```
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 ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ
```

Dedicated to the pursuit of security awareness.............

==
Volume 3 Number 1   January 1993
==

In This Issue:

Securing Your Phone Switch

Virus Alert

Social Security Numbers & Privacy

Clyde's Computer Security Hall of Fame

Dear Clyde

COMMCRYPT Lives

Computer Speak

Computer Security Day Slogan Contest Winners

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: Ed Alesius
           Kim Clancy
           Joe Kordella
           Jim Heikkinen
           Mary Clark

Securing Your Phone Switch

By Dave Goldsmith, a student at Rockland Community College. He is working towards a degree in Computer Science. His hobbies include learning other technologies to include telephone systems and switches. He also edits an electronic magazine that focuses on computer technology issues.

"If it has a dialup, a hacker can abuse it". This, as some companies have already found out, applies to the System 75 telephone system. Hackers have, within the last year, figured out how to penetrate and manipulate a System 75. This gives them complete control over your PBX. If you allow them to get access to the controller, they will end up setting up a DISA (Direct Inward System Access), and make outgoing phone calls on YOUR bill. This can result in thousands of dollars in fraudulent telephone calls, that you are going to have to pay. Even if you decide to battle it out in courts, it is going to cost. In this article, I plan to outline the steps to secure your System 75.

One question you should ask yourself is "Do I really need DISA on my system?". I highly discourage having DISA, as it increases the chance of being a victim of toll fraud. If it is vital for your employees to use DISA, then I suggest that you have a barrier code of at least 7 digits. Any less then that is a definite security risk.

If a hacker has already penetrated your system, there are some tell-tale signs. Logon to your system and type 'DISPLAY REMOTE-ACCESS' followed by a carriage return. If you haven't set up a DISA, then there shouldn't be an extension number. If there is one, type 'CHANGE REMOTE-ACCESS' and remove the extension. That will remove the DISA, and is the start of locking the hacker out of your system. Your next step will be to change the passwords on ALL of the accounts. The common login/password combinations that hackers use are:

cust	custpw
rcust	rcustpw
browse	looker
craft	craftpw

It is my recommendation that you change ALL of the passwords on the system. Be warned, you should change the passwords to something alpha numeric, and it should be something personal, so a hacker can't attempt to brute force any of the accounts. If you find that you can't change browse's password, don't despair. Login under one of the higher level accounts, and type 'CHANGE PERMISSIONS BROWSE'. Then strip browse of all of its privileges. This will keep hackers from displaying remote-access and finding out where your DISA is, if you have one.

To ensure system security, it is suggested that you DISPLAY REMOTE-ACCESS on a fairly regular basis, just to make sure that your system remains untouched.

Editors Note: Issue 41 of Phrack magazine was recently released and contains another article on hacking this phone switch. Phrack 41 is available on the AIS BBS. Information on the BBS can be found on Page 4.

************* End of Article ****************

Virus Alert

Free diskettes distributed by the Cobb Group at the Federal Computer Conference December 8, 9, or 10, may contain a virus which is very difficult to detect. One diskette has a blue label with the words "DOS/Software Connection" in large print. The other has a red label with the words "Windows/ Software Connection" in large print. If you or anyone you know has received such a diskette, please do not use it in any computer. The virus detection software installed on your computer will not detect the virus. Bring the diskette to your Information Systems Security Manager (ISSM) or call the AIS Security Branch at (304) 420-6355.

************* End of Article ****************

Social Security Numbers & Privacy

by Chris Hibbert
Computer Professionals for Social Responsibility
Reprinted with permission from 2600 Magazine

(Kim Clancy was recently training Public Debt employees in Washington D.C. on computer security. Her approach to computer security training is to first convince class participants that the information they are being asked to protect is worthy of protection. She mentioned the following article regarding the protection of social security numbers and stated that it is important that as employees of Public Debt we understand the value of a social security number, both for our clients protection and also on a personal basis for our own protection. Many members of the class requested a copy of the following article initially published in 2600 magazine (it was also published in Phrack issue 35). We have received permission from 2600 to reprint the article.)

Many people are concerned about the number of organizations asking for their Social Security Numbers. They worry about invasions of privacy and the oppressive feeling of being treated as just a number.

