APPENDICES

Introduction:
Hackers: Heroes or Villains?
by Gareth Branwyn

Hacking in the Village
"Where am I?"
"In the Village."
"What do you want?"
"Information."
"Whose side are you on?"
"That would be telling. We want... information... information... information."
"Well you won't get it."
"By hook or by crook, we will!"

Remember the '60s TV show The Prisoner? Created by and starring Patrick McGoohan, this surrealist series was basically a platform for McGoohan to explore his own fears of modem surve-illance/spy technology, behavioral engineering, and society's increasing ability to control people through pacifying pleasures.
He was convinced that all this might soon mean the obliteration of the individual (expressed in the defiant opening shout: "I am not a number, I am a free man!"). McGoohan's #6 character became a symbol of the lone individual's right to remain an individual rather than a numbered cog in the chugging machinery of the State. McGoohan, a Luddite to be sure, despised even the TV technology that brought his libertarian tale to the masses. He saw no escape from the mushrooming techno-armed State short of out-and-out violent revolution (it was, after all, the '60s!). As prescient as The Prisoner series proved to be in some regards, McGoohan failed to see how individuals armed with the same tech as their warders could fight back. The #6 character himself comes close to revealing this in a number of episodes, as he uses his will, his ingenuity, and his own spy skills to reroute #2's attempts to rob him of his individuality.

cybernetic range as data rustlers for hire, ultimately sad and alone in their harsh nomadic world. They are both loner heroes and bad assed predators of the law abiding cyber citizenry they burn in their wake.

I don't think I need to tell readers here what impact Gibson's fictional world has had on fueling hacker fan-tasies or what potent similarities exist between Gibson's world and our own.

Like the cowboy tales of the wild west, the myth of the hacker as cowboy is undoubtedly more image over substance (as are most of the myths we will explore here), but there are some important kernels of truth: a) hackers are often loners, b) there are many nomadic and mercenary aspects to the burgeoning cyberspace of the 1990s, and c) it is a wide open and lawless territory where the distinctions between good and bad, following the law and forging a new one, and issues of free access and property rights are all up for grabs (remember the Indians?). Not surprisingly, Electronic Frontier Foundation co-founder John Perry Barlow (a Wyoming cattle rancher himself) chose frontier metaphors when he wrote his landmark essay "Crime and Puzzlement" (Whole Earth Review, Fall 1990). The first section of this lengthy essay, that lead to the birth of the EFF was entitled, "Desperadoes of the DataSphere."

The Hacker as Techno-Terrorist

When I was a budding revolutionary in the 70s, with my Abbie Hoffman and Jimi Hendrix
posters and my cache of middle class weapons (.22 caliber rifles, .12 gauge shotgun, hunting bows), 1, like McGoohan, was gearing up for the Big Confrontation. With a few friends (who seemed more interested in firearms than revolutionary rhetoric), I used to do maneuvers in the woods near my house. We would fantasize how it was all gonna come down and what role we (the "Radicals for Social Improvement") would play in the grand scheme of things. It doesn't take a military genius to see the futility of armed force against the U.S. military on its own turf. The idea that bands of weekend rebels, however well trained and coordinated, could bring down "The Man" was pure romance. Part of me knew this the same part of me that was more interested in posture than real revolution and in getting laid more than in fucking up the State. My friends and I were content to play act, to dream the impossible dream of overthrow.

One of the first "aha's" I had about computer terrorism in the late '80s was that the possibilities for insurrection and for a parity of power not based on brute force had changed radically with the advent of computer networks and our society's almost complete reliance on them. There was now at least the possibility that groups or individual hackers could seriously compromise the U.S. military and/or civilian electronic infrastructure. The reality of this hit home on November 2, 1988, when Robert Morris, Jr., the son of a well known computer security researcher, brought down over 10% of the Internet with his worm
(a program that self propagates over a network, reproducing as it goes). This event led to a media feeding frenzy which brought the heretofore computer underground into the harsh lights of television cameras and sound bite journalism. "Hacker terrorists," "viruses," "worms," "computer espionage"...all of a sudden, everyone was looking over their shoulders for lurking cyberspooks and sniffing their computer disks and downloads to see if they had con-tracted nasty viruses. A new computer security industry popped up overnight, offering counseling, virus protection software (sometimes with antidotes to viruses that didn't even exist!), and work shops, seminars and books on computer crime.

Behind all these lofty notions lies the tedious and compelling act of the hack itself. Hacker-monikered "The Knightmare" presents his complex view of hacking in Secrets of a Super Hacker. In this classic hacker cookbook, the author has gone to great pains to explain the massive width and breadth of hacking, cracking, and com-puter security. With Sherlock Holmes-like compul-sion and attention to detail, he presents the history of hacking, the how-tos of hacking, the legal and ethical issues surrounding hacking, and his own personal reasons for hacking. Numerous examples and "amazing hacker tales" take the reader inside
each level of the hack. Reading Secrets will change the way you look at computers and computer se-curity. It has already been very valuable to me. I am a smarter computer/net user now and. much more attuned to computer security.
When Patrick McGoohan conceived of The Prisoner he wanted to create a show that would de-mand thinking. He wanted controversy, argu-ments, fights, discussions, people waving fists in his face. You might love the show, you might hate the show (or both), but you would HAVE to talk about it. Computer hacking and the wooly frontiers of cyberspace are similar domains of controversy. In the true spirit of freedom of information, Secrets of a Super Hacker is being made available to anyone who cares to read it. It is my hope that it will help keep the debate alive and that those who make use of its privileged information will do so responsibly and without malice.

Be Seeing You,
Gareth Branwyn August 29,1993 Nantucket Island, Mass.

PART ONE
BEFORE THE HACK

Page Intentionally left blank

"Given that more and more information about individuals is now being stored on computers, often without our knowledge or consent, is it not reassuring that some citizens are able to penetrate these databases tofind out what is going on? Thus it could be argued that hackers represent one way in which we can help avoid the creation of a more centralized, even totalitarian government. This is one scenario that hackers openly entertain.
Tom Forrester and Perry Morrison in Computer Ethics

Chapter One:
The Basics
Reading vs. Doing

There are two ways to write a book about computer hacking.
The first is to write an encyclopedic account of every known system and its dialup numbers, passwords, loopholes, and how to increase one's access once inside.

system before you make the first call. If it really is a top-secret database, it's reason-able to assume that your call will be traced, or at the very least, will arouse suspicion. As a novice one tends to get excited with one's first big break -and tends to do stupid, dangerous things. You may not yet have the expertise to alter phone company data, or call from a pay phone, or in some other way make it seem like you are not the person placing the call. The rookie who calls a number of this kind after doing a bit of research might be taking a stupid risk, but that's a few steps higher on the professional hacker's scale than the one who calls without any preparation at all. That's just be-ing stupid, period.

So, as far as targeting is concerned, you may not want to follow up that first big lead right away. It may be preferable to wait awhile, until you have the expertise to do it properly. If you know some-thing about a system no one else knows, it's very likely going to remain a secret unless you spill the beans. If you try to act on your inside knowledge and fail, you are ruining your chances of getting in later, as the system managers might see their mis-takes and correct them.

My word of caution is this: Don't get in over your head. Get familiar with floating on your back before trying to scuba dive for sunken treasure or else you may end up being the one who's sunk.

Targeting also involves other research. What if you do have some exciting secret that will let you get in somewhere? Perhaps you should think about the best way of reaching that system in the first place. For instance, if the system you're seeking is on the Internet, you would have to determine a way to access the Internet disguised as someone else before you could proceed to your main goal.

If you are enrolled at a college, or live near one and have access to your own Internet computer account, it is a trifling matter to log in as yourself and, from there, attempt to connect to other systems. It's not only trifling - it's dumb! Regardless of whether you have mischief in mind, it's irresponsible and lazy to do hacking logged in as yourself. Before you can move out of the few directories allowed by your minimal access level, you will have to figure out a way to disassociate yourself with what you do. That is - and I can't repeat it enough - you will have to find a way to connect as somebody else, and through that connection go on to bigger things.

Breaking into major league computer systems is very often a matter of, first, personal hacking, and second, institutional hacking. That is, first you hack a person (figure out a way of masquerading as that person), and then you hack the institution (figure out a way of disguising that person as a legitimate user of the protected system).

Time, money and effort can be spent needlessly on attempts to access systems that ultimately turn out to be dead ends. Maybe your target is a school's computer, because you want to change your grade from an F to A. You may think your target individ-ual would be the dean or some other school head, but as it turns out, in many instances you would be wrong. School heads often have little or no access to the computers which hold grades, unless they themselves teach classes. In this case you would want to target a professor or more likely, a teaching assistant (T.A.). They're the ones who have to do the actual inputting of grades. Consequently you would want to research the professor or T.A. to get a handle on what their passwords might be.

Then there's the matter of the computer. Which computer should you target for your hack? Teach-ers, especially in math and computer science courses, will usually tell you their computer ad-dress so you can send them e-mail. But that isn't necessarily where you need to go to change your grade. More likely there is

Keep in mind that I read this document from a public terminal, without having to log in as any-body. It was accessed from a public information system. It is information available to anybody, and look at the wonderful clue it holds for all who see it! Now, when I read this I didn't know what Net 19 was, but I knew immediately to target all efforts to finding that system and penetrating its security. This is an example of accidentally found knowl-edge being put to good use. But don't forget - I was reading through every publicly available document for the SOLE PURPOSE of breaking into the system. The specific bit of information I found was accidental, but my finding it wasn't.

In a way, doing this kind of on-line research -exploring every inch of the system available to you before going after the private regions - is a kind of targeting. If your goal is a specific private computer system, target all public systems related to it before you begin. This can only help you in the long run. It might lead to helpful hints, such as the mention of Net 19, or it might at least familiarize you with various aspects of the system.

Things you should be looking for when you target a public system in this way, with the intent of going after a correlated private system, are: how it handles input and output; if any bugs are present and how the system reacts to them; what the com-mand format is (three letters? control sequence?) and what kinds of commands are available; and machine specifications and hardware. Of course, there are numerous other things you should either be looking for, or will unconsciously be picking up anyway as you look around, like what the visual display is like and how long it takes the computer to process commands. These are things that will be helpful later on, because when you actually are trespassing, you won't want to spend hours trying to find the help command or how to log off.

Targeting may seem not just trivial, but dis-tracting as well. After all, a scientist can analyze a rainbow us-ing specific technical terms that explain what a rainbow is, how it is formed, and why it displays its colors as it does. But in a way, this

complicated description of a rainbow is completely unrelated to the rainbow being described. The ex-planation ignores the beauty of it. The techno-jar-gon shuns the poetic connotations that we associate with the rainbow we are so interested in describing.

You may use similar arguments to complain that targeting and pre-thought and planning of hacking attacks distract from the pleasure of the hack itself. If you are a hired hacker you will need to get the job done if you expect to get paid. But otherwise, why should we bother to discipline our-selves with such nonsense as targeting? You're right! Certainly you're correct! There is no reason to feel obligated to apply these suggestions that I pre-sent. There is no pressing need to think carefully about what you do before you do it, but you should be aware of these things as you start. At least, if you break the rules, you should understand how following them might have helped.

