```
ÚÄÄÄÄÄÄ InformationÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿
³                          °°°Û   °°°°°Û  °°°°°Û   °°Û       °°Û     ³
ÃÄÄÄÄÄÄ Systems ÄÄÄÄÄÄÄÄÄÄÄ °Û ÄÄ °°°Û ÄÄ °°°Û ÄÄÄ °°°°Û ÄÄ °°°Û ÄÄÄÄ´
³                           °Û    °°°°°Û  °°°°°Û   °°°°°°°°°°°°Û     ³
ÃÄÄÄÄÄÄ Security ÄÄÄÄÄÄÄÄÄÄ °Û ÄÄÄÄÄ °°Û ÄÄÄ °°Û Ä °°Û Ä°°Û Ä°°Û ÄÄÄÄ´
³                          °°°Û   °°°°°Û  °°°°°Û   °°Û       °°Û     ³
ÀÄÄÄÄÄÄ Monitor ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ
```

"Dedicated to the pursuit of security awareness."

```
======================================================================
Volume 2 Number 4                                         October 1992
======================================================================
```

/////////////////////////// In this Issue \\\\\\\\\\\\\\\\\\\\\\\\\\\\

///

BPD SECURITY INTERVIEW

Editor's Note: The following interview was conducted by Jim Thomas, Department of Sociology, NIU, Dekalb, Il., editor of Computer underground Digest (CuD), August 12, 1992. Permission to reprint the article has been given by the editors of CuD. Computer Underground Digest is an open forum dedicated to sharing information among computerists and to the presentation and debate of diverse views.

(MODERATOR's NOTE: We heard about the AIS BBS from several readers, and checked it out. We were impressed by the collection of text files, the attempt to bring different groups together for the common purposes of security and civilizing the cyber frontier, and the professionalism with which the board is run. AIS BBS is a first-rate resource for security personnel who are concerned with protecting their systems).

THOMAS: What is this Board? (Name, number, who runs it (dept & sysop). What kind of software are you using? When did the board go on-line?

CLANCY: The Bulletin Board System (BBS) is run by the Bureau of the Public Debt's Office of Automated Information System's Security Branch. The mission of the Bureau is to administer Treasury's debt finance operations and account for the resulting debt. The OAIS Security Branch is responsible for managing Public Debt's computer systems security. The AIS BBS is open to the public and the phone number for the Board is (304) 420-6083. There are three sysops, who manage the Remote Access software. The BBS operates on a stand-alone PC and is not connected to any other Public Debt system. The Board is not used to disseminate sensitive information, and has been up operating for the past 15 months.

THOMAS: What are the goals and purposes of the Board?

CLANCY: The BBS was established to help manage Public Debt's security program. Security managers are located throughout Public Debt's offices in Parkersburg, WV and Washington DC. The security programmers saw a need to disseminate large amounts of information and provide for communication between program participants in different locations. Because the Board was established for internal purposes, the phone number was not published. However, the number was provided to others in the computer security community who could provide information and make suggestions to help improve the Bureau's security program. Gradually, others became aware of the Board's existence.

THOMAS: What kinds of files and/or programs do you have on the Board? Why/how do you choose the files you have on-line?

CLANCY: There is a wide variety of files posted. In the beginning, we posted policy documents, newsletter articles from our internal security newsletter, bulletins issued by CERT, such as virus warnings, and others for internal use. I located some "underground" files that described techniques for circumventing security on one of the systems we manage. The information, from

Phrack magazine, was posted for our security managers to use to strengthen security. When we were called by others with the same systems, we would direct them to those files as well. Unexpectedly, the "hacker" that had written the file contacted me through our BBS. In his article he mentioned several automated tools that had helped him take advantage of the system. I requested that he pass on copies of the programs for our use. He agreed. This is how our "hacker file areas" came to be. Other hackers have done the same, and we have also received many files that may be useful. It is, indeed, an unusual situation when hackers and security professionals work together to help secure systems. However, this communication has been beneficial in strengthening an already secure system.

THOMAS: Since you and the Secret Service are both part of the U.S. Treasury, was the Board set up to catch "hackers?"

CLANCY: No, the BBS was designed to manage our internal security program. We do not allow individuals to sign on with "handles." We do not know if people are hackers when they sign on unless they identify themselves.

THOMAS: How did you get the idea to set it up?

