc designs, tactics and strategies to survive an increasingly dangerous world. We all face increasingly physically and financially brutal times! Field-expedient use of technology in various threat and conflict environments and scenarios. Comprehensive. $49.

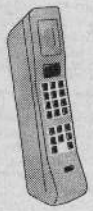
ULTIMATE SUCCESS MANUAL
Underpaid? Harassed or abused? Manipulated? Taken for granted? Stuck in a dead-end job? Can't find a good job? Expect to be laid off, fired or transferred soon? The ultimate no-holds-barred, looking-after-#1 Machiavellian techniques to find, obtain, optimize and keep top jobs, pay and benefits. THE RULES OF THE GAME FOR A GAME WITHOUT RULES! From first resume to CEO. $29.

HARD DRIVE MANUAL
Covers all hard drive and controller implementations (emphasis on PCs). How to select, interface, initialize, set up, use, maintain, troubleshoot and repair them. How to protect them from mistakes, sabotage, prying eyes and sticky fingers. How to recover damaged and lost files. How to prevent crashes. Includes software reviews. Loaded with info, advice, tips. $29. DISK SERVICE MANUAL: Maintain, adjust, align, troubleshoot, repair floppies without special equipment or software. 3.5"/5.25"/8", PCx86, MAC, Apple, Atari, Commodore, etc systems. All floppies need some upkeep. $29. DISK DRIVE TUTORIAL: Theory, practical facts on floppy drives, disks, including many tips, recommendations, formatting, interfacing, FDC, etc. $24. Any 2, $49. All 3, $69.

Your choice has got to be...

M.F.M. COMMUNICATIONS.

for...



CELLULAR PROGRAMMING SOFTWARE



!!! SPECIAL OFFER !!!

Motorola Software

version 9122 & above.

"same product as other top distributors supply"

only **$149**

MPC.EXE **EMPS.EXE**

Please call for other Special Offers & details on our wide range of Software, Programming Services and kits. We can offer you all these services for most phone models.

Call Us Now on... 011-44-88-333-0060

M.F.M. COMMUNICATIONS.

57 Addison Road, Caterham. CR3-5LU. UK.

Prices do not include shipping.

"For Information Purposes Only"

Write in 124 on Reader Service Card.

FLUKE. TEST EQUIPMENT 1-800-90METER

> FLUKE 21-2	MULTIMETER - YELLOW W/ 10A & 300MA	$121.00
> FLUKE 23-2	MULTIMETER - YELLOW W/ HOLSTER	$141.00
> FLUKE 25	MULTIMETER - YELLOW or GRAY	$197.00
> FLUKE 27	MULTIMETER - YELLOW or GRAY	$251.00
> FLUKE 33	CURRENT CLAMP - W/ MIN-MAX	$250.00
> FLUKE 37	MULTIMETER - BENCH / PORTABLE	$270.00
> FLUKE 45	MULTIMETER - DUAL DISPLAY	$625.00
> FLUKE 51	K/J THERMOMETER	$125.00
> FLUKE 52	K/J THERMOMETER - DUAL INPUT	$167.00
> FLUKE 73-2	MULTIMETER - GRAY W/ 10A	$88.00
> FLUKE 77-2	MULTIMETER - GRAY W/ HOLSTER	$142.00
> FLUKE 78	MULTIMETER - AUTOMOTIVE W/ TEMP/RPM	$195.00
> FLUKE 79-2	MULTIMETER - W/ FREQ / CAP / LO OHMS	$175.00
> FLUKE 83	MULTIMETER	$214.00
> FLUKE 85	MULTIMETER	$267.00
> FLUKE 87	MULTIMETER - W/ TRUE RMS	$273.00
> FLUKE 88	MULTIMETER - AUTOMOTIVE	$335.00
> FLUKE 80T-IR	INFRARED TEMPERATURE PROBE	$167.00
> FLUKE 80i-410	A/C - D/C CURRENT CLAMP - 400A	$151.00
> FLUKE 80i-1010	A/C - D/C CURRENT CLAMP - 1000A	$250.00
> FLUKE 80TK	THERMOCOUPLE MODULE	$58.00
> FLUKE T88	AUTOMOTIVE DMM TRAINING PACKAGE	$110.00
> AES-1	SCOPEMETER WAVEFORM SOFTWARE. PKG	$150.00
> FLUKE 97A	SCOPEMETER - AUTOMOTIVE	$2425.00
> FLUKE 93**	SCOPEMETER - FACTORY RECONDITIONED	$1080.00
> FLUKE 95**	SCOPEMETER - FACTORY RECONDITIONED	$1300.00
> FLUKE 97**	SCOPEMETER - FACTORY RECONDITIONED	$1500.00

** COMES COMPLETE FROM THE FACTORY WITH A FULL WARRANTY

VISA & MC ACCEPTED *AUTHORIZED DISTRIBUTOR*

WE STOCK
- √ CARRYING CASES
- √ FLUKE LITERATURE
- √ TEST LEADS & CLIPS
- √ REPLACEMENT FUSES
- √ SCOPEMETER ACCESS.
- √ TEMPERATURE PROBES

WE WELCOME
- √ SCHOOLS
- √ GOVERNMENT
- √ CORPORATE POs
- √ DEALER INQUIRES

FREE UPS SHIPPING+

+ SOME RESTRICTIONS MAY APPLY

GMP Parts Company
8765 Cooperston Way
Elk Grove, CA 95624
(916) 685-1055
FAX (916) 685-3139

Write in 123 on Reader Service Card.