Targeting specific computers that hold interest to you, and that you are sure hold the information you seek, and targeting people who have specific access levels and abilities - all of this is like ana-lyzing a rainbow and ending up with nothing but gobbledygook. But in the long run, if you really want to end up at a position further from where you started, if you want to hack for the enjoyment of it and maintain high pleasure levels throughout the endeavor., I suggest you do these things. They will help lessen the amount of frivolous searching and brute-force monotony needed to get in, and will help you stay out of trouble. So, set up a gen-eral plan of action.

You can very carefully tape a ripped disk back together with thin transparent tape. Make sure to only put tape on one side at a time. Once you've gotten all the data you can off one side, you can remove the tape and repair the other side. As be-fore, it is imperative that you don't let the tape get onto the side of the disk which the drive will be reading, or you could throw off your drive's read/write head, and may get sticky stuff on it, too.

Imperfections

If a disk looks okay, but will only give you "Read Errors," it is probably physically damaged on a microscopic level. It may have little holes or dents in it, imperfections that are too small for the naked eye to see. You can push past bad spots on a disk by manually rotating the disk inside. If the damage is limited to a small area of the disk, it may be that the damaged segment is the part the drive tries to read first. If you manually rotate the disk a little to the left or right, the new section of disk which you reveal may not have that damage and may there-fore be readable. Keep rotating the disk, a little at a time, until you've found a spot that is readable.

If you never find a readable spot, perhaps you've been duped! Maybe the disk is blank, or it isn't suitable for your computer. Or maybe it's single sided and you've inserted it with the wrong side facing the drive's read/write head.

A disk that you find in the trash bin may hold corporate data, proprietary software, maybe even a tutorial or simulation like we discussed earlier.

You never knew there was an archaeology side to computer hacking, did you? But that's exactly what all of this is; we are looking into people's lives to see what they think about, to find out what's important to them, and to learn from their experi-ences. Hacking a damaged disk that you have unearthed from a trash bin will lead you to details you would otherwise never have imagined existed. I highly recommend the exercise for the thrill value, and for the intellectual workout to be gained from this pursuit.

Examining Screenshots

The photographs of computers you see in books, magazines, system documentation, promotional literature such as posters and pamphlets, government publications and booklets, as well as the pictures of computers available on television documentaries, news shows and commercials -can all contain valuable hacking information.

Computer photos might show just the screen (or monitor), or the entire computer, including keyboard, CPU and accessories. Or the picture might depict an actual computer in its natural envi-ronment with perhaps an operator visible.

The first group, essentially "screenshots," can be helpful in showing you what it looks like to be in-side a particular system that you have never really accessed. This can clue you in on what accessing style the system uses, if the password is displayed on-screen as it is typed, username and password styles, what features are available, and much more, depending on what the photographs are attempt-ing to illustrate. Similarly, in user manuals and other instructional aids, drawings of screens are often found containing the same information, also default login codes, text specifics, error messages, and other handy stuff.

Knowing error messages and knowing the lay-out of the screen will make you a more believable system administrator or low-level user when you attempt some of

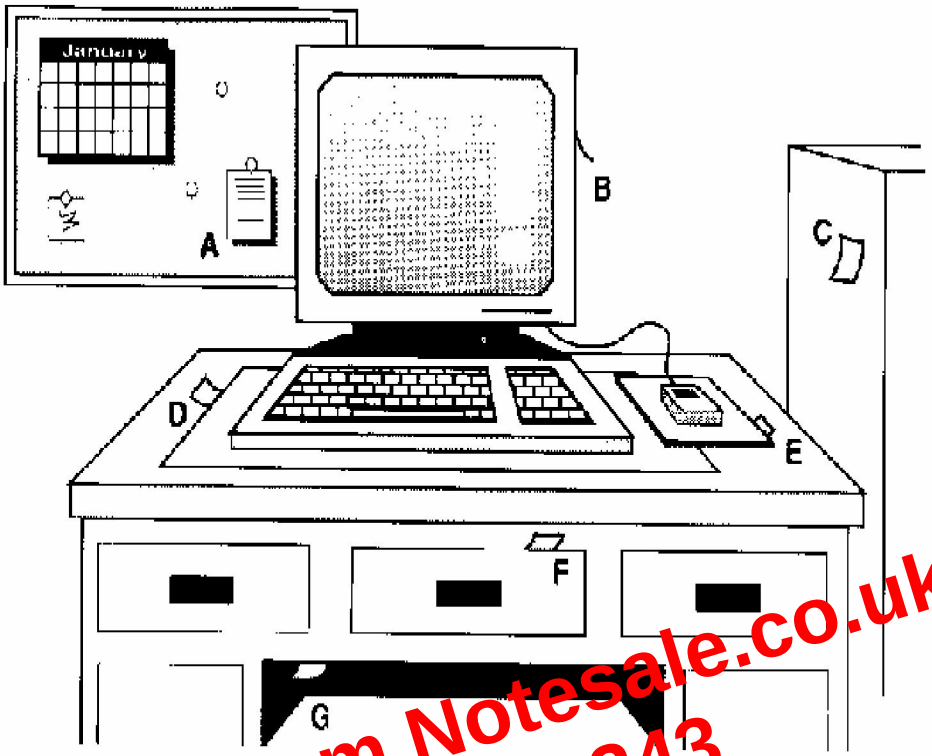

Figure 3

Secret information that must be used every day (such as access codes) is oftenfound hiding on little scraps of paper:(A) on a cork board, (B) attached to the side or top of the monitor, (C) on nearbyfile cabinets or other furniture,(D) under blotter, (E) under mouse pad, (F) in desk drawer, or (G) underneath the the desk.

decade-old literature from a defunct computer users group, programmers' guides, and other stuff. This wasn't all necessarily useful for hacking pur-poses, but it was interesting to read. And it was in-teresting to rescue it from its dusty box on the top shelf of a closet.

In that same building I found a little room whose door was closed and had four signs attached to it. The first, formal and engraved said, "Computer Room." The rest were menacing, either hand lettered or printed by computer: "Keep this door locked at all times!" "For authorized persons ONLY!" And lastly, another stem reminder, "ALWAYS lock this door when you leave!" Needless to say, the door was unlocked.

Inside there was a huge and informative operating system reference manual and two PCs, each of

which had modems. From surfing the hard disks on one of those computers, I found that the termi-nal program was set up with script files <A "script" is a file that you use with a terminal program. You set up the terminal program so that when you log onto a system, the contents of the script file are sent to that system.

So if you have to go through some long and convoluted login procedures, you can put the commands into a script and have the computer automatically log in for you. This is handy, both for legitimate users, and for hackers who happen to gain access to those script files.> that contained phone numbers, passwords and other login procedures. Always look for such things when you snoop.
Snooping can bring to you those tutorial and simulation disks, as well as damaged disks, trash

and insider literature which one can only get from either being employed by a company, or by snooping around. It adds a bit of physical excite-ment to the usually passive art of hacking, and it gets you away from the eyestrain of computer screens for a while.
It is not always necessary to research before a hack, but it is always helpful. Research in any form doesn't have to be undertaken with a particular hack in mind. Like my random snoopings of the torn-apart building and the university lounge, general explorations can lead to fruitful information. In other words, all hacking doesn't have to be done on computers. There is also such a thing as the person who hacks -joyously -life.

Chapter Four
Passwords And Access Control

Three dominant classes of access control have developed to protect computer installations.
They are:
• knowledge-based controls (passwords)
• possession-based controls (keys)
• controls based on personal characteristics (biometric devices)
Possession-based controls have to do with things the user owns, like a physical key or mag-netic card. Sometimes there is a metal clip of a pe-culiar shape that must fit into a hole in the com-puter before the computer will operate. A "key" could also be an identification badge, or a signed letter from a person of high status in the company, granting permission to access a site.
Biometric devices are those which look at some trait of a potential user and compare it to traits previously recorded, such as fingerprints, signa-ture, or geometry of the hand.
These two forms of computer security may be designed for remote access control, although usu-ally they are implemented at the site where the computers are located to limit access to either the computer room or the computer itself. Thus, de-scriptions of biornetric and physical keys will be further developed in the on-site hacking section of this book.
The first class of access control - also the most common - is knowledge-based. That is, control is limited to those persons who can prove they have knowledge of something secret, usually a pass-word. Discovering that password constitutes a large portion of hacking. Here, then, is everything you need to know about passwords: how they work, how they are stored, and how they are bro-ken.

Passwords

security-aware person changed his or her number. Sure, ten thousand is a lot of numbers to try, but it's certainly not impossible. A touch-tone auto-dialer can phone

through all of those in about seven minutes, given unlimited PAC-entry retries per phone call. In any case, I'm using this story to illustrate the principle of least resistance: Users are not going to go out of their way to change access codes if they don't have to. And even if they do, it doesn't matter much. After all, we are hackers.

Let's move back to our discussion of non-random passwords which are generated by computer; or rather, passwords decided upon by the programmer or administrator and selected from data files by the computer.

Computers will select passwords any time a large number of passwords must be assigned at once. During the first week of a college semester, thousands of new accounts must be created for students enrolled in computer classes. For the most part, these accounts are going to be set up with username equal to some truncation or bastardized form of one's real name, and the password will be either one's Social Security number (SSN) or student ID number.

So if you want to hack a college system, start early in the semester - before those passwords get changed by the user to something more secure. Social Security numbers may be easily hacked by brute force, especially when you know how they are distributed.

Social Security (or other ID numbers) may also be obtained through social means (see the chapter on Social Engineering) or by other forms of chican-ery. I've sat in on college classes where the instruc-tor hands around a sheet of paper, on which the students are asked to write their name and ID number. This sheet is then handed to the teaching assistant, who enters this information as accounts into the computer system. If you have to find some classes that operate like this, make sure you sit in the back of the class, where nobody will no-tice you copying other people's private data. A hand-held scanner/copier makes life easier at times like these.

You can also get names and SSNs from atten-dance sheets, or class rosters, which usually list both pieces of information for every individual in the class. If the professor doesn't make the roster available for student perusal, make up some excuse to swipe a look at it. For instance, say the registrar had your name incorrectly spelled on your last transcript, and you want to make sure they've corrected the problem. Professors will love any excuse that points out slip-ups in the bureaucracy of the school system. Use their mindset against them!

Several court battles have ruled that use of one's Social Security number in conjunction with one's name in a public environment is unconstitutional, as it is an invasion of personal privacy. Therefore, we may see a trend starting, with SSNs getting used less and less for identification purposes, and an organization-defined ID number being used in its place. If that's the case, you will have to rely more on brute force to access the array of ID numbers assigned to a person.

Pre-usage passwords won't always be Social Security numbers or other ID numbers. If some non-computer communication is possible between the sysadmin and the user, other words may be as-signed as temporary passwords (to be changed when the user logs on).

There might be a generic "new user" password which is given to all accounts, which shouldn't be very hard to crack. Or the password might be something very obscure

computer department (from your home or wherever) and this is the conver-sation that follows:

PERSON ON OTHER END: "Hello; Jack Chipper, Computing Department. "

YOU: 'Hello, Jack, this is Gary Harris from the Researching Department. Maybe you could help me
with a problem?'

JACK: 'Maybe... What is it?"

YOU: "Well I'm the first one here, and I can't seem
to get things started up. Will you talk me through it?"