CLANCY: The security branch accesses many BBSs on a daily basis for research purposes, information retrieval and to communicate with others. Since our security program is decentralized, the BBS seemed to be an effective way of communicating with program participants in diverse locations.

THOMAS: What distinguishes your board from sources like CERT, or from "underground" BBSes?

CLANCY: First, there is a wide diversity to our files, ranging from CERT advisories to the 40Hex newsletters. Also, many of the files on our system are posted as a resource we use for the implementation of our security program. For example, the Board lists computer based training modules that we have developed, policy documents, and position descriptions. These are files that other security programs can use to implement or help start their programs. On the message side of the BBS, what distinguishes it would have to be the open interaction between hackers, virus writers, phone phreaks and the security community.

THOMAS: What kinds of difficulties or problems have you encountered, either from superiors or from users, in operating the Board?

CLANCY: I can recall few, if any, difficulties from anyone, users or superiors. Upper management understands the value of the technology and has been extremely supportive. All users have been courteous, professional, and supportive. Security professionals constantly thank us for providing "underground" information for them. It allows others in the field to gain access to valuable information without having to access "underground" systems. Users appreciate the opportunity to share their knowledge with others and seem grateful to have an avenue to communicate with security professionals who will listen to "hackers" experiences.

THOMAS: Can you describe any unusual or humorous experiences you have had with users while running the Board?

CLANCY: It is unusual for "hackers" and security professionals to work together to help secure systems, but that is what is occurring on our system. I have had requests from other government agencies asking for resumes of "hackers" that may assist them.   I have been contacted by numerous government and private agencies asking for our "contacts." I just direct them to the BBS and advise that they post messages regarding the questions they need answered. If anyone is interested in helping, they will respond. It is an unusual situation, but, in my opinion, I can attest that the information we have received has been very useful to our security program.

THOMAS: What future plans do you have for improving the hardware, such as upgrading modem, number of lines, or storage capacity, or for developing the services of the Board?

CLANCY: Starting July 13th, the Board will be down periodically for system upgrades. We are adding an additional phone line, and a 315 mb hard drive. Also, we are going to make a few changes to reorganize files. It is hoped that group information will be more efficient in this manner. We are also adding RIME relay net conferences and will carry topics such as Data Protection.

THOMAS: What should potential users know about the Board or your policies before attempting to receive access?

CLANCY: Users must be aware that we do not allow handles on the BBS. If they sign on with a handle it will be deleted. We also reserve the right to review all E-mail, public and private. All users have access to the BBS upon sign on. If a user wants access to the "hacker" file area, they need to send a message to the sysop requesting access. Potential users should know they are welcome to call in and communicate with us and others.

---------------------- End of Article --------------------------------

DID YOU KNOW THAT...

Public Debt's ISSMs recently completed Disaster Recovery Training at classes held in both Parkersburg and Washington. The classes consisted of both disaster recovery theory and the use of the Bureau's purchased software product "DISASTAR", which is to be used to prepare each application's own portion of a Bureau wide recovery plan...

There is an ISSM meeting that is held every month. Your ISSM would be happy to hear from you about any computer security questions, issues or concerns that you may have so that they can be addressed at that meeting...

---------------------- End of Article --------------------------------

PUBLIC DEBT "HACKERS"

After reading the article in this issue of the ISSM about our bulletin board system, it is no secret that we actively use hacking tools against our computer systems to test their security. One tool I have used to test our security is called GETIT.COM. (later known as THIEF) . It is a program floating around the underground community designed to capture logonids and passwords for Novell Networks. I must say I found the program pretty impressive. It is extremely easy to use and install and it works wel

Another file not included states that this program can be easily spoofed if a user types "login userid". This allows the program to only capture a password and not the logonid associated with it. Of course, capturing passwords is not a good thing to let happen but at least it does not give a person all the pieces at once. Following is the documentation for the program.

Thief is a TSR (Terminate and Stay Resident) utility written in 8086 assembly language that attempts to steal Novell passwords. It originates from a site with consummate hackers and a long, colorful history of mischief: George Washington High School in Denver, Colorado.

The school is well endowed with a large variety of IBM microcomputers. Five rooms of about 30 computers each are all tied together on a Novell network. Four of the five rooms solely use boot proms* for initializing the workstations. However, the fifth houses IBM PS/2 model 80s with hard drives. The power users tend to congregate in this area, including the "administrators" with Supervisor equivalence. These machines do not use boot proms.