Unfortunately, I can't offer any hope about the dehumanizing effects of identifying you with your numbers. I *can* try to help you keep your Social Security Number from being used as a tool in the invasion of your privacy.

Surprisingly, government agencies are reasonably easy to deal with; private organizations are much more troublesome. Federal law restricts the agencies at all levels of government that can demand your number and a fairly complete disclosure is required even if its use is voluntary. There are no comparable laws restricting the uses non-government organizations can make of it, or compelling them to tell you anything about their plans. With private institutions, your main recourse is refusing to do business with anyone whose terms you don't like.

Short History

Social Security numbers were introduced by the Social Security Act of 1935. They were originally intended to be used only by the social security program, and public assurances were given at the time that use would be strictly limited. In 1943 Roosevelt signed Executive Order 9397 which required federal agencies to use the number when creating new record-keeping systems. In 1961 the IRS began to use it as a taxpayer ID number. The Privacy Act of 1974 required authorization for government agencies to use SSNs in their data bases and required disclosures (detailed below) when government agencies request the number. Agencies which were already using SSN as an identifier were allowed to continue using it. The Tax Reform Act of 1976 gave authority to state or local tax, welfare, driver's license, or motor vehicle registration authorities to use the number in order to establish identities. The Privacy Protection Study Commission of 1977 recommended that the Executive Order be repealed after some agencies referred to it as their authorization to use SSNs. I don't know whether it was repealed, but that practice has stopped.

The Privacy Act of 1974 (5 USC 552a) requires that any federal, state, or local government agency that requests your Social Security Number has to tell you three things:

1. Whether disclosure of your Social Security Number is required or optional;

2. What law authorizes them to ask for your Social Security Number; and,

3. How your Social Security Number will be used if you give it to them.

In addition, the Act says that only Federal law can make use of the Social Security Number mandatory. So anytime you're dealing with a government institution and you're asked for your Social Security Number, just look for the Privacy Act Statement. If there isn't one, complain and don't give your number. If the statement is present, read it. If it says giving your Social Security Number is voluntary, you'll have to decide for yourself whether to fill in the number.

Private Organizations

The guidelines for dealing with non-governmental institutions are much more tenuous. Most of the time private organizations that request your Social Security Number can get by quite well without your number, and if you can find the right person to negotiate with, they'll willingly admit it. The problem is finding that right person. The person behind the counter is often told no more than "get the customers to fill out the form completely."

Most of the time, you can convince them to use some other number. Usually the simplest way to refuse to give your Social Security Number is simply to leave the appropriate space blank. One of the times when this isn't a strong enough statement of your desire to conceal your number is when dealing with institutions which have direct contact with your employer. Most employers have no policy against revealing your Social Security Number; they apparently believe the omission must have been an unintentional

Lenders and Borrowers

Banks and credit card issuers are required by the IRS to report the SSNs of account holders to whom they pay interest or when they charge interest and report it to the IRS. If you don't tell them your number you will probably either be refused an account or be charged a penalty such as withholding of taxes on your interest.

Insurers, Hospitals, Doctors

No laws require medical service providers to use your Social Security Number as an ID number (except for Medicare, Medicaid, etc). They often use it because it's convenient or because your employer uses it to certify employees to its groups health plan. In the latter case, you have to get your employer to change their policies. Often, the people who work in personnel assume that the employer or insurance company requires use of the SSN when that's not really the case. When my current employer asked for my SSN for an insurance form, I asked them to try to find out if they had to use it. After a week they reported that the insurance company had gone along with my request and told me what number to use. Blood banks also ask for the number but are willing to do without if pressed on the issue. After I asked politely and persistently, the blood bank I go to agreed that they didn't have any use for the number, and is in the process of teaching their receptionists not to request the number.

Why Is The Use of Social Security Numbers A Problem?

The Social Security Number doesn't work well as an identifier for several reasons. The first reason is that it isn't at all secure; if someone makes up a nine-digit number, it's quite likely that they've picked a number that is assigned to someone. There are quite a few reasons why people would make up a number: to hide their identity or the fact that they're doing something; because they're not allowed to have a number of their own (illegal immigrants, e.g.), or to protect their privacy. In addition, it's easy to write the number down wrong, which can lead to the same problems as intentionally giving a false number. There are several numbers that have been used by thousands of people because they were on sample cards shipped in wallets by their manufacturers (one is included below).