JACK: 'Sure. You by your computer?"

YOU: 'Yes."

JACK: 'Okay. Turn on the red switch on the floor.
You see it there?'

YOU: 'Yes, okay. I see it... Okay.

JACK: 'It'll take a few minutes for everything to boot up.

YOU: "To what?"

JACK: 'Uh, boot up. I mean, it'll take a minute or two for the computer to set itself, to get ready to use.

YOU: "Okay, it stopped.

JACK: 'What do you see?

YOU: "Just what you always see. It worked up to
here fine before, but after this, it didn't work. What do I do when it doesn't work here?

JACK: "What do you usually type?"

YOU: 'I don't know. This is my first day here. I'm just a temp - they said someone would tell me!

JACK: 'Okay, press Enter.

YOU: "Enter... Okay.

JACK: 'Now type 'TEMP'spacebar 'PUPPY."'

YOU: "Okay... Oh!"

JACK: "See?

baby.'

RECEPTIONIST: "Just read the number off your ID badge.

YOUR RESPONSE: "I didn't get my badge yet there was some mix-up or something. My supervisor said
she would give it to me tomorrow, maybe. You know how it is, no one knows what
they're doing, and all that..."

RECEPTIONIST: "Who's your boss/supervisor/manager?

YOUR RESPONSE: "M_____,Do you know any-thing about him1her? "

(You should've done your research, so you should know the answer to this sort of question. If you don't know and it's a large company, or a large building, you can try either answering with a false but common name, or try the old, "Uhm.... Something with an 'S' - Schindler? Schindling? Schiffer? Schifrin?")
Here's a different situation:

RECEPTIONIST: "But I don't have a computer!"

YOUR RESPONSE: 'I'm sorry. I must've dialed wrong. Is M available? '

(M_____,is the name of the receptionist's boss.)

If you can manage to work in some company news or personal tidbits in an unobtrusive way, then do
so- if the person you're speaking to seems friendly. This is just another way of gaining credibility points.

YOU: "Sorry, I didn't hear that last thing you said. It's really loud here with that construction they're
doing next door."

YOU:"By the way, does M have a kid in the Little League? My son has a friend named

Note that for maximum benefit, credibility questions, should be worked in before asking about login procedures.

Miscellaneous Social Engineering Tips

To improve your chances of getting in with social engineering, here are some tips. Notice how the person you speak to reacts to your questions. If you speak to a receptionist or other worker on the bottom of the pay ladder, he or she may not want to chit chat or fool around with computers if he or she's being monitored, or if calls are being screened by the boss.

While your name was, luckily, not on that stolen tape, there is still some threat to you. As of now we are uncertain whether any users with programmer-level computer access were backed up on the stolen tape. Therefore, we request you fill out this application and mail it back immediately in the postage paid envelope provided.
Fill out the form and return it to us as soon as possible. Once received, we will update you to this new, secure ID.
Thank you for your cooperation, and to offset any trouble this may cause you, we will be subtracting 75% off your August bill.

Name

Address

Zip

Day Phone(_)

Night Phone(_)..-

Old (Invalid) Password

New (Updated) Password

PinkyLink, America's Largest On-Line Information Service, guarantees that the above personal data will be inputted no later than September 1, 19--, (following verification), and will be kept confidential before and after such time.

Please keep a copy of this for your records.

Imagine Joe User gets this letter in the mail. It looks authentic, having the logo and letterhead of the service, and arriving in a metered, typed en-velope. But will Joe believe that PinkyLink actu-ally sent this to him?
The whole situation is preposterous! Any real life computer service with a password problem would require that all password updating occur on-line. It's simply the cheapest and easiest way to update hundreds or thousands of pieces of user information. Still, when Joe User looks at this letter, he will notice that he isn't in immedi-ate danger as some other users of the system are; unlike those other poor losers who got their passwords stolen, Joe doesn't have to be con-cerned that he'll start getting huge bills in the mail from the criminal charging system usage to Joe's account.
And what about that 75% deal at the bottom? That makes Joe twice as likely to respond to the letter. Not only does he have a responsibility to himself to make his account secure again, he has a responsibility to the database: if they were nice enough to warn him of this and pay him for it, the least he can do is comply with them. And the return envelope is postage paid!
Of course, PinkyLink probably has an on-line way for users to change their password, but you don't have to mention that when you write a letter like this.
Remember, the style is more important than the wording of the letter. Before you send out something like this, be sure to look at real examples of PinkyLink's correspondence, to get an idea of the kind of paper and printing used, sizes of fonts, coloring, etc.

consequently, the following discussion is based mostly on the computers found there.

71

Computers for the use of the general public are available now at most public and academic librar-ies. They fall into three groups:

- CD-ROM databases and information computers,
- public access terminals, and
- general purpose microcomputers.

Let's look at each one of these in turn, and see how these can help the hacker help himself.

CD-ROM Databases And Information Computers

CD-ROM databases, like InfoTrac and News-Net, are computerized listings of periodical articles, updated monthly. Other databases are available with slants toward business news, census data and the like. Some libraries have CD-ROM encyclope-dias, and many government depository libraries will have databases listing government publica-tions available.

In a similar vein, I've seen libraries with com-puters (usually Macintoshes) set up with user-friendly programs designed to teach patrons how to use the library and to dispense other helpful advice. All of these computers are useful to the hacker only for the information they carry, due to the fact that they are set up on independent ma-chines, without modems, and without access to telephone lines. They usually serve the single pur-pose of dispensing information on their specific topic.

Finally - this is rare and a bit odd, but occa-sionally you will see a computer being used as a "register". As people walk into the computer room, office, or wherever, they sign into the computer with a name and ID number, and perhaps answer a few questions about themselves. The purpose of this sort of computer setup is to keep a timed and dated record of who uses the public facilities. Of course, unless a light pen or graphics tablet is used, signatures can not be collected and so their use for security purposes is lost.

Unlike databases and tutorials, there is a bit more you can do hacker-wise with a guest record computer, though not much more. One application might be to use the computer to see who else has been using the facilities. This information could be helpful if the facility in question is a computer room. You might be able to find exploitable patterns in computer usage by certain individuals, or an overall tendency for less people to be in the room at certain times, both of which are helpful to know, as we will see.

If the guest register program itself doesn't let you see who was there before you, try exiting out to the operating system and checking for relevant data files. This will be discussed in the upcoming section on general-purpose micros.

Access to CD-ROM databases and information computers is not usually of much use to the hacker. There are exceptions of course, and it's well worth investigating any computer of this kind that you find.

Public Access Terminals (PATs)

times the sum of the alternating digits (starting with the separated digit to the left of the bar code), minus the sum of the remaining digits. The check digit is the last digit in your answer.

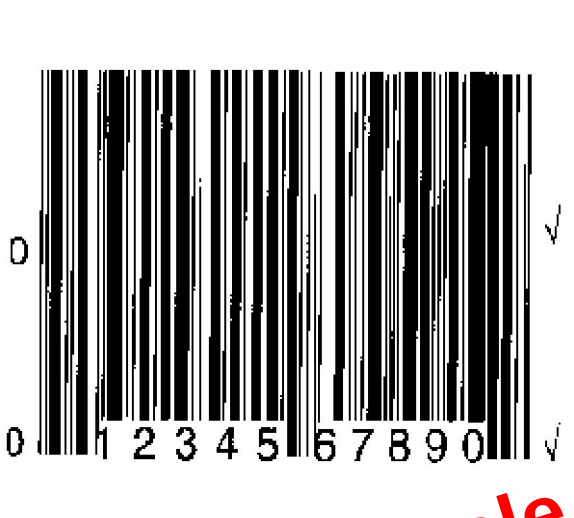

Figure 6
The UPC check digit system. The initial digit may appear in either of the spots marked with a 0. The subsequent digits are placed under the bar code, with the check digit appearing in either of the two places marked with a check mark.

The UPC check digit formula is:
210 - 3 (a + c + e + g + i + k) - (b + d + f + h +j)

For this sample bar code, theformula is:
210 - 3 (O + 2 + 4 + 6 + 8 + 0) - (I + 3 + 5 + 7 + 9) = 125

The last digit of the answer is 5.
Thus 5 is the check digit.

Back to the target of my attack, that academic library near my home. The light pen at one of the computers was attached with a telephone-style modular clip. It could easily be removed. I bought a receiving jack of appropriate size and used a cable to connect it to the modem port of one of my smaller portable computers. Then I modified an auto-dialer program to spit out bar code numbers in the range I needed. I was all set.
A few days later it was Saturday, and it was a gorgeous day. I had expected to pull off this stunt on a Sunday because I'd seen the results of a user survey which indicated that less people came into that particular library on Sunday than any other day of the week - the last thing I needed was a bunch of onlookers. But it was such a beautiful day I figured everyone would be at the beach. I was right; practically no one was there.

Breaking Free

The first thing you'll notice is there's some kind of menu system on these micros. The people who run the joint don't need some snot-nose kid coming along and formatting their hard drives or leaving behind obscene messages, so certain protective de-vices are used to guard against such activities. It is generally a trivial matter to get out of the menu program, even though its very existence - at least partially - is to keep you from doing just that.

If the computer is turned on already and at the main menu, look on the screen for any indications of commands that shouldn't be there, such as "Alt-X to Quit." Try it - does it work? You might

exit the menu, only to get a message like this: "Error! Press any key to return to Menu." What happened is this: when the computer was first turned on in the morning, the menu system was called up by the ALJTOEXEC.BAT file. By typing Alt-X, you have been returned to the AUTOEXEC.BAT shell, and are experiencing the next line of that BAT file. Simply Ctrl-C your way out of there.

Even if it doesn't say on the screen how to leave the menu, you will want to try various function keys, the Ctrl-Break key, the Escape key, and differ-ent combinations of Alt and Ctrl with C, X, and Q.

Often menu systems will have you enter a password before allowing you to exit to the operat-ing system. If this is the case with the one you're hacking, by all means try various passwords -starting with blank lines, the name of the building or company, and other obvious work-related and business like words.

Computer systems are at their weakest when they're moving from one program to another, so try choosing a menu item and using Ctrl-C as soon as it's selected. Actually, for best results you should repeatedly tap Ctrl-C and the Ctrl-Break key simu-laneously.

If none of this works, turn the computer off, then turn it on again and see if you can Ctrl-C or Ct4-Break your way out of the ALJTOEXEC.BAT startup procedures. Alternately, you should have your own program disk ready to boot. If both of these tactics fail, use the menu system to run the various programs listed and see if any of them have an escape to the operating system.

For WordPerfect, you can shell out with Ctrl-F1. Wordstar allows shelling or single commands to be entered with Ctrl-K, F.

Freedom Means Free Roaming

Once you are able to exit the menu system you will be able to explore the computer.

If there are lots of computer-wise people around, or people looking over your shoulder, or people in charge running all over the place, then you'll want to get back to authorized sections of the computer ASAP so you're not discovered in the private parts and thrown out of the building.

My recommendation is to copy everything relevant to your cause onto floppies, then take them home to examine them at your leisure. This is akin to the burglar who steals the entire unopenable safe so he can work on it in his basement with noisy power tools and blow torches.