So it was on one of these computers where the "thief" was first discovered because it takes advantage of weaknesses in the security at the boot phase. Into the regular flow of action in the AUTOEXEC.BAT file, the creator inserted a line that executes the (hidden) program copied onto the boot disk. The TSR remains in the background and the process continues. Visual signs of thebreak-in are imperceptible.

Then, as soon as a program named LOGIN is executed, the thief springs to life and records all the keystroke action into a hidden file on the boot disk. The human thief may then later return to the computer and see what the trap caught. Before a more detailed description of the "metabolism" of the thief, consider now the weaknesses that led to the breach:

o a localized boot process, or at least one that is corruptible.

o physical access to a sensitive computer.

Both are controllable, of course. The boot prom is a solution for the former, and lock and key (on the computer or a room that surrounds it) is for the latter. Now return to the "metabolism". Surprisingly, THIEF uses the same "hook" that the Novell shell does! That is, it captures the centralized portal to DOS interrupt 21h.** Then, it intercepts all function calls. Specifically, it checks for the EXECute file function call and the "terminate" interrupt.

Whenever an EXEC call is made with a filename LOGIN, THIEF springs to life and records keystrokes until the program terminates. This is somewhat sophisticated; however, an even more effective method could be realized: it could simply wait for the specialized Novell function call to log in, and record the calling parameters. Note that the above technique requires the program to be loaded subsequent to the Netware shell.

By no means are these types of programs new; they have been around as long as password-based program security. Here, however, is an example that is tangible and immediate. Study of it is beneficial because knowledge of Netware security is one thing; knowledge of how to defeat it is quite another! The latter demands cutting-edge sophistication and comprehension. The future will certainly see improved identification techniques, and timeless, devious ingenuity will be there to greet them.

Note: THIEF was formerly named GETIT by its creator, who was careless and cocky enough to leave the source code.

* "Boot proms", for those not familiar, are accessory chips that reside on network interface cards; they redirect local drive activity to the server during the boot process, thus allowing a

workstation to initialize without a (boot) disk.
** Interrupt 21h is that used by any program when requesting a DOS function. The Netware shell, of course, intercepts this regular flow. It may pass the information directly along to DOS or process the call itself.

------------------------ End of Article --------------------------------

CLYDE'S SECURITY HALL OF FAME

Office of Public Debt Accounting (OPDA) inducted to Hall of Fame:

Through their dedication and commitment to information security, they have helped Public Debt's security program grow. OPDA management has dedicated the time and resources to ensure that security issues are addressed to the utmost degree of accuracy and completeness. OPDA management recently mandated that all of their users receive a two hour end user security training class. This was above and beyond the security training requirements currently being fulfilled with the ISSM newsletter. OPDA ISSMs, Sa
ndra Woods, Mike Goodwin, and Alex Kendjoria-Ganoe have assisted the AIS Security Branch in developing procedures and guidelines that will assist other ISSMs when its "their turn" to complete the same tasks. Their dedication and assistance has been extremely beneficial to the development of Public Debt's security program. OPDA'a ISSMs have gone out of their way to tutor themselves in computer security topics. They have utilized the automated lesson plans made available on our LAN and made extensive use of our security library books, magazines, videos and audio tapes. OPDA has shown that the ISSM program works when the proper time and resources are dedicated to the management of information systems security.

Submitted by Kim Clancy, Manager of the AIS Security Branch

------------------------ End of Article --------------------------------

"DEAR CLYDE..."

(Responses to questions for those who are searching for the truth.)

Dear Clyde;

I have a personal computer (PC) on my desk in the office. What types of security controls do I need to protect my computer?

PC (perplexed and confused)

Dear PC;
The greatest measure of security you can provide to your PC is to physically secure it so that no one can gain access to it. If that is not possible, look for methods that will prevent someone from powering up the computer or using the keyboard. If I can gain access to your computer, I have the capability to load programs (called trojan horses, these are not the same trojan horses from my day but follow the same logic) that can capture you logonids and passwords as you sign on to systems. That means I can act as you on the computer and everything I do will be traced to you, not me. If you leave your PC on at night with a modem set up so that you can call in from home, you've made it possible for me to load the same programs without having to gain physical access to your computer. That type of configuration should be reviewed by your ISSM before setting it up.

