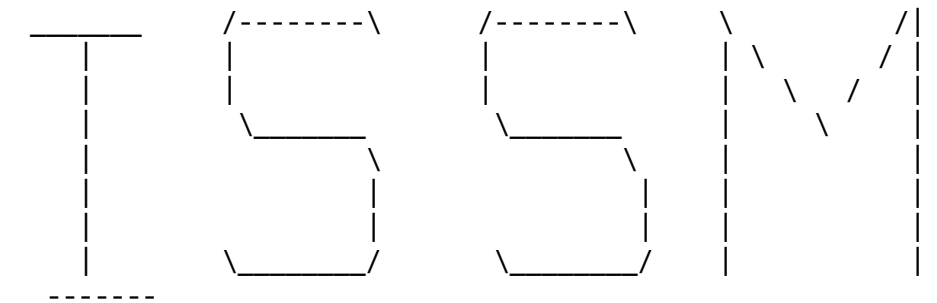
The Information Systems Security Monitor



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

==========

Volume 2 Number 1 January 1992

==========

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

\\

ONE NERD'S APPROACH TO COMPUTER SECURITY

Hi, my name is Bill Strouse and I'm a NERD (Network Emergency Repair Dude). I've been a Sysop or systems operator now for better

than a decade and I've learned a great deal about human nature and

security in general.

Back in 1980 it dawned on me that if I connected a modem to my computer I could access it from anywhere I happened to be. But I

would have to have some sort of security or others would be

accessing it, possibly in a destructive way. The solution I decided on was to setup a bulletin board system that used a combination of a unique name and password for each caller to control what that caller had access to. Once I got the system working I found it was a great way to keep in touch with friends that also had modems and an even better way to get answers on technical problems. Plus the latest PD (public domain) software regularly showed up on my hard disk. I publicized the number in electronic lists that were distributed worldwide and was soon getting calls from all over the continent and foreign countries like Sweden, England and Australia. I soon had one of the best collections of PD software in the country and the phone line was in constant use day and night.

Along with all the great people I met there were always those few who had nothing better to do than try to destroy or disrupt what others had built. One of the first things I learned was not to allow just anyone the ability to leave public electronic mail. Kids would call and leave grossly obnoxious public messages with all sorts of foul language. We devised a system whereby a caller could only leave a message to the Sysop on the first call then we would call them back voice and verify who they were. Most importantly we had verified they were connected to a legitimate phone number which could be traced to a physical location and person. After verification their security level was raised so they had full access and an hour of system time a day. One of the next lessons I learned was not to allow anyone to upload a program they could then execute on the system. A friend, who continually worked at busting the security to see if he could find holes uploaded a

game with a hidden copy of BASIC embedded in the program. When he ran the program online he could issue a control code and jump to the interpreter which allowed him to walk all over the security like it didn't exist! After that all files were uploaded to a private area no one but the Sysop had access to till they were thoroughly inspected.

By 1985 I had so many people asking for help with computer related problems I went into business for myself as a VAR, or Value Added Reseller. Someone who not only sells you the goods but sticks around and makes them work for you. Not long after that networking looked like it might be the wave of the future. Since a network was a shared resource, similar in nature to a bulletin board system and even used a name and password for security I was right at home. And I learned even more about security.

Number one. The weakest link in security is the employee using the computer! They put their password on a sticky note and paste it on their monitor so they don't forget; loan their account to fellow employees; use passwords such as "secret", "love", or their social security account number (every 14 year old wanna-be hacker has the list of most commonly used passwords). They go to lunch and leave their workstation logged into accounting records, bring in new (virus infected) programs they want to use at work and just generally gum up the (security) works. A good employee security education program is worth its weight in gold.

And, security must be physical as well as electronic. I read a book about a group of young hackers (Inner Circle) that could not

gain access to a mainframe because the security was well designed

so they posted a kid in the lobby of the company with a questionnaire. He passed himself off as a high school student who

had been given an information gathering assignment as a school project. Some of the questions asked were "What is your first and

last name", "Do you use a computer at work", "Are you married",

"What's your wife's name". Needless to say they were into the system within days.

Mainframe managers are somewhat aware of this and protect their

iron (computers) from anyone without proper authority but most of

the LANs (Local Area Networks) I've worked with are in an area that's easily accessible by anyone. Remember, something as simple

as a cup of coffee, or a boot disk with the proper utilities in

the hands of a disgruntled stockboy can turn your data into random

1s & 0s and truly ruin your day, if not your career.