Copy the AUTOEXEC.BAT file and the menu system first of all, and any directories you find containing files with BAT, DOC or TXT extensions; miscellaneous disk

When you go out on a public hacking expedi-tion, you'll want to be prepared by taking along your PACK: Public-Accessible Computer (hacking) Kit. This kit should include:

Plenty of blank, formatted disks, in both 3%" and 51/4" sizes, so you can quickly copy the menu's security programs. Make sure these disks are the proper density for the drives you will be using.

Auxiliary programs, such as superzappers and other utilities. You will also want to bring any special programs you have written (such as menu simulations, as discussed in the next sec-tion). Public domain programs are available to shut off the internal speaker. This can be useful if you're hacking a computer that lets out a loud and suspicious beep every time a wrong pass-word is entered.

Other tools: A Swiss Army knife is good, or at least bring a little screwdriver. Very often, es-pecially on CD-ROM workstations, you will find locks or covers placed over the disk drives to limit access. A large, unbent paper clip is handy for hacking Macs. If you have to leave in a hurry, you can slip the end of the paper clip into the hole next to the disk drive, and your disk will pop out. That's often the fastest way to eject a disk.

Menu Simulation And Other Sneakiness

For protection and simplification purposes, just about all general-purpose public computers will boot up to a menu program. There are three fruitful programming ideas the hacker can employ with these:

- altering the menu,
- altering the menu program, or
- creating your own simulation of the menuing system.

Menu programs will have a menu-editing op-tion. This allows the people who maintain the computers to create menu categories such as "Business Programs," "Word Processing," and the like, and to add and edit the programs available for public use. The way to work menus to your advan-tage is to use the editing feature to add or change an option that will appear to be taking the user into an area where a password is required. However, what the menu will really do is take that user to a program that you wrote, that simulates an envi-ronment the user is familiar with. The user inno-cently enters his user ID and password (which your program stores), then an error message is given and the user is returned to the menu. Later, you can go to where the computer hid the passwords and IDs, and retrieve them for your personal use.

The first question is, how does one edit the menu?

The menu-editing feature may be part of a sec-ondary program, such as INSTALL.EXE or SETUP.EXE. You may also be able to do editing di-rectly from the menu program itself, by pushing a function key or control code.

Problems start arising because you were not meant to be able to change the menu setup on pub-

licly available computers. The menu-editing feature may have been eliminated once the menu was set up, or a password might be required to do any-thing.

Maybe you can re-install the program, recreat-ing the present menu from scratch, while putting in your own additions (to be discussed soon, hold your horses!). Alternately, you might be able to use a text editor or superzap program to change the file where menu information is stored. If you start get-ting error messages

program. If the cleaner does delete these external commands you will have to figure out some solution to get them onto the disk and protect them from the cleaner. This batch only works on text files - EDLIN will mess up binary files.
Second, you will have to make sure beforehand that the DOS directory is in the PATH. What that means is, for a particular file to be executable, it must either be located in the current directory, or in a directory that has been predefined (usually by AUTOEXEC.BAT) as a place for the operating sys-tem to look for files to execute. This is no problem of course - just add a PATH or CD statement be-fore the first EDLIN - but it is something you could easily overlook, especially if you had to add the special commands yourself to an unusual or unfamiliar directory.
Also notice before installing any programs: will there be enough space on the disk? Enough mem-ory? Does the program try to create the temp file in a locked directory? (If so, open temp in a USERS di-rectory, or some other writable one.) Does a file named "temp" already exist? How about "Corrunandl," "Command2" and "Command3"? There are alternate ways to use this program. In-stead of having the date-changer execute before the clean-up program, it could be run every time the password file gets updated. Though it takes a few seconds to run and that time might be enough to noticeably slow down the user's application pro-gram. Recall that this program is meant to be used in conjunction with some sort of Trojan horse you've installed; the horse itself will slow down the computer somewhat already, the combination of the two programs might be too much to go unnoticed.
The clean-up program might use some other criteria which helps it decide which files to save and which to throw away. You will have to use similar programming techniques to thwart its ad-vances accordingly.
If there is no special clean-up program, the hard drive will be cleaned by an actual human being. That human being might not be clever enough to look outside the designated USERS directory for files, but you have to act as if that person is as clever as you. Anyhow, you never know who else is using a public computer, so you will have to take measures to hide your precious password files from view. Here are a few suggestions:
Change the hidden-file attribute so that it is not listed in the directory.
Place it in an obscure directory or in an unreach-able one. Try this experiment. Put the following commands into a batch file:

```
:Start
mkdir dir
cd dir
goto Start
```

and then execute it from the root directory. After sixteen nestled directories named "dir" are created you will get an error message. Press Control-C and look at what has been created. You will find that within the innermost directory it is impossible to make any more directories - there's a limit to what the computer has been programmed to handle. However, you can use a disk management utility or your own system calls to prune and graft many more directories inside the deepest one. Those grafted directories will be impossible to see or ac-cess from the DOS shell. If the clean-up program uses the DOS command TREE to scan all the direc-tories, it will crash or freeze once it gets to those il-legally nestled directories you put there. You don't want that to happen: that would lead to discovery of your secret files hidden within that directory. Accordingly, this trick requires that you have the programming prowess to write prune-and-graft programs on your own. Your Trojan horse would have to be able to move the data file from its pro-tected position, then back again afterward.

of a Johnson & Johnson building one rainy night, and as I got closer to the building, I looked up to see two guards with their faces pressed against the glass, staring at me.
If you absolutely must trespass a building or its property to get to its computers, try to go at night during a thunderstorm. Visibility will be poor, you can use your umbrella as a face-shield, and if you get chased away they will be reluctant to chase you very far.

Biometric Systems

Controls based on personal characteristics are the ultimate in computer access control - when they work properly. Known as biometric systems, these devices limit access to a computer or the computer room by verifying physical attributes of a person. A biornetric system may look at any one of these individual traits to verify user identity: fin-gerprints, voiceprint, handwritten signature, palm print, hand geometry, or retinal patterns.
Biometric systems are costly to implement, but they are not always as accurate as television would have one believe. For example, a legitimate user's voiceprint may be rejected because of a change in voice pattern or voice speed due to illness or stress, or because of interference from outside noises. One system I tested would occasionally offer responses to the noise my finger made as it scratched the mi-crophone!
Similarly, finger and palm print technology can be thrown for a loop due to cuts and scratches on the hand, dirt on the hands, bandages and blisters, or scrapes in the glass tray on which a user places his finger or palm for scanning. Signature and handwriting analysis systems sometimes fail to pick up changes in pressure, style and velocity; people do not always write their names the same way every day. I imagine this would be especially true for someone rushing into the computer room to print out a report three hours past deadline. Hand injuries could also make a person's signature look different.
Hand geometry devices - those which meas-ure the length and translucency of fingers - don't seem to have much going against them, although again a Band Aid or scraped machine tray could easily cause the rejection of an otherwise legitimate system user. Finally there are retinal pattern rec-ognition systems, which look at the pattern com-posed by blood vessels in the eyes. These too have been shown to be reliable in their accep-tance/rejection rates when user cQmplicity is high.
I point out the flaws in these systems so you will get a feeling for what it must be like to work in a building where you're required to get your eye-balls scanned every time you want to walk through a door. Or imagine being in a place where you have to speak foolishly aloud to switch on the computer. The first few times it may be seen as a novelty, but soon these gadgets become another ho-hurn part of office life. Add to that the time delays these devices cause, the frustration when they don't work prop-erly, the feeling of subservience that comes from having to remove gloves and glasses, speak dis-tinctly into a microphone, present a clean hand, or hold one's face immobile, and you will find a bunch of people who - even under the strictest of security conditions - are sick of the whole damn thing!
Unless there is some incentive for workers to use these biometric devices - for example if their time cards will be punched depending on the time they register in, or if their actions are being moni-tored by guards - unless there is a motivation to follow the rules, you know very well that everyone is going to try their hardest to break them. People like showing how friendly they are. People like to show that they are not a part of the stupid bureauc-racy that runs the place - they like

If you hook up a VCR to your monitor, you'll get a hard copy of your target's activities. It may even be possible to directly connect the VCR to the computer your target will be using. If you do so, it is best to have a remote way of turning the VCR on and off, so you don't record while the computer is idle. If the target has a regular schedule you can simply program the VCR to tape at a certain time.
There's no law saying all screen output has to go to a screen - if for some reason you can't use any of the above techniques. An alternative is to

have information sent to a printer buffer. Make sure that either the printer is fast or the buffer is large. Otherwise the target's computer will slow down tremendously and he won't know why. Also, of course, the printer has to be located far away from the target, preferably in another room or an-other building entirely.
As an example of one limited way in which this can be accomplished, consider the "print from key-board" option found on many word processors. "Print from keyboard" causes that several thousand dollar machine to act like any old junky typewriter, printing characters directly as they are typed on the keyboard.
While your target slips away from his word processor for a coffee break, you can slip over and activate the "print from keyboard" feature. From then on, anything further he types within the pro-gram will be sent to the printer. As I said, this is of limited use, but it shows one more way that even impromptu situations can be exploited by the cornputer-knowledgeable investigator.
By printing "Shift-PrintScreen" on any DOS computer the "print from keyboard" mode will be activated. However, if the printer is not ready the system may hang up.
As an example of passive computing which is really very active, in that hacking is required, it might be reasonable to log on to a network and use programming to direct the target's output to your own terminal. If you have the target's password, the host computer would have to be tricked into allowing the same user to be logged on twice si-multaneously. Additional programming might be required if the computer refuses to send the target's output to your screen, or if the target is getting your output.
If you have a password other than the target's, some programming could send the target's screen to yours, or yours to the target's (if you want to get into simulation). On UNIX systems, you would be thinking in terms of altering already existing pro-grams such as TALK or WRITE to get the job done. These two programs induce a link between two separate accounts. Any time two accounts are joined, there is a potential for misuse of that link-age. But these programs are written with security in mind; the hacker's job is to rewrite the programs, eliminating the security measures.
Another option is to make use of monitoring software which is commercially available - or write some yourself, to satisfy your own personal needs. Managers of offices routinely spy on their secretaries, data entry clerks and other computer operators through the use of software which stores key presses. Other monitoring software keeps track of which programs are being used and how, often time-stamping such information as well. Doing this form of research does not, as you might at first think, necessitate going back to your target's com-puter to see what keystrokes have been recorded. I hot-wired one such keystroke-capturing program to print a weekly report to a hidden directory. When secretly installing the program (visiting the site, posing as a confused user who had a vi-rus-attacked disk that needed repairs), I also al-tered the computer's startup file which executes upon

Menus! Options! Choices to be made! Files to read and to learn from, software to run, games to play. You let the directories sift past you, letting yourself be mesmerized by their framework. So much to do, and then you see connections to other sites, and more sites, and more secret files to read! You smile as you realize something: every hack, no matter its size, leads to new hacks, new computers, new horizons of exploration and gain.

Reality

When I say "Hacking at Home" I don't really mean it. Most computer hackers nowadays won't hack from their houses for fear of Caller ID, line tracers, tricks, traps and federal agents. When I say "Hacking at Home," what I'm really referring to is the phenomenon of dial-in lines. Ways in which, if you are so inclined, without even leaving your house, you can connect yourself with the world.