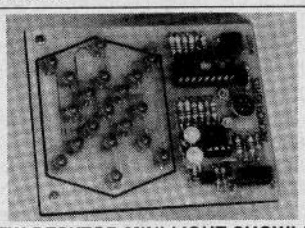
#150 PLANS – KITS – SCHEMATICS *cont.*

CNC DRILL MACHINE SIMPLIFIED. Build a very low cost 12x12 CNC drill machine for drilling printed circuit boards, robotic parts, model airplane and woodcraft projects. Using your computer and drill, cost to build this experimenter's CNC machine is under $300. Detailed plans, schematic, manual, and information that covers all aspects of construction, interfacing and operation. Information includes everything from programming, computer interfaces, X-Y-Z axis drives, steppers to operation. Plans $21 + $4 S/H USA. Send check/MO to CAMTRONICS, INC., 18230 130th PL. NE, Bothell, WA 98011.

VCR BELT KITS! Save big bucks by changing broken or worn belts. Send make, model & $15 to Minute Man Electronics, 37111 Post St. #1, Fremont, CA 94536. Visa or MC. 510-791-5036.

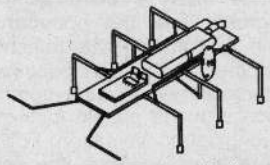
VIDEO GAME cartridge design plans and memory maps for the 8 and 16 bit systems. Explore game design using a C64 or IBM computer. For more information send a SASE. Andrew S. Pakerski, PO Box 86, Thorndale, PA 19372.

140,000 VOLT INDUCTION COIL! Generate sparks so HOT it resembles Thick Purple High-Voltage Fire! Unique H-bridge resonant tank circuit drives ignition coils into self-resonance creating screaming loud electrical flame! Configure two coils for 280,000 Volts Biphasic output! Special precautions required. Easy-to-make. Unbelievable coil energizer plans $8.95, Science plan catalog $1. **B&L SCIENTIFIC,** Box 1054NVF, Duvall, WA 98019.



NEW DESKTOP MINI LIGHT SHOW! Microcomputer controlled, produces dazzling displays. Built-in microphone, circuit responds to sound and music. Eight selectable sound-display routines. Battery operated, based on PIC16C71. Complete kit: $59. Assembled: $69. $3.50 S&H. Phone 818-996-5073. Silicon Sound, PO Box 371694-NV, Reseda, CA 91337-1694.

WANTED WORKING units, plans, kit, schematics for the Code Buster. A device that opens garage doors and gates by randomly throwing out numerous codes. Also looking for working K-band radar unit. Call 1-800-717-0150 between 5:30 PM and 11:00 PM Eastern time only.



WALKING ROBOT. HexWalker six legged robot kit. Basic stamp controlled, servo driven. $125 + $5 S&H North America, $15 all others. Manual only, $10 + $1 S&H (applicable to kit purchase). CA folks add 7.75•. M&T Systems, PO Box 7816, Huntington Beach, CA 92615. Tel. 714-969-3166, Fax 714-969-3167, E-Mail Mandtsys@ix.netcom.com.

COLLINS OPERATING/Maint. Manuals: RT KWM2A + amps 30L1, 30S1. Set $21. R-390A, 51S1, R388 $19.ea (Post Pd.) All schematics included. DMT, PO Box 9064-NV, Newark, NJ 07104.

FREE! THE ETC CATALOG of manuals for Amateur, Audio, and Test Equipment. AG Tannenbaum, PO Box 110, East Rockaway, NY 11518. 516-887-0057, FAX: 516-599-6523.

Robot Kits

✓ Academic-Level Books
✓ Build it Yourself
✓ Action Packed

EASY TO BUILD You do ALL electronic & mechanical assembly using 2-color Instruction Books with step-by-step, well-illustrated directions for assembly, experiments and testing. Each Robot Kit applies different electronic & robotic principles. Learn how Robots work and have fun at the same time!

606A *"Scrambler"* **All Terrain Robot** This 6-legged Robot walks over rough terrain. Uses high-tech infrared beam to sense and avoid avoid objects in its path. 32 page Book. **$37.95**



603A *"Copycat"* **Programmable Robot** Program direction, light and sound using detachable keypad (included) or optional PC. Learn digital logic basics. 44 page Book. **$57.35**

602A *"Blinky"* **Pathfinder Robot** Follows path made with a marker pen or tape. Red/green LEDs react to steering changes, adding fun and interest. 28 page Book. Infrared emitter/detectors. **$36.95**



601A *"Scooter"* **Sound Controlled Robot** Backs up, changes direction, goes forward when it hears loud noise or hits an object. Florescent red. 24 page Book. Fast-paced excitement! **$18.95**

DEPENDABLE PRODUCTS Since 1963, Graymark's ONLY business has been producing educational electronic kits. We do one thing and we do it right. That's why Graymark has the largest selection of electronic kits. And, our *"It works or we fix it"* policy guarantees success for YOU!

ORDER TODAY! ***Phone:*** *VISA/MasterCard/Discover/AMEX*
Mail: *Check/Money Order, Credit Cards*
Add: *$4.00 Shipping*

CALL FOR ***FREE*** 40 PAGE CATALOG

Graymark P.O. Box 2015, Tustin, CA 92681 **800-854-7393**

Write in 122 on Reader Service Card.