The system I run is called The Ring of Fire after the tectonic plate we live on the edge of here in California. Over time it has

grown to four (4) phone lines and over 350 megabytes of downloadable software packages and graphics images. There are well over 1,000 regular callers and the system averages about 3,000

calls a month but the electronic mail is where the real action is.

The E-mail is shared with other similar computer systems all over

the US and some foreign countries. Callers can leave a message in

a conference and it will show up on other systems all over the

country. Replies are automatically routed back to the originator

and show up as return mail addressed to that person. Thus, callers

can converse with a large number of diversely scattered individuals

at minimal cost (usually a free local phone call). To further reduce online time we support SLMR off-line mail reader. With it

you can download a compressed mail packet of pre-specified conferences then read and reply off-line with a full screen editor and upload a compressed set of replies.

All of this runs on a Novell network that spans several computers

and large hard disks, a read/write CD, Fax server AND all of our

inhouse workstations. Hopefully, I'll see you online and we can

continue this as an interactive discussion ;-).

Author bio:

Bill Strouse has been a systems analyst for more than twenty years now and has worked as a consultant for IBM, Amdahl, Ford Aerospace and Stanford University's SLAC (Stanford Linear Accelerator).

Bill Strouse has been telecommuting since 1980 when he started his first electronic bulletin board service, back in the CP/M days. He has been the system operator ever since and currently has one of Silicon Valley's most popular boards, the Ring-of-Fire, at 408-453-3326 and 408-453-2460. He was President of PRACSA (Public Remote Access Computer Standards Association) for many years before leaving three years ago to found and become President of United Sysop's Association, an organization of bulletin board system operators and users.

Mr. Strouse is a president of Stoney River Networks, an authorized Novell Reseller. His company has installed many remote communication systems for various clients. He is also President and Co-founder of the Silicon Valley Novell User Group and serves on the Board of the Northern California Netware User's Association. Bill is also the editor of NetWare News, the newsletter of the California Netware Users Association.

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

WHAT DID CLYDE SAY?

It's been brought to our attention that everyone that reads the ISSM isn't always well versed in computer terminology. Well, in an effort to remedy that situation we will be providing an article called "Computer Speak", starting in this issue, that will be devoted to getting every reader to understand computer jargon.

We appreciate hearing from our readers about any items or topics that they would like to see appear in the ISSM. So let's keep hearing from you. Just drop a note to Clyde or call.

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

DIGITAL SIGNATURES STILL ARE MYSTERY TO MANY IN GOVERNMENT

By Darryl K. Taft

A fight has erupted over the government proposal of a new standard for digital signatures, and questions remain as to just what a digital signature and public-key encryption actually are.

The National Institute of Standards and Technology has proposed a standard for digital signatures that would securely verify a message sender's identity.

Miles Smid, manager of the security technology group in NIST's Computer Systems Laboratory, defined a "key" as a binary number used with an algorithm to encipher or decipher data.

Public-key encryption requires the use of a matched pair of such keys for each user, one that is publicly known and one that is private and known only to the user. More traditional data encryption methods, like the government's Data Encryption Standard (DES), require only one key to encipher and decipher data.

Under the old method, "if I were to scramble a message with my secret key, the only way you could descramble it would be to use my key," Smid said. DES requires exchanging secret encryption keys with each party, thus requiring prior relationships.

However, rather than using the same key to both encrypt and

decrypt the data, public-key encryption uses a matched pair of encryption and decryption keys. Each key performs the inverse function of the other.

Thus, a user makes his public-key publicly available, perhaps via a directory or certifying authority, and keeps his private key secret. To send a private message, an originator scrambles his entire message using his intended recipient's public key. Once this is done, the message can only be decoded with the recipient's private key.

Inversely, a sender also can work over a file using his private key, and it can only be decoded using that sender's public key.

This provides the basis for the digital signature, because if you can unscramble a signature in a message with someone's public key, they had to use their private key to scramble it in the first place.

The proposed standard, known as the Digital Signature Standard (DSS) is based on a digital signature algorithm (DSA) derived from a concept known as ElGamal encryption. It is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage and other applications that require data integrity assurance and data origin authentication.

NIST, on Aug.30, proposed to adopt the DSS as a Federal Information Processing Standard (FIPS). The proposed standard specifies a digital signature algorithm based on a public key.