Who To Connect To

Who can you expect to connect to, calling from home? Lots of places. There are other home com-puters,
mainframes, minicomputers, companies, government offices, clubs - you will be able to call any organization or individual who owns a computer, and has need to communicate via computer with other entities.
You might also find yourself calling on-line databases and pay-for-play services.

Paying For The Pleasure

A hacker named Rebel was recently telling me how enthralled he was with CompuServe, except for one aspect - the stiff price one pays for using the service. For this reason, CompuServe is often known as Compu$erve, with an oversized dollar sign replacing the S. CompuServe is not the only vendor charging the public a fortune to pay back their huge advertising budget. There are literally hundreds of on-line services to which one may sub-scribe, or hack one's way in if that's more your style.
Databases are available to look up any sort of data: census data, news, stock market information, results of government research, science and tech-nology reports, books, personal information, his-tory, and popular culture. There have been times late at night when I needed one crucial piece of in-formation for something I was writing, or just to satisfy my curiosity. Anybody can access one of these databases and find what he or she needs any time of the day or night. Of course, we must be prepared to pay through the nose. There is usually a charge to subscribe to the service, then there may be any number of the following charges:
A display charge for each piece of data pre-sented on the screen, or a search charge for each query made to the database.
Minute-by-minute charges as long as you stay connected to their computers.
High-speed surcharge for using a faster modem (thus gaining the ability to grab more info per minute).
Long distance phone charges if the service doesn't have an access number in your local-dialing area.
Many hackers refuse to pay the inflated bills

Other Networks

The only other network that counts is the Internet.
Internet is an international network of net-works. There are academic networks, government networks, businesses and organizations throughout the world, all connected together (by PDNs) to ex-change ideas, software, technologies, gossip and guacarnole recipes.
Before Internet there was ARPANET, a military network which has since been replaced by MILNET (a well-guarded network of United States military sites) and other smaller networks used by the US military. Altogether, these make up DDN, the De-fense Data Network. DDN is now just one of many networks participating in the Internet.
Others include the National Science Foundation NETwork (NSFNET), which includes supercom-puter centers and other research sites funded by the NSF. CSNET is a network established to encourage cooperation between sites doing development work in computer science. JANET is the United Kingdom network, one of many national networks around the world that is bridged with the Internet. Internet is truly a global community.
Some of the pay-for-play services offer access to the Internet. Many university computer accounts are connected to it. Basically, having an "in" with the Internet allows one to travel around the world and back without leaving your armchair.
We were talking before about packet switched network addresses. An Internet address is a series of code words punctuated with periods, and refers to one particular computer in the millions that make up the Internet. A typical Internet address might be "danielk@cs.zowie4.ubould'er.edu." We can deduce that at the University of Boulder there is a computer in the computer science department called zowie4, and on that computer there is a person whose first name is Daniel, and last name be-gins with K. The "edu" is a standard thing stuck at the end of educational computer addresses. Other identifying components used are:

COM for commercial sites,
MIL for military sites,
GOV referring to governmental organizations,
ORG for non-profit organizations, and
NET meaning Internet administrator sites.

An Internet address may also end in a two-character country abbreviation. Some exam-ples of these are:

AUAUstralia
IL Israel,
US United States
JP Japan
UK United Kingdom
DE Germany (tricky! DE is for DEutschland).

Finding Dial-Up Numbers

To "direct connect" with computers, you will need their phone numbers. Very often you can call up a company and ask the switchboard operator for the computer department and/or computer lines. If that doesn't work, try calling individual of-fices at the firm and ask if they know how to access the company computer from

their home computers. If they don't know the phone numbers, perhaps they have a terminal program on their office com-puter which has the phone number stored for use.
Phone books are a big help. First there are the internal kind: companies and other organizations will have a directory of people who work there, with their extension numbers. Internal directories might also be of the kind that list numbers for the different departments; some go so far as to list home phone numbers and addresses of the people who work there. Names can be used to pretend

familiarity with the people you speak to when you call. But you won't even have to call and ask for dial-up lines if those numbers are listed in the di-rectory.
A second useful source is phone company data grade line directories....
When a person speaks on the telephone, it doesn't matter if every once in a while the voice on the other end gets a bit fuzzy, or if the tone gets momentarily higher or lower. When you're trans-ferring data between computers, however, audio noise can be a problem. So the telephone company has special lines which offices can install (for a price) to ease the flow of data between telecom-munications devices such as moderns. If you can et a data grade line telephone book, you will have 9
found a huge and wonderful collection of computer phone numbers (and fax numbers too). Many hack-ers get theirs by scavenging.
The third way phone books can be helpful is by looking in the public white pages and yellow pages that every phone owner gets for free. Large corn-Panies will own big blocks of telephone numbers, with each office or extension being one digit differ-ent from the preceding one. To call the different departments at Company J, you would dial 390-WXYZ. The 390 stays the same for every de-partment, but the last four digits change for each phone line. So turn on your computer and type up a text file listing every occurrence of those last four digits you see listed for that company in the phone book. Then sort the list and try calling everything in that exchange that is not on your list.
It can be helpful to use a criss-cross directory for this task. Criss-cross directories are sorted by number, not name, so if you know that Company J's numbers fall into the 390- range, using such a direc-tory you will have an even bigger list of numbers to avoid. This makes the job of calling every potential number much quicker and easier.
Software is available to repeatedly dial up a se-ries of phone numbers, reporting on whether a mo-dem is connected. These programs, often available on hacker and cracker BBSs, are known by many names: "WarGames Dialers," "autodialers," or "demon dialers." If you can't find such a program, write one for yourself; it's simple to do and will cost you only a few hours of time.
Once you have your autodialer, be very careful how you use it. The phone company security patrol
knows what you're doing when you make that many calls that quickly, and with such precision. I've often thought it would be a good idea to com-bine one of those computerized telemarketer ma-chines with an autodialer. That way everything looks legit: if a person picks up, they get a short re-corded message: if a modem picks up, they get a callback later.

Dial-Up Security Measures

Chapter Ten:
Electronic Bulletin Board Systems

The Electronic Bulletin Board System (EBBS, but usually referred to simply as a BBS) is how most people get introduced to computer telecommuni-cations. A BBS is a computer program that anyone can set up on his or her computer. The program watches the computer's modem, waiting for the telephone to ring. When it does, the BBS program answers the phone. If it is another modem calling, the two computers are connected. The person who is calling is then able to use the computer on the other end of the line as if he or she was sitting di-rectly at that computer's keyboard. The BBS pro-gram allows the caller to choose various options from menus, letting the caller write messages to be displayed to other callers, read messages, send files back and forth, or play games on the remote com-puter. In essence, the caller actually controls the computer through the phone lines. However it is only the BBS program that he or she is allowed to control. The BBS program separates the caller from the computer itself. At least, it tries to.

BBSs are generally run by computer hobbyists on their home computers, and are used as a way to share information in the spirit of the original hack-ers. Usually there is no charge to call these up and look around, but that is at the discretion of the person running the BBS - the system operator (sysop). Schools, libraries, stores, user groups, churches, and organizations often run BBSs to spread the word about activities and to keep mem-bers in touch with one another. Sometimes com-panies will set up electronic BBSs as a way for their customers to mail order products from them, to see new product information, or to report problems with products or services.

The US Congress has even set up a bulletin board system. Run on RBBS software, the BBS was created in late 1991 by Congressman Bob Wise and his House Government Operations subcommittee on government information, justice and agriculture as a way for government employees to anony-mously inform inspectors about wrong-doing at the workplace.

Other BBSs are private ones, the phone num-bers to which are not made widely available. For example, the FBI runs the National Crime Informa-tion Center (NCIC) which makes use of a BBS to keep track of wanted persons, missing persons, and people with criminal records. Franchise businesses such as fast food places often use BBSs to upload inventory or financial data to their company head-

quarters on a daily basis. And of course, there are otherwise "public" BBSs which maintain silence be-cause the people who use them do so for illegal purposes.

Access to most BBSs is controlled by a name/password combination. When you call up a BBS you are asked to enter your name, or NEW if you have not called before. If you are a new user, you will be asked if you wish to register for the, sys-tem and, if so, you will be asked some questions, welcomed to the system, perhaps given a short tour, and shown the rules of the house ("Please keep messages clean... No discussion of illegal activities such as computer hacking, fone phreaking, stolen credit card numbers, etc...").

After that, you might be given guest access to the BBS until the sysop can validate your request for admission, or you might be logged off and asked to call back the next day. This isn't always the case, of course, but sysops like to make sure you are who you say you are - if you registered with a phony phone number, they want

Occasionally you will find an electronic conver-sation with some intellectual value to it. Embrace it, add to it, and pretty soon you'll find yourself accepted into its underground. If you find such a BBS, one whose members proclaim themselves to be hackers, and yet the conversation is smart and con-servative, you can bet that there are secret sub-boards lurking behind trap doors, where all the real-hacking news gets discussed. Prove yourself as a worthy member of the above-ground community, and after awhile the sysops and assistant sysops will vote you into their elite society. To be accepted as a hacker you must be willing to exchange infor-mation. You must have good information to share and to give.

If you log on to a respectable PBS which you suspect contains a secret hacker subsection, acci-dentally try a different unlisted command each time you log on. (Don't do more than one per login, to avoid generating suspicion.) If you find a com-mand that works, and you're asked for a password, then you'll know you're on the right track. Talk to the sysop or other group members about your feelings on hacking, and ask them what they think about it. Modestly tell of your hacking achievements. You will already have impressed them by finding the secret section, but you don't want to agi-tate them by hacking it out. <One of the criticisms that law enforcement officers make about hackers is that they say we live by a double standard: That we think it is no crime to violate other people's privacy, but we can't stand the thought of being probed ourselves. Well, I don't find a need to defend myself If a hacker can get through the safeguards I've set up, that's fine, because I know that hacker will not damage me by it As far as hacking a hacker BBS is concerned, since the users of that BBS do not know you, they don't know that your intentions are honorable. Thus, to invade them is to get their guard up. In your talking to the sysop you might want to mention that you refrained from hacking the hole that you found, in order to reassure them that you are a fellow hacker and not a cop.>

Any you certainly don't want to post a public message stating that you found their trap door; you can be sure there are plenty of others without that secret access who are also roaming about. Talk to the sysop and assistant sysops privately about your find, via e-mail or on-line chats.

Making Connections

Many of the BBSs you encounter will be strictly legit operations. There will be no talk of hacking, no trading of break-in secrets, and certainly no sensitive information of any kind being distributed to newcomers. You will have to start by jumping into already established, possibly ho-hum conversations.

Be polite, try to be helpful. Add thoughtful comments to the discussion. Having an experi-enced hacker as a friend will do more to boost your skill in that area than anything else - except per-haps some persistence, research and luck.

Soon you will have a few favorite systems that you'll call on a regular basis, but you should also be constantly branching out, trying all the new sys-tems you find, your goal being to eventually find an access into the "computer underground."