When more than one person uses the same number, it clouds up the records. If someone intended to hide their activities, it's likely that it'll look bad on whichever record it shows up on. When it happens accidently, it can be unexpected, embarrassing, or worse. How do you prove that you weren't the one using your number when the record was made?

A second problem with the use of SSNs as identifiers is that it makes it hard to control access to personal information. Even assuming you want someone to be able to find out some things about you, there's no reason to believe that you want to make all records concerning yourself available. When multiple record systems are all keyed by the same identifier, and all are intended to be easily accessible to some users, it becomes difficult to allow someone access to some of the information about a person while restricting them to specific topics.

What Can You Do To Protect Your Number?

If despite your having written "refused" in the box for Social Security Number, it still shows up on the forms someone sends back to you (or worse, on the ID card they issue), your recourse is to write letters or make phone calls. Start politely, explaining your position and expecting them to understand and cooperate. If that doesn't work, there are several more things to try:

1. Talk to people higher up in the organization. This often works simply because the organization has a standard way of dealing with requests not to use the SSN, and the first person you deal with just hasn't been around long enough to know what it is.

2. Enlist the aid of your employer. You have to decide whether talking to someone in personnel, and possibly trying to change corporate policy is going to get back to your supervisor and affect your job.

3. Threaten to complain to a consumer affairs bureau. Most newspapers can get a quick response. Some cities, counties, and states also have programs that might be able to help.

4. Tell them you'll take your business elsewhere (and follow through if they don't cooperate).

5. If it's a case where you've gotten service already, but someone insists that you have to provide your number in order to have a continuing relationship, you can choose to ignore the request in hopes that they'll forget or find another solution before you get tired of the interruption.

If someone absolutely insists on getting your Social Security Number, you may want to give a fake number. There is no legal penalty as long as you're not doing it to get something from a government agency or to commit fraud. There are a few good choices for "anonymous" numbers. Making one up at random is a bad idea, as it may coincide with someone's real number and cause them some amount of grief. It's better to use a number like 078-05-1120, which was printed on "sample" cards inserted in thousands of new wallets sold in the 40s and 50s. It's been used so widely that both the IRS and SSA recognize it immediately as bogus, while most clerks haven't heard of it. It's also safe to invent a number that has only zeros in one of the fields. The Social Security Administration never issues numbers with this pattern. They also recommend that people showing Social Security cards in advertisements use numbers in the range 987-65-4320 through 987-65-4329.

The Social Security Administration recommends that you request a copy of your file from them every few years to make sure that your records are correct.

************* End of Article ****************

CLYDE'S Computer Security Hall of Fame

The Savings Bond Operations Office (SBOO) Division of Accounts and Reconcilements (DAR) has been inducted to the Computer Security Hall of Fame.

The SBOO/DAR's dedication to the Bureau of Public Debt's computer sercurity program has consistently been evident in all aspects of their computer security administration. SBOO/DAR ISSM's, Glenn Siber, Liz Abram, Sharon Abbott, Don Hainkel, and Tom Jamison have pioneered the ISSM's role in administering computer access capabilities by being the initial ISSM group to interact with the AIS Security Branch in administering user logonid password resets, reviews, etc. utilizing ACF2 software.

SBOO/DAR ISSMs have promoted security awareness training not only to their own personnel through distribution of the ISSM newsletter, but also distribute copies of the newsletter to all of the FRBs. They have consistently dedicated their time and resources to ensure that computer security awareness and computer security issues are addressed not only throughout their organization, but also others that interface with the Bureau.

SBOO/DAR's dedication, interest, and leading edge participation to all aspects of the Bureau of the Public Debt's computer security program is of the type that makes any undertaking successful.

Submitted by Kim Clancy, Manager of the AIS Security Branch, and Ed Alesius

************* End of Article ****************

"Dear Clyde;"

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

Dear Clyde;

One day, while I was away from my desk, someone sent an E:Mail message to my boss that said "Bite It". Since it was sent from my PC, my boss thought I had sent the message. Needless to say, I was in big trouble with the boss. Isn't it an invasion of my privacy for someone else to use my CC:mail?