The government's DSS is not intended to encrypt the data in a message, but primarily to authenticate. The DSS is intended to verify the author and verify the integrity of the data in the message.

Public-key encryption algorithms are based upon what are known as "hard problems," Smid said. These hard problems are mathematical

operations involving very large numbers. The government's proposed DSS uses one of a variety of public-key encryption algorithms, Smid said.

The NIST proposal's scheme differs markedly from that of a popular encryption system from RSA Data Security Inc. of Redwood City, Calif. The difference lies in the algorithms used to encrypt and decrypt data. Smid said the RSA algorithm is based on the difficulty of factoring very large numbers. This involves finding a number that is the product of two other numbers.

Breaking that system for a small number would be pretty simple, "but if I give you a large number, like 150 digits, that would be difficult. Factoring very large numbers is a difficult problem," he said.

The algorithm used in the NIST proposal is based upon the difficulty of finding discrete logarithms. Essentially, this method involves finding the remainder left over when you divide one number by another one. Again, when dealing with very large numbers this becomes a very difficult problem, Smid said.

Trap Doors

RSA's president, D. James Bidzos, has attacked the NIST proposal as one that is not secure and that encourages trap doors. Smid said many cryptographers rate the discrete logarithm problem as more difficult or at least as difficult as the factoring method RSA uses.

Ironically, Tahar ElGamal, whose work is recognized in the NIST encryption scheme, is RSA's director of engineering.

"What NIST has proposed is a modification of the idea. Their algorithm is about half from my work and half from theirs. The key size is limited to 512 bits, which is questionable," ElGamal said.

ElGamal added that while he believes the NIST proposal will work, he questions its security.

To use the DSS, a user need only use the system with his everyday mail software.

"What you'd see is the regular message under whatever mail system you have, but somewhere there would be a place for a digital value, from three to 500 bits of data. This would be the sender's signature. You'd have to have some software that would be able to pull off the signature and verify it," Smid said.

Using the DSS, messages appear "in the clear," Smid said because the DSS does not account for privacy. The DSS does not encrypt the entire message, it adds an encrypted "signature" onto the message.

The RSA system does allow for privacy -- with or without another encryption scheme. The RSA system lets the user "sign" a message with his private key and then add privacy by encrypting the message with the recipient's public key. In trying RSA Data Security's Mailsafe software for MS-DOS on the GCN local area network, we found it to work quickly and easily, whether a message was just "signed" or signed and "sealed."

Signed and Sealed

Signing the message with the sender's private key put an encrypted digital signature at the end of an openly readable message. Any person receiving the message with RSA software could verify that it had not been changed and that it came from the sender who scrambled the signature.

Sealing it with the recipient's public key then scrambled the entire message so only the recipient could read it with his private key.

At the receiving end, we decrypted the message first with the recipient's private key, then verified the signature with the sender's public key.

Full encryption and decryption took less than five seconds each for a 10K file on AST Research Inc. Premium 386/25 computers. Varying hard-drive speeds had no measurable effect at this file size.

Though all this sounds very good, it appears to be practical only in close-knit computing communities. As yet, no third-party certification authorities have been established. To use these schemes, users must be able to verify that a public-key/private-key combination fits the right person. Without a certification authority this is difficult in a large network.

The U.S. Postal Service is vying to provide that service. Without certification of keys, someone could establish a key in someone else's name.

The 90-day comment period for the NIST proposal ends at the end of November, but NIST probably will not formally adopt the standard until February, Smid said. The DSS would be mandatory for federal users and for private companies protecting government data, he said.

Though questioning claims that the DSS is less secure than RSA's method, Smid acknowledged that the DSS lacks a necessary hashing function. A hashing function is a cryptographic algorithm used to create a message digest that is unique to each document, much like a fingerprint, said Bidzos. This function ensures the message has not changed since the sender "signed" it. However, Smid said NIST will deliver a hashing function soon.

Public-key encryption is not simply a black art that just happens. "To use public-key encryption, you need a system that knows how to use it," said Robert E. Frank, project leader for electronic commerce at the Lawrence Livermore National Laboratory in Livermore, Calif.

Frank heads a Defense Department funded project to move DOD

to electronic commerce. One area his group has focused on is public-key encryption. The pilot system that Lawrence Livermore has developed gives users an option to use either the NIST proposal or the RSA method.

"Our main objective is to provide a trusted mail capability that makes it possible for vendors and government buyers to use the security features if they want to, and to use what they're most comfortable with," Frank said.