There is no single, organized underground per se, but there are groups of hackers and others inter-ested in technology scattered here and there. They will keep their conversations of illegal activity se-cret, so it will be difficult to find them. The message boards they use to communicate will often remain hidden to the uninitiated, and the BBSs on which the most interesting tales are traded will not have their phone numbers publicized at all. Your best bet is to keep searching. If

Midnight Masquerade

One night, at around 1:30 a.m., the Treacherous Den BBS received a visit from a hacker. The hacker tried logging in a few times using my handle, The Knightmare. The sysop of the system, my friend DR dendryte, was sitting there watching the hacker go at it unsuccessfully until finally he pressed the function key which brought the two of them to chat mode. The following is a transcript of the ensuing conversation, copied exactly as it appeared in the sysop's printout, but with unnecessary carriage re-

turns removed. [My own comments are in brackets, like this.]

SysOp wants to Chat!

This is DR dendryte, Who RU?

this is Knightmair i Forgot my password. Log me on.

[At this point, DR dendryte knew for certain he was dealing with an impostor. He knew that I never called that late at night, and that I would never for-get my password, considering that it was the same password I'd been using for several years. DR den-dryte, however, decided to play along.]

How Did you forget your password??!

I dont know it just slipped my mind i guess! I can't just give out passwords like that you don't have to you can just log me in.

If you're really The Knightmare then tell me, what is your REAL NAME?

[A pause, and them]

don't you trust your own best friend & co-sysop?

come on

i cant beleive you!!!!!

You are definitely NOT The Knightmare...

[Here DR dendryte was referring to the hacker's bad spelling and grammar; DR dendryte knew that I am meticulous in my on-line chat writing.]

he never makes stupid spelling mistakes like that, or uses bad grammar or

[Here, both are trying to type at once. DR dendryte lets the cracker speak:]

That does igt! I don't want to be your friend anymore! just delete me off the BBS.

You won't be able to pull a stunt like this unless you can gain access to the source code for the soft-ware, as he must have been able to do (unless you want to recreate from scratch an entire bulletin board system).

112

Once again, another of those pesky hacker attacks was thwarted!

Crashing BBSs

On another BBS that I was a part of, the sysop would come home from school every day to find his system had crashed. It had simply frozen up and would have to be rebooted. Eventually he found out from someone that there was a bug in that version of that particular BBS. A "\x" typed at the password prompt caused everything to halt. Key por0ons of the BBS software were written in easily changeable, interpreted BASIC. To remedy the problem I simply added a line after the prompt that would disconnect anyone who tried typing in the dreaded 'Ax."
It worked.
I've always wondered about that "\x." Why would such a harmful thing be there? I can't imag-ine the programmer putting it in purposely, unless perhaps it was a means to bother unlawful users of his software. Maybe it was some trap door that had gone awry. Maybe if I had studied the program more I would have figured out its meaning.
Maybe - this is a credible possibility - that bug had been placed there by the person who had given the copy of the software to the sysop, or by the pirate who had first bootlegged it, or by anyone at all along the line. Pirated software travels so rapidly across the country and around the world that literally thousands upon thousands of persons might have had the chance to add the 'Ax' thing and distribute the buggy code. Hey, are you starting to get an idea there? I know I am!
You could either write your own BBS program or alter a currently existing one, with some secret features such as an exit to DOS, or whatever trap doors tickle your fancy. You could put in a line which checks to see if a very obscure and unlikely control code is entered at the login prompt, and if so, highest system access is gained.
A twist to this tactic is to write or change a terminal program, which you give to the user. When it receives an internal code while connected to your BBS, you gain access to the calling com-puter. For example, a user would be running your special terminal program while calling your BBS. The BBS, would send a code to the caller's modem, which would allow you to wander around the caller's hard drive. To cover up the fact that you're roaming around in there, entry would have to take place during a long file transfer or, if it is a slow modem, during those time lags between modem action. The terminal program could continue pre-tending to receive data while you surfed the remote user's drives.
PRODIGY, a graphic-oriented interactive, on-line service, was accused of engaging in a variation on this theme in the summer of 1991. Users were finding personal data buried inside the software that is used to dial up PRODIGY. After complaints and outrage, PRODIGY's senior vice president mailed out a utility to those concerned, which would erase non-essential data from the service's terminal software. In an accompanying letter he sincerely asserted:
As we have stated publicly and written on-line, the PRODIGY software does not read, collect or transmit to PRODIGY Services Company any information or data that is not directly connected to ur use of the service. We want to assure you yo

that we will continue to work to safeguard the privacy of all of our members.
Maybe theirs doesn't do those things - but yourscan!
Years ago, one group of enterprising hackers distributed their own homebrewed, broken termi-nal program for the Macintosh line. The program gave users the convenient option of allowing them to store passwords and other login procedures on disk so that one would never have to worry about forgetting them. The information was stored in en-crypted form on a hidden part of the disk. The pro-gram was developed to "go bad" after several phone numbers and passwords were stored, the hope being that users would send back the disks, and the hackers would end up with a bunch of precious login information.
This should be taken as more theory than actual practice: PRODIGY can get away with requiring users to boot from their software because of the unique graphics and mouse interface provided. Unless you work something like that into your term program, who's going to want to bother in-stalling and learning your software when they are already familiar with one or several commercial

packages? In fact, this is what happened to that group of hackers. Initially there was great interest in their terminal program (which they gave away free), but no one wanted to go through the trouble of using it. The problem was, the hackers gave the program out to experienced users who had already developed an intimacy with one or more commer-cial programs. No one needed the hacker's terminal package, and so what seemed to be a great idea net-ted the hackers nought.
As for the first idea - changing a BBS to in-clude trap doors - now that is a viable possibility. There will always be plenty of people looking to set up their own bulletin board system, or who are looking for ways of acquiring new software. Distri-bution is less of a problem than the program ming, especially considering that you will not only have to interject code for the trap door but, for best re-sults, determine a way to hide that code from inter-ested eyes.

Trojan Horses

It is usually easy for a hacker to infiltrate a BBS with some version of a Trojan horse program. The hacker writes a program which performs some interesting function, such as playing a game or putting pretty pictures on the screen. Hidden in that program are instructions to read BBS password files, or carry out some other covert operation. The hacker then uploads the program to a BBS and -here's the important part - hopes the sysop runs the program.
You will want to procure a copy of the BBS program before writing a Trojan horse, so that you know exactly what those secret instructions should be doing. Otherwise, how will you know what files to look in or where to go on the disk for information?
What kinds of things can you program a Trojan horse to do? Here are some suggestions:
Have it secretly reprogram the BBS itself to in-clude a trap door. If the BBS program is written in an interpreted language, you can have the Trojan horse add some lines which would give you sysop ccess upon entering some code word. This actu-ally has been done on a popular Commodore 64 bulletin board system that was written in BASIC.
You can program the Trojan horse to look into the password file and send data contained in it back to you somehow. Many BBSs have a text file section. You can

who happens to pass by. If the sysadmin has been editing the password file, or some other file containing sensitive data, you could be in luck. Electronic mail is often not automati-cally deleted, and it accumulates in (perhaps hid-den) files on disks. Deleted files may not be deleted right away, but become hidden or moved to a spe-cial directory.
See if you can find evidence of security logs. One of the most common errors for a user to make while logging in is to type the password at the username prompt. If you can find a readable secu-rity log it will often contain records of these login errors. For example, if George Washington tries logging into his UNIX account with his password, "cherrytree," but he types a little too fast, the following ensues:

WashingtonUs [Enter]
ername:cherrytree [Enter] Password:

George realizes he has messed up. He has typed his name before the login prompt, and he has put his password (quite visibly) on the "Usernarne:` line. He presses Enter a few times to clear every-thing, but the damage is already done. Somewhere in the administrative directories, there is a log file that reads:

Unsuccessful login of user cherrytree @ Tue,
Mar 24,1992,14:16:03

Now you just have to go through the various users on the system until you find the one who uses this password.
Security logs may also keep track of files sent and received, errors resulting from unauthorized commands, new accounts or new users being granted superuser status.
Speaking of security, the first thing you should do any time you log in to an account for the first time is try to get a sense of who this person is whose account you are borrowing (assuming you don't already know). When you log on you will most likely be greeted with a message telling you the last time that account had been active, and possibly which location or server the user had con-tacted it through.
If the message tells you that the legitimate user logged in recently then you may have a problem. Note the time of day the account was used and try to hack around it. Try logging in two times simul-taneously on two separate computers and see what happens. Do you get an error message the second time? Is it possible to detect the presence of another

person using the account with you concurrently? You want to know such things because you want to be able to deal with having the account holder co-incidentally log on at the same time as you.
Let's look at this first scenario. You are logged into the account... the actual user tries logging in but gets a "User hjones already logged in on port 116" message. You have no way of knowing that this has occurred, but you can prepare for its eventuality by sending an e-mail message to the ac-count, purportedly from the system manager, and leave it unread. So if the legitimate account holder were to log in she would find something like this waiting for her:

Message #01
From 1513 SuperUser

of software naughtiness detail the willful, knowing, and unauthorized modification, destruction, accession, possession, or copying of computer data, computer programs, or "supporting documentation."
The final offenses have to do with the hardware aspect. "Whoever willingly, knowingly and with-out authorization," either modifies, destroys, uses, takes or damages a computer, computer system, network, equipment or supplies related to comput-ers, is guilty under this statute.
There are eight different penalties listed, depending on whether the act in question is consid-

ered a misdemeanor or a felony under the law. The magnitude of the crime is based on how much damage was caused money-wise, how much threat to others there was, and whether the hacker did the deed with intent to defraud or obtain property. Penalties range from life imprisonment (sheesh!) to various fines in the $500410,000 range.

Traditional State Crime Laws

just because your state doesn't have a law that specifically forbids snooping around in someone else's computer, doesn't mean what you're doing is completely legal. Prosecutors will try to convict hackers on violations of any law, even if there's a large void between the hacker's actions and the original intent of the law. In some circumstances, the prosecutors may feel there is not a good enough case against a hacker using the computer laws. For other reasons, such as a rural jury - prosecutors will press the issue of guilt, but try to sidestep the technical aspect of it. They will charge a hacker with infractions of traditional crime laws, such as malicious mischief, burglary, larceny, and what-ever other nasties they can squeeze into play.
There are problems applying traditional laws to modern "crimes," and the focus changes from whether Hacker X is guilty or innocent, to whether Hacker X is guilty of that particular crime. Can hacking be considered a kind of burglary? In a blue collar computer crime, such as the theft of the ac-tual hardware, there is no question whether or not a law has been broken. On the other hand, if a hacker steals records from a database, do the bur-glary statutes still apply? What if the hacker didn't actually deprive anyone of their information, but only made a copy of it for him or herself? Is this a different issue?
These topics have been addressed differently in different court cases. If you are ever unfortunate enough to be tried for hacking-related offenses, the judge's decision will be based on the exact defini-tions of "software," 'burglary," and other key words for your particular state. If the state has no com-puter crime statutes, then "software" may not be defined; in that case it is up to the judge entirely to decide what these terms mean.
Since we do have 50 states worth of laws to consider, in addition to federal laws, space constraints dictate that we not list every single statute and definition that might apply to a hacker's trial. For the specifics you will have to do your own research into your state's laws. Here is a generalized overview of traditional crimes, and how they can be applied to convict you of computer hacking. I want to stress this point of "generalizations." All the definitions of law to fol-low are simplifications of the laws throughout the land. Individual states add their own