-------------------------- End of Article ------------------------------

COMPUTER SPEAK COMPUTER TERMS AND THEIR MEANINGS

CYBER - As in CYBERSPACE
Term used to describe the electronic "playground" in which computerists use, publish and share information with distant computer users and electronic bulletin boards.

SUPERVISOR -
1) Network Supervisor - Person responsible for the smooth operation of the entire network. The supervisor may also install the network, maintain the network, reconfiguring and updating it as the need arises.
2) SUPERVISOR (as user) - Special username that is automatically created when a file server is initialized. This user is permanent and cannot be deleted or renamed. The user SUPERVISOR has all rights in all file server volumes and directories, and these rights cannot be revoked.

CERT - Computer Emergency Response Team

--------------------------- End of Article -----------------------------

VOICE MAIL TOLL FRAUD

For computer hackers, PBX toll fraud has become an annual $500 million boon. For corporations, it's become a $500 million nightmare. Since only a fraction of PBX toll fraud is actually reported and compiled, this $500 million per year estimate is a rather modest one. Historically, hackers broke into a PBX through its Direct Inward System Access (DISA) feature. DISA allows travelling employees to call into a switch and avail themselves of a company's long distance services. All too often, it is now offering hackers the same privilege.

Once a hacker has cracked a four- or six-digit DISA code, he can commandeer the long distance lines for his own unauthorized use. DISA-based toll fraud remains the simplest and most prevalent form of PBX toll fraud. Until recently, it was considered the ony form.

Jim Ross is president of Ross Engineering (Sterling, VA), a surveillance counter-measures firm. During the past month, he received two highly unusual complaints of PBX toll fraud. Instead of using DISA, the culprits broke into the PBX through the voice-mail system. They were able to whisk right through voice mail, obtain dialtone and make thousands of dollars worth of international calls.

"In the first instance," Jim recall, "the toll fraud artists dialed into an Octel voice-mail system with Aspen software and attached to an AT&T System 75 PBX. After hours, incoming 800 callers could grab dialtone after punching in any three digit sequence with '75' in it and dial into the outside world." The company was taken for a $170,000 long distance ride.

Jim stresses that all voice-mail systems "have some kind of vulnerability and, sooner or later, the hackers are going to pinpoint it." In fact, he is quite surprised that it has taken them so long to discover this new point of entry. "The easiest way to prevent these assaults is to program your PBX to shut down immediately whenever the caller reaches a second dialtone," he advises. "Without the second dialtone, their hands are tied."

Evasive Tactics

Toll fraud felons are experts in evasion. Typically, they'll bounce the call from one to another, switching interexchange carriers several times before they invade the targeted PBX. They'll make the calls from transient numbers, as opposed to their home phones. These evasive tactics make them quite difficult, and sometimes impossible to trace.

Jim Ross provides an intriquing example. "A few years back, a Harrisburg, PA, company called us for assistance. They were getting burned badly. Every night, the hackers dialed up their DISA number and made thousands of dollars of calls to a single number in Columbia."

Although the company had recognized the problem, and had changed the DISA access code from four to six digits, they could not stop the deluge of unauthorized outbound calls. They eventually had to shut their PBX down while the local phone company investigated the matter.

The investigation led from the local telco to AT&T, the interexchange carrier, and on to the originating telco, New York Tel. By the time New York Tel managed to locate the originating numbers, they had been terminated. But they were able to outline the makings of a clever, evasive and quite successful method of PBX toll fraud.

According to New York Tel records, a mysterious company had put in a request for 12 new telephone lines. The company claimed to be a construction firm. Although they were planning to put up a major office tower, they had no references, and no credit history to speak of.

New York Tel demands a healthy deposit to service such a shaky entity. The company paid the deposit in cash. New York Tel duly installed the 12 lines at a trailer on the edge of the alleged construction site.

After a month, the company abandoned the deposit and the site. But not before running up thousands of dollars in long-distance charges on the Harrisburg PBX. And probably several other switches as well.

Some External Measures

In addition to implementing toll restriction, daily diagnostics and other PBX procedures, there are several external ways to control toll fraud. A few companies are now issuing DISA smart cards, with ID numbers which change every minute. These cards are virtually impervious to outside meddling.

Smart cards are not cheap. They are an administrative pain. And it is often quite difficult to get the card back after an employee resigns or quits. However, it remains one of the most effective alternatives currently available.