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

A journey behind (way behind) CYBERSPACE hackers in their illusive world

by Kim Clancy

In the last issue of the ISSM, I explained that I would be documenting my journey behind hackers in cyberspace. Let me start by saying that cyberspace is fascinating; it is another world that quietly but actively exists. I mean ACTIVELY. I have no idea what the traffic is of electronic interactions but I can tell you that within minutes I can send a message to Japan and get a response. I can write this article in West Virginia and send it in electronic format to San Francisco. As a matter of fact, almost every guest article we have received has been sent to us through cyberspace. Within minutes of receiving the article, it is imported into the

newsletter and finalized. This is a fascinating technology.

The dark side of cyberspace

Alas, while the technology offers major advantages, it also offers some very frightening avenues as well. What is scary to me in regard to some of the avenues is the ability for individuals to get to so many different types of information, individuals that may initially be too naive to know what they are stumbling into. I am not stating that I think information should be shielded from individuals. I am saying that turning people, children for example, loose in cyberspace may have some unpleasant results. I once went to a presentation about hackers. The presenter told a story about a mother who took her child's computer modem out into the driveway and ran over it after her son had been arrested for hacking. The presenter said that you should never let your child use a modem unattended. While hackers spend time developing their skills and learning how to master cyberspace they also use cyberspace to share information about what they have learned. Information has been found on how to steal long distance phone calls from the phone company, how to make a pipe bomb and how to perform satanic rituals before sitting down to hack. I hesitate to write the above because I don't want people to avoid the technology. Everything I have found is in most libraries, but the accessibility of it through computers makes it much easier to obtain. In an earlier issue of the ISSM, we published a code of computer ethics being used by schools throughout the nation. If you have purchased a modem for your child for Christmas, you may wish to dig that issue out and go over that with him or her.

On a brighter note

I thoroughly enjoy cyberspace. Cyberspace has fantastic legitimate resources and places to visit that are good for the entire family. For example, you can dial up CompuServe and get access to encyclopedias. This is a great way for a child to research a school project. The AIS Security Branch accesses numerous electronic bulletin boards(bbs) that keep us up to date

on security issues and provides us with a network of security professionals. As a matter of fact, we actively participate in cyberspace by running our own bbs.

There is really no way of knowing where a person will end up once

he/she starts exploring cyberspace. The technology is addictive and

before you know it you are constantly searching for more computers

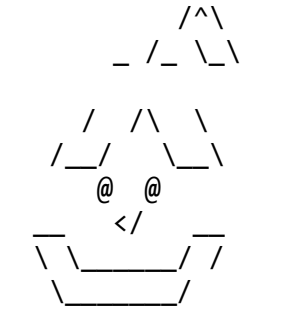
to call and more people to learn from. Cyberspace is a great world,

but if you are not careful, it can carry you away. Don't ignore the

technology, if you don't know about it, you are already behind. Dive in, experience it, have a great time. You will be fascinated

by what you discover.

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



Clyde....dedicated to the pursuit of security ...

DEAR CLYDE...responses to questions for those who are searching for the truth.....

Dear Clyde,
How do I select a good password?
Signed, ABCDE

Dear ABCDE,
One method is to choose a 5 or 6 character word at random and then

add 2 or more random characters to it. This should give you something relatively easy to remember with the additional characters making it more difficult to compromise. It is not a good practice to choose a word that can be associated with you.

Send your comments or questions to Clyde c/o the AIS Security Branch in Parkersburg, WV, Room 1011, or leave them in Clyde's mailbox located on the Security bulletin boards located throughout

the Parkersburg office. You may also leave Clyde an email message

on the AIS Security Branches bbs (304-420-6083)

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

//Computer Speak: Computer terms and their meanings\\

SYSOP n. The operator (and usually the owner) of a bulletin-board system.

MODEM n. A device that connects a computer and a terminal via a telephone line. Short for modulator/demodulator.

NETWORK n. A data communications system that allows a number of systems that allows a number of systems and devices to communicate

with each other.

TRAP DOOR alt. trapdoor n. A breach created intentionally in an EDP

systems for the purpose of collecting, altering, or destroying data.

HARDWARE n. Physical equipment used in data processing. Such as

PC, disk drives, mainframe, keyboard, etc.

SOFTWARE n. Computer programs, procedures, rules, and possibly associated documentation.

----------End of Article----------
^^^^^VIRUS FIGHTERS

What is a computer virus?