WHAT IS YOUR NAME? TYPE IN FIRST AND LAST:

WHAT IS YOUR PASSWORD? TYPE <RETURN> ON A
BLANK LINE IF YOU DON'T HAVE ONE:

A few months after I began actively hacking, I was using my computer and watching the evening news when a story came on about the governor breaking his arm and being rushed by helicopter to a hospital. I thought to myself, "Hey, hospitals must use computers, right? I can probably get into one!" So I got the supposedly private number for the Greenwood Family Hospital Network, and I called up, and I got that welcoming screen. Guess what I did next?
It's not too hard to figure out what I did! Natu-rally, I typed in ROGER CORNWALL for my name. Unfortunately, the real Roger Cornwall had a password of some sort; pressing Return on a blank Me just got me an error message. So I tried HAROLD LIPNICK. Again, no go.
I went into the kitchen, got out the phone book, looked up the telephone number of Greenwood Family Hospital, and I called it. A woman an-swered:
"Greenwood, may I help you?"
"Yes, please," I said, "Is Tom there?"
'Who?"
"Uhm.... There's some guy there I spoke with earlier... Your supervisor or somebody?"
"Lee Brown., you mean?" she asked.
"Oh yeah, I guess that's it. I don't know where I got Tom from. Uh, is he there?"
"Nope. Lee left at five."
"All right, thanks."
"Bye-bye."
I went back to my computer and called back GFH-NET and tried LEE BROWN for the name. Once again, I was out of luck. However, after a few more phone calls to the various numbers listed for the hospital, I came up with a guy (a resident) who had not bothered with a password.
GFH-NET turned out to be nothing special after all. It had nothing to do with hospital billing, pa-tient records, or anything else pertaining to the ac-tual running of the place. Mostly it was like a doc-tor BBS. From what I could make of it, it was medi-cal students discussing problems with the doctors on the system. No file transfers or anything; just a very simple messaging system. It was no big deal, but it was fun to get into.
The next day I looked through the doctors in the yellow pages, and I found about eight listed who had Greenwood Hospital addresses. Out of those names, three had no password.
So anyway, I was puzzled as to why Pretty Theft couldn't get on there. I called it up for the first time in years, and to my surprise found this nasty logon screen awaiting me:

USE OF THIS SYSTEM IS
RESTRICTED
TO AUTHORIZED PERSONNEL
ONLY!
EVERYONE ELSE MUST HANG UP
NOW!

sharing secrets on a hacker BBS, you'd better make sure the sysop takes all of the following safety precautions: user screenings, a false front and hidden back boards, double blind anonymity, encryption, and affidavits of intent.

The most important aspect of any hacker group, club, or BBS, is secrecy. A true hacker BBS will not advertise, because it does not need new members. A hacker BBS will seem to be a very homey, fam-ily-style BBS up front, but type a code word from off the menu, enter a password or two, and you en-ter the hidden realm. Hacker BBSs should further protect themselves by only allowing specified users to enter the secret parts of its domain, to prevent unauthorized hackers or pseudo-hackers from breaking in to your meeting place.

Any hacker BBS which does not take this mini-mal precaution of pretending to be legitimate, is ju-venile, dangerous, and not something you want to be a part of.

Going up the scale of stupidity just a bit, I've seen plenty of "hacker" BBSs which allow access to the hidden part by entering words like "DEATH" and, yes, even "PASSWORD" as passwords. Need-less to say, the information found on such boards is very low content, and usually consists of the vari-ous users calling each other dickheads.

No new users should be allowed on a hacker BBS unless one or several existing members can verify that the potential user is not a cop, will abide by the club's law of conduct, has information to share, and will not be a big blabbermouth. As a sy-sop, you will enjoy composing the list of rules that govern the way the BBS takes in new members. Remember, any new member should not even know that the BBS exists until the time when he or she is accepted into it. That will keep out law en-forcement people, and keep in only the best hackers available.

Once a member has been verified as clean, his other private information should be destroyed from the computer records. In fact, think about the BBSs on which you are a current member. Are there any which are likely to be busted in a raid? Even if

you aren't doing anything wrong on the system even if nobody on the system is doing anything illegal you know very well how mixed-up the feds get when it comes to computers. You don't want your name brought into a computer crime trial, even if the case is thrown out of court before it begins. So if you're a member of any subculture BBS, tell the sysop, to replace your personal infor-mation (name, address, phone number) with false-hoods.

If you ever register with a BBS but decide not to call back, make sure to inform the sysop that you want your information deleted. (Verifying that such information has been altered or deleted is one legitimate reason for hacking a BBS. Legitimate, that is, from a hacker's ethical point of view.) It is important to do all this, because there are impos-tors out there who are very good at catching hack-ers when they least expect to be caught. In June of 1987, an AT&T security official logged onto a Texas BBS and found messages from a hacker boasting about how he'd gotten into a certain company's computer system. This led to the hacker's arrest.

Note that since the hacker undoubtedly used a handle on the BBS, and it was a hacker board, the official might have hacked himself to get the hacker's real name. In any case, make sure your real name, address and other identifying data never stray to unsafe waters.

Before we start talking more about what you can do as the sysop of a hacker BBS, let's conclude with a real life example of what happens when hackers DON'T follow the advice I've listed above. In 1986 a BBS called simply and arrogantly, "The

It should be a hell of a series. Thanks for your help. And don't bother trying any harassment. Remember, we've got YOUR real names.

Mike Wendland
The I-team
WDIV, Detroit, MI.

Board: General Information & BBS's
Message: 42
Title: BOARDSCAN
To: ALL
From: THE REAPER
Posted: 8/20/86 @ 3.31 hours

This is John Maxfield of Boardscanl. Welcome! Please address all letter bombs to Mike Wend-land at WDIV-TV Detroit. This board was his idea.

The Reaper (a.k.a. Cable Pair)

Is any comment required?

You can see from this that the people who come after hackers - the people who will be coming af-ter YOU - are not all Keystone Cops. Maxfield knew enough to pick '1001" handles like The Reaper and Cable Pair. The newuser password to get into The Board was HEL-N555,Elite,3 - a quite nice password considering its origin. Maxfield, and others like him, are as into hacking as we are. They are knowledgeable of the culture and the lingo and the way we think. This last is particularly hurtful. And it means you can't allow yourself to think like everyone else. You won't become an elite hacker without the strength of your entire common sense working for you. When you call up BBSs, be sure and exercise that strength.
Now let's talk about exercising First Amend-ment rights.
We do have the right to run our own BBS, and to exchange information on it. On a hacker board, that information is likely not going to be the kind of thing you'd read to your mother.
Disclaimers, such as, "This BBS will not tolerate any unlawful discussion of blah blah blah..." are Boardscan is a company headed by John Maxfield, which seeks out and destroys hackers and their ilk.
worthless, but you may want to throw them around anyway to complement my next sugges-tion: Many of the traditional laws which hackers get nailed on have to do with "harmful intent." That is, can it be shown that the hacker or cracker will-ingly caused damage to a computer?
If you are running a hacker BBS or club, you might then consider having members sign an affi-davit which makes their good intentions known. Members should sign an agreement stating that they would never willfully damage another's com-puter or its contents, that any information ex-changed on the BBS was for knowledge value only and that none of the illegal activities discussed will be actively pursued, etc. Basically this should be a way to let the members feel they are actively par-ticipating in your code of ethical hacker conduct which should be prominently displayed upon login to the BBS. Signing such a goody-two-shoes affi-davit may not get you out of legal trouble, but it will do two things. It will stress the point that a member who does not follow the agreement is un-worthy to be a part of your

the way it would turn out. In real life one can't count on others seeing things from your point of view.
At the very least, one would hope that by providing a code of ethics, you could more easily weed out undesirables from your group, and keep your members safe and happy. More importantly, I feel there is some indescribable underlying goodness

about having a code to guide you. If I sound preachy, fine. I'm done.
This is my Hacker's Ethic. These are my beliefs about computers and hacking, as I attempt to live them.

My Code Of Ethics

Computers have enabled a great deal of infor-mation to be available to anyone, and quicker and cheaper than ever before. The free flow of informa-tion is good, but not when it violates human rights. There are two kinds of human rights. There are rights which pertain to individual humans, and rights which pertain to humanity as a group.
All of humanity should have the ability to ac-cess virtually any known information. There should be a free flow of information, and informa-tion and technology should be used in moral ways. People should know how things work if they choose to know, and such information should not be kept from them. New ideas should be heard, and there should be the capability for ideas to be discussed, and questions answered, from multiple viewpoints. People should be made aware that all this knowledge exists, and can be brought to them. Technology should be used to this end, not for profiteering or political gain.
Individually, people should have the right not to have data pertaining to them available for use in ways which are adverse to them. People should have the right to be notified when information about them is added to a database, when and to whom it is sold or given. Because it is their own personal information, individuals should have the right to control how information about them is dis-tributed.
A person should have the right to examine in-formation about him or herself in a computer file or database, and should be able to do so easily. The person should have the right to easily correct inac-curacies in that data, and to remove information that is offensive to that person. People should be guaranteed that all makers and suppliers of data-bases will enable these rights to be granted, in a timely fashion.
All of this is what should be the case, and in some situations these rights are currently acknowl-edged. However, most of these rights are almost unanimously ignored. Therefore it is necessary to hack. Hacking is using computers (or whatever) to live according to these ideals. Hackers have these ideals about individuals in general and humanity in general, and I have a set of ideals which I personally follow so that the general ideals may be carried out:
• Never harm, alter or damage any computer, software, system, or person in any way.
• If damage has been done, do what is necessary to correct that damage, and to prevent it from occurring in
the future.
• Do not let yourself or others profit unfairly from a hack.
• Warm computer managers about lapses in their security.

I called up the system from my home and ex-plored every inch of it. It was a command-run sys-tem. The opening screen allowed one to select a function by entering commands such as CAT to search the library catalog, or HOL to place a hold on an item. The proper way to end a session was with the END command. I tried other, unlisted commands to see if any would work. More than you n-ught realize, this is a very common practice on computer setups where part of the system is public and part is private. Almost always the pub-lic part of the system will have at least one secret command to allow entry into the private side. So I tested a whole slew of key words: EXIT, BYE,LATER, START, LEAVE, LOGIN, QUIT, USER, PASS, LOG, LOGI, CIRC, and the like. Some of these I have seen used in actual applications. (For example, CIRC is often used to enter the part of a li-brary program that takes care of circulating mate-rials. I discovered LEAVE on a computer that was situated in a museum - typing it in allowed one to exit the menu arrd enter a special area for museum curators and employees.) None of these, nor any of the other words I tried, worked.

Since it was a brand spanking new system, I was sure there would be lots of bugs hanging around that I could exploit. Indeed, when I spoke to the director, he bemoaned the fact that certain function keys on the terminals had not been set up yet, and that pressing them would exit one to an incomprehensible programmer's environment. Aha! This is what I needed! But when you're calling in over the phone lines, you don't have access to the function keys that are available on the computers in the company offices.

I thought perhaps the function keys were mac-ros for commands which a user would otherwise have to type in by hand, but I didn't know what those commands were. I was doing nightly excavatings of the building's garbage bins to see if anything would turn up, and finally something did - a badly mangled reference card from the com-pany which had supplied the software package. I painstakingly searched every last inch of the trash that night, but could only come up with half of the card.