Our own solution was to get rid of DISA altogether. In its place, we'd distribute corporate credit calling cards. Each card would be attached to the company account, not to its CO trunks. Each would have a unique credit card number.

Thus, when an employee is terminated, so is his credit card number. If the card is stolen, the employee will report it immediately and the other travelling execs could make calls as usual. If $500 worth of calls were made to Pakistan in the course of an hour, the carrier could call the user's beeper or the company headquarters. If neither responded, they could void the card automatically.

"As far as the telecom industry is concerned, that's an excellent idea," responds Jim Ross. "But it won't be acceptable to the travelling executives.

"You've got to understand. These guys get to be such big wigs and muckety-mucks that they don't want to fool around with a nine digit credit card number, plus the seven-digit long distance number. The idea of dialing a few extra digits is an intolerable burden to them.

"As a corollary, you may remember that former secretary of state Alexander Haig made a number of calls to the While House from Air Force One. This exchange was recorded by short wave radio enthusiasts, who handed it over to the media." Faced with the flak, the goverment contended that the encryption equipment in the plane was just not compatible with that in the White House.

"Nonsense," says Jim. "Like many executives and high officials, Haig just didn't want to go through the hassle of using the encrytion equipment or the hardship of listening to a warped, encrypted voice. Look at (Virginia) Governor Wilder. He talks about his nemesis, Senator Robb, in the clear."

Jim asserts that there is only one foolproof method to eliminate toll fraud. "If the FCC would demand that all interexchange carriers and local telcos implement comprehensive, compulsory caller identification, then you've done away with the problem. You've also done away with bomb threats, harassment and obscene phone calls, as well."

Even the most evasive hackers would be instantly identified at each point along their tortuous journey -- from town to town, and from carrier to carrier. And they would open themselves to exposure and apprehension, in real time.

Furthermore, hackers can not mask Automatic Number Identification (ANI) by obscuring digits. Because caller identification data is entered from your exchange, and not from your phone, it is impervious to meddling. Hackers could only avoid ANI detection by dialing for live operator assistance. Which carries its own threat of exposure.

"Unfortunately, universal, compulsory caller identification is 'pie-in-the-sky' at this juncture," laments Mr. Ross. The Pennsylvania Supreme Court has already prohibited caller ID, citing right to privacy violations. Even where the service is currently offered, subscribers have the right to withhold their phone numbers from public inspection.

The CIA would be a fine source for toll fraud prevention. "Without doubt, our neighbors in Langley have purchased practically every modern PBX and voice mail system to see what their weaknesses are," assents Jim. "I wish that this information would be made public. I think it should be made public, since it is paid for with our tax dollars."

That's only one of several things the CIA does that the American people get no value from, the interviewer quipped.

Reprinted with permission of Teleconnect Magazine 800-799-0345
Subscription $15 per year

----------------------- End of Article ------------------------------

COMPUTER SECURITY DAY

December 1, 1992 will mark the fifth annual nation-wide observance of Computer Security Day. Computer Security Day is our opportunity to focus attention on our agenda - Computer Security. Computer Security Day is the first workday in December, although official observances vary to avoid conflicts in some countries or in some organizations. Computer Security Day keeps everyone alert to proper computer security procedures as the holiday season approaches and security might otherwise become lax.

The Bureau of Public Debt will participate this year in Computer Security Day by holding a contest to select the best security slogan as submitted by the ISSM Newsletter readership.

The slogan can relate to any computer security-related topic, such as access security ("Logoff! - An open terminal is a hacker's terminal!"), or password security ("Share a Password, Share your Protection!").

First through third prizes will be awarded and will consist of basketball hoop security reminders, as displayed throughout BPD, Parkersburg. Winning and runner-up slogans, plus the name of the submitter, will be printed in future issues of the ISSM Newsletter, & be posted on physical security bulletin boards throughout the building.

---------------------------- End of Article --------------------------

>>

The AIS Security Branch Runs an Electronic BBS. Give us a call at (304) 420-6083. An electronic version of the ISSM is posted on the board and can be downloaded. Articles in the electronic version may include more detail in that we are not limited by space constraints as we are in the paper copy.

>>

The ISSM is a quarterly publication of the Department of Treasury, Bureau of the Public Debt, AIS Security Branch, 200 3rd Street,

Parkersburg, WV 26101 (304) 420-6368.
Editors: Jim Heikkinen, Ed Alesius, Kim Clancy, Joe Kordella, Mary Clark