The term "computer virus" is derived from and analogous to a biological virus. The word virus itself is Latin for poison. A computer virus is a computer program that will copy (infect) its code into the machine codes of other programs, and when those infected programs are run performing some apparently useful function, such as a login, it executes its hidden code performing an unwanted, usually malicious function.

How does a computer virus work?

A program infected with a virus and loaded and executing in the main memory of a computer can infect another executable (object) program in the computer's disk storage system by secretly requesting the computer's operating system to append a copy of the virus code to the object program, usually at the start. The infection makes the object program slightly longer.
When the newly infected program is itself loaded into memory and invoked, the virus in it takes control and performs hidden functions, such as infecting yet other object programs. The virus may also perform destructive functions before transferring control to the original entry point. The virus code contains a marker so that the virus won't attempt to infect a program already infected by its own kind: multiple infections would cause an object file to grow ever larger, leading to easy detection.
The same principle works in personal computers, where floppy disks play the role of object programs in the description above. In this case, the virus usually attacks the copy of the operating system contained on the floppy disk so that the virus is automatically invoked whenever the disk's operating system is started. Since the operating system then resides in the PC's main memory, it can infect any diskettes inserted into the PC.

What can be done to protect against viruses in a computer or workstation?

An additional measure of protection can be obtained by care in the way one uses a computer. Analogies with food and drug safety are helpful. Just as one would not consider purchasing food or capsules in unsealed containers or from untrusted sources, one can refuse to use any unsealed software or software from untrusted sources.

Can the operating procedures followed by those who use a computer system lower the risk?

Yes! The following are some procedures that would help lower the risk:

. Never insert a diskette that has no manufacturer's seal into your PC.
. Never use a program borrowed from someone who does not practice digital hygiene to your own standards.
. Beware of software obtained from public bulletin boards.
. Purchase programs that check other programs for known viruses.
. Be wary of public domain software (including virus eradicators!).
. Monitor the last-modified dates of programs and files.
. Don't execute programs sent in electronic mail--even your friends may have inadvertently forwarded a virus.
. Don't let employees bring software from home, unless it is approved and checked to be virus free by user management.

What are some of the computer virus symptoms?

When a strange behavior occurs, do not dismiss it as simply a bug. Instead, suspect a virus and respond accordingly - acting quickly may save your data. The following are possible symptoms of a viral

infection:

. Strange screen graphics or displays.
. Unexpected musical tones or sound effects.
. Alteration of text or commands.
. Unusual behavior on reboot.
. Reduction in system performance.
. Unexpected disk access patterns.
. Changes in file length or alteration times.
. Bugs in previously reliable software.
. Bad sectors on floppy disks, or unusually large numbers of bad

  sectors on hard disks.
. Reduction in available memory.
. Unexplained changes in the system clock.
. Unknown, new files or directories/folders appearing on disk.

. Problems in time-dependent tasks such as communications or

  printing.
. The system will not reset or reboot.

What to do if you expect a virus.

. Leave the machine on! Any evidence of intrusion or
  infection may be lost if the machine is powered down. Turn off

  the machine only at the instruction of your management, your

  security group, or your technical support group.
. If your desk-top computer is connected to any kind of network,

  break the network connection logically.

NOTE: BPD EMPLOYEES MUST CONTACT THE COMMUNICATIONS BRANCH IN THE

      DIVISION OF PROGRAMS AND COMMUNICATIONS (OAIS) SO THAT THEY

      MAY BREAK THE PHYSICAL CONNECTION.

. Let people know about your suspicions. Alert your own
  management.
. Use your regular trouble reporting procedure to notify technical

  support of your problem.

Additional information on viruses can be obtained from publications

available in the AIS Security Branch. The information above was

obtained from the publication "Computers Under Attack - Intruders,

worms, and Viruses" by Peter J. Denning.

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

DON'T FORGET, THE AIS SECURITY BRANCH RUNS ITS OWN ELECTRONIC BULLETIN BOARD SYSTEM(BBS). GIVE US A CALL AND LET US KNOW WHAT YOU THINK. THE NUMBER IS 304-420-6083.

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) 420-6363. The ISSM is also available in paper format. Let us know if you would like a copy or if you would like to download a copy of the print file. The print file can be copied to a HP II or III laser printer and you will receive a copy with all graphics and formatting.
Editors: Bob Settles, Ed Alesius, Kim Clancy, Joe Kordella