At home, I saw that among the things listed on the card were indeed the names of commands mapped to the function keys. Only two of them were legible, and the rest were either torn off or smeared beyond readability, but those two turned out to be enough.

What was immediately apparent was that I had made a wrong assumption - not ALL the com-mands were standard English words or abbrevia-tions of words, like CAT or END. There were two-letter commands and dot commands, too.

When you input a dot command you type a period (.) followed by an alphanumeric command. They are often used in applications where entering the alphanumeric command by itself would be misinterpreted as inputted data. For example, let's say you're using this library system, and at the prompt where it asks for an author to search for,

you decide to search for books by title instead. So you type the TITLE command. What's going to happen? The computer thinks that "Title" is the name of the author you want, and starts a search for someone with that name. To get around that sort of problem, this system allows a period to be typed before a command. Now if you type ".TITLE" at the author prompt, the system sees the leading period and recognizes that what follows should be treated as a command.

Programs often use a period before the com-mand because a period is a small, undistracting character and is also very easy to type. But occasionally you will run

fictitious rep-resentative from the database company that had written the software. The bulletin instructed the di-rector to call this person about some new im-provements that could be gotten for free now that version nine had been released (reverse engineer-ing!). I supplied a phone number to call. The num-ber I gave him was that of a friend of mine, a fellow hacker named Morriskat, whom I had thoroughly briefed on how to act when the library director called. We set up Morriskat's answering machine so that if the director called when he wasn't there, a convincing song-and-dance would tell about the new products this company was offering at the time.

When the director did make the call, Morriskat talked about some upcoming features, then asked him some technical questions about the particular way the software had been installed for his library. The director didn't know the answers but, he said, he had a terminal right in front of him - he could log on...

"Perfect," Morriskat said. "Just go through your usual stuff. Circ. JSC. Uhm, Social Security Number 402-66-0123. Are you still using the personal pass-word we originally set you up with?"

"Yeah, 'Firebird.'Okay I'm in.....

Knowing three out of the four security controls, projecting an air of omniscience, and having the spoofed e-mail as support, getting that final pass-word was easy as pie.

For the last phase of the project, Morriskat and I sat down to see what we could do with the library director's system access. It turns out we could do plenty. We made up new superlevel accounts for ourselves. We were able to toggle access to virtually every aspect of the software to any other user. And we could print out personal information about every employee at the company - because every employee, whether they ever stepped into the company library or not, had a record in the li-brary's computer. We knew what materials they had borrowed, their home and office phone num-bers and addresses, and year of birth.

Exiting from this level to the network server was simple to do, and from there we could log on to

one of the host computers using the library direc-tor's name and his password "firebird."

As the coup de grace, and to prove conclusively that I had done what I had set out to do, I used the programmer's interactive debugger editor to alter the library program's opening screen so that in-stead of giving an explanation of commands, it told a dirty joke. Then I left a file inside the library di-rector's directory which explained how I had bro-ken in. This story as I've told it here is pretty much that file, although here I've expanded more on the hackerish side of things.

Principles Combined

If you are to be a truly successful hacker, one who can hack on demand like this, then you must be a hack-of-all-trades.

It's not enough to be a spontaneous and smooth-talking social engineer. It's not enough to be a programming genius. It's not enough to have the perseverance of a marathon runner. You must have all of it and an imaginative, goal-oriented mindset as well. And the ethic. I truly believe that a hacker who lacks the hacker's ethic will be going nowhere fast, because if you don't show an honesty and

plaint or concern will be able to deal with the situation. All others will be hackers.
Set up a means by which legitimate users can question a suspicious character lurking about the offices without seeming to be rude or obnoxious if the "character" has an honest reason for being there.
Don't let your users become complacent about security, but don't overwhelm them with it either. Most people will follow a few rules, even if it in-conveniences them slightly. If your demands are too outrageous however (changing passwords at every login, for example), none of your users will comply. Make sure they understand why you are concerned. Point out the loss to them if security is breached. Make sure they understand how impor-tant all of them are in maintaining safety not just for themselves, but for every other member of the organization, and every other member of any group connected with yours.
Finally, to really ensure that security is as close to 100% as possible, set up a regular maintenance and clean-up schedule. Actively look for holes in your system's armor. If you hear of hacker attacks or viruses at other sites, learn about their problems and see that they don't happen to your own site. Fix known bugs immediately and promptly remove all debugging tools and options. One investigator has estimated that a third of the security holes he has found were due to debugging options.
If an employee leaves your organization, im-mediately erase their access and change everyone else's access codes. Notice that when you erase the ex-employee's account, you must strike a balance between fair warning and urgency. A disgruntled employee will be even more vengeful if you de-stroy a year's worth of work in addition to firing him and closing his account. But giving a warning too far in advance allows viruses, time bombs and trap doors to creep into your system.
Numerous pieces of literature are available for any machine detailing specific security measures an administrator should take. Make use of these. They will point out flaws you could never have dreamed existed.
Ultimately, the little bit of extra work this all involves will prove its immense worth.

Some Thoughts
To The Concerned Hacker

You've come this far and you still have doubts about success? I guarantee you, if you care about learning to hack, you will become proficient in the art.
If you've tried and tried and tried, but you still haven't managed to get past finding a phone num-ber - or perhaps you can't even get to that - you can still count yourself among one of the few true hackers so long as your intentions are good, you play it safe with hacker security, you intend to act ethically when you do come onto a system, and you intend to enjoy your life to its fullest potential.
After all, that's what a hacker is and does.
Congratulations and good luck to you: now you know the Secrets of a Super Hacker!
And you, too, are one.

Further Reading

Hacking begins and ends as an intellectual exercise. What that means is, if you want to continue to experience the thrill of tap dancing through the nation's

Terminal - Usually refers to a dumb terminal. In general, it is a combination input/output de-vice (a monitor and keyboard) connected to a remote computer.

TG - Technical Guide.

tiger team - A hacker or group of hackers who are engaged by an organization to find the security flaws in that organization's computer system.

tone generator - A device which includes two exterior components - an acoustic coupling device and a telephone keypad - with interior electronics that generate tones needed to operate a telephone. Often seen as a portable tone dialer, these devices are small enough that they will generally include a clip so that they can be hooked to one's belt and easily carried. Also called "tone dialer."

trapdoor - An undocumented way of gaining access to a computer system, usually thought of as a method of entry put in by a system programmer who wants to break into the computer after he is no longer employed by the company. A trapdoor may also lead to hidden areas of a system. A different kind of trapdoor may be unintentional; for example, a laxness in encryption procedure that allows one to deter-n-dne the plaintext without knowing the key. Synonym for back door.

tracking - An investigator's use of system logs and other audit trails to look and see where a hacker has been and what the hacker has done.

Trashing - To scavenge through the garbage of a business or organization, in the hopes of finding useful information, discarded manuals and the like.

Trojan horse - A section of code hidden inside an application program that performs some secret action.

Trusted Hosts - On some UNIX implementations, it is a list of other computers and users who require no password for entry.

TSR program - Short for Terminate and Stay Resident program. A TSR program is one that is put into memory and stays there, even after other programs are loaded in. The TSR usually stays "hidden" in the background until a person or the computer decides to use it. For example, a program to keep track of what keys are being pressed might be loaded into memory as a TSR. As the user switches from one application to the next, the TSR continues to run silently in the background, capturing keystrokes.

UNIX - An operating system originated by Ken Thompson and Dennis Ritchie at the Computer Research Group at Bell Labs. True hackers, they wrote what would become one of the most predominant operating systems so they could play Space Travel without getting a jerky response from the MULTICS time-sharing system they had been forced to use.

USENET - A huge Internet-based message ex-change. Users from all over the world read and exchange news, notes, comments, stories, files, humor and help on all topics under - and above - the sun.

hobbit
home
horizontal
host
hotkey
human
index
input
iris
isis
j1p
kermit
king
kirk
klingon
Ian
lang
language
laser
lee
lord
male
man
mark
mask
master
matrix
memory
menu
modal
mode
model
modem
modulate
moon
msdos
nc-101
net.god
network
next
nil
nill
nim
node
null
object
ohm
OOP
operation
oscillator
output
overload
picard
piggy
power
pres
primos
procedure
prodigy
protocol
quartz
quattro,
query
quit
qwerty
radio
random
ravel
register
riker
robot
romulan
romulon
romulun
rtty
scotty
scraft
shuttle
shuttlecraft
skip
skipzone
space
speed
spock
star
stars
startrek
sting
strek
sttng
Su
sundevil
super
superuser
support
SWI
synch
szone
tasha
overheat
tech
technical
technician
test
time
tng
transport
transporter
travel
trek
treker
trekie
trekker
trekkie
trekky
tribble/s
troy
tsupport
tyar
unix
var
variable
vax
vecto
virus
VMS
Vulcan
wcl
Wang
warf
warp
WC
wheel
wizard
worf
worm
xmodem.
xterm
ymodem,
zmodem
yar
zero
zoo

Screen Stealing: How to secretly record every image that appears on a computer screen.

Data Delivery: How to hide the information you've collected; How to e-mail it to your computer.

Stair Stepping: How to use a low-level account to gain ever-higher levels of access.

And Much More! Including a brief history of hacking, lists of likely passwords, and a summary of computer crime laws.

The Super Hacker reveals all his tricks: Trojan Horses, Viruses, Worms, Trap Doors and Dummy Accounts. The how-to text is highlighted with bare-knuckle tales of The Knightmare's hacks, including on-site hacking, remote-access hacking and bulletin board busting.

Chapters include: * Researching the Hack * Passwords and Access Control 0 Social Engineering 0 Reverse Social Engineering o Public Access Computers and Terminals 0 On-Site Hacking: The Trespasser-Hacker * Hacking at Home: Dialing Up Computers with Your Modem * Electronic Bulletin Boards 9 What to Do When Inside 9 How to Keep from Getting Caught * The Hacker's Code of Ethics Bibliography * Glossary * And Much, Much More!!!

No system can withstand the ingenious, unrelenting assaults of The Knightmare. And no person concerned with computer security should miss this amazing manual of mayhem.

To order more copies of this book, please include $19.95 per copy plus $4.00 for the shipping and handling of I to 3 books, $6.00 for 4 or more. Be sure to enclose your name and shipping address with your request. Send your order to: Loompanics Unlimited, PO Box 1197, Port Townsend, WA 98368.

Washington residents please include 7.9% sales tax. Also see the You Will Also Want To Read Section and the Catalog Ad at the end of this book.

BLANK PAGE

• 61139 Methods Of Disguise, Second Edition, by John Sample. This new edition is expanded and updated with many easy-to-follow ideas for changing your facial characteristics, altering the look of your eyes and mouth, changing the shape of your body, disguising your voice, controlling and changing habits and mannerisms, along with how to make a pocket disguise kit to carry with you for those quick changes. 1994, 51/2 x 81/2 268 pp, over 130 detailed illustrations, soft cover. $17.95.

• 10048 The Big Book of Secret Hiding Places, by Jack Luger. This is the biggest and best book on concealment of physical objects ever printed! This book tells how searchers find hidden contraband and how to hide your stuff so it can't be found.