Miss Imin Bigtrouble

Dear Imin,

Yes it is an invasion of your privacy when someone else uses your CC:mail, however you can easily prevent this type of invasion by simply remembering to secure your PC whenever you are leaving the area. If you log out, or activate software that requires your password to be entered prior to your PC being able to be used, you will prevent this type of situation.

Remember to protect your logonid as you would your credit card. Don't make it available for someone elses use, the consequences can be very expensive.

Send your comments or questions to Clyde c/o the AIS Security Branch in Parkersburg, Room 1013, or leave them in Clyde's mailbox located on the Security bulletin boards throughout the Parkersburg office.

************* End of Article ****************

COMMCRYPT Lives!

by Jim Heikkinen

"SCANNER" grafted to Public Debt network servers!

During the month of December, an ad hoc group consisting of Jim Heikkinen, Joe Kordella (Security Branch), Richard Montalbano, and Dave Frietsch (LAN Committee) sucessfully developed and implemented a plan that will scan the Bureau's NOVELL network file servers for viral infestations.

The plan called for installation of an anti-virus software package named COMMCRYPT, and was to be carried out in two phases.

Phase one called for the continuous scanning of each server for viruses. This was accomplished with the installation of Scan Plus, one of the two main ingredients in COMMCRYPT. The implementation of this phase was accomplished by December 14. The second and final phase, the installation of Detect Plus, was in place two days later on Wednesday, December 16th. This phase consists of comparing the "signatures" of executable files of each server against those previously captured in a hopefully virus-free file list called a "watchlist".

Should either Scan Plus or Detect Plus encounter suspicious activity, a notice is automatically sent to the Help Desk for immediate resolution.

Prior to the installation of COMMCRYPT, a user-centered scheme relied heavily on the individual computer user as the first line of defense against viral infection. Security awareness programs are in place that promote the use of virus detection software, etc., and have been regarded as generally successful.

Recently however, the server-centered philosophy suggested the computer user should, but might not always offer the level of protection needed to continually safeguard every BPD network.

COMMCRYPT will provide that protection at a minimal cost in server performance.

An expanded team has been developed to review network scanners recently released on the market to ensure that the greatest level of protection is provided for Public Debt computer resources.

************* End of Article ****************

COMPUTER SPEAK

COMPUTER TERMS AND THEIR MEANINGS

scanner.......... Software that is designed to help identify viruses within files, boot sectors, partition tables, memory, and other hiding places; to name them; and potentially to help remove them.

PBX.............. A telephone system operating within one building, company, etc. and having outside telephone lines.

access controls.. Restrictions on the ability of a subject (e.g., a user) to use a system or an object (e.g., a file) in that system. Such controls limit access to authorized users only. Access control mechanisms may include hardware or software features, operating procedures, management procedures, or any combination.

********** End of Article *************

Computer Security Day Slogan Contest Winners

Congratulations! The following are the award winning Computer Security Slogans that were submitted by ISSM Newsletter readership. The slogan selection committee was so impressed with the quality of the slogans that they unanimously decided to award a prize to each entrant.......

Brenda McFarland; DTRA-3

Keep your PC secure,
And don't ever slack,
Or you could be the victim
Of a big hack attack.

Barb Milliron; DDS/Data Retrieval

A virus is to a computer
What AIDS is to a human.
Protect your computer
As you would yourself.

Ken Kirby; OAIS/ASD/WTB

Security and Securities
You have to invest.

Becky Marks; OA/Search & File

As the day enters night
Your machine enters QUIeT.

Rick Montalbano; DPC/Communications Branch

Your data, Your job... Protect them both.

A BPD man shared his password
In security, felt his was the last word.
A disgruntled employee
Logged into his PC.
His now scrambled is data back-s-wards!

Kaye Dobson; DTS/Software Branch

Keep it SHUT
Lock it UP!

Keep it Clean
Clear the Screen.

Lee Ohringer; Engraving & Printing

PSSST. Can you keep a secret? Begin with your password.

At BPD we Backup and Protect our Data.

Don't let them "Read your bits" -- Logoff and lock up.

Comp?ter sec?rity is not right without "U".

Patina V. Waters; Securities Audit Section

A password unprotected is an invitation for data elimination.

Disks on the go can carry viruses unknown.

Steve Berenson/Mary Davis-Demick; DPPA

Protect your PC: Practice safe software.

*********** 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.