Story #1

Volume 3 Number 2
April 1993

Story #2
In This Issue

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

Story #3

NLM Anti-virus review team

Story #4 -- "VIRTEAM"

In 1992, Public Debt was hit with its first virus. As a result it was decided that an anti-virus plan was needed. The plan would consist of assigning responsibilities in the area of preventing viruses from being introduced, recovering once they had been discovered, purchasing software to accomplish this task, and installing it on Public Debt's local area network (LAN) servers to aid in the detection of viruses once they were introduced.

Currently, the AIS Security Branch has installed scan and detect programs to run consistently on every server connected to Public Debt's LAN. This requires a dedicated PC running scan software and another to run detection software at each Public Debt location, those locations being: E Street, C Street, Parkersburg Main Building and Town Square.

A new technology was developed that would significantly enhance the integrity of Public Debt's LAN anti-virus program. This technology enabled an anti-virus tool to reside and operate on a Novell server instead of operating off of DOS. This provided additional functionality not possible with a DOS-based protection scheme. For example, a Netware Loadable Module (NLM) could sit on a server and scan a file everytime it was uploaded or downloaded to the server. A DOS-based product would not be able to di

stinguish this activity, therefore, it would be unable to perform the scan at that time.

The AIS Security Branch was assigned the responsibility of reviewing NLM anti-virus products and reporting on their feasibility for Public Debt. As a result, a team was developed, a testing plan was agreed upon,NLM anti-virus products were procured, tested, and a recommendation was made. The following will outline the details of the team and the testing.

The Public Debt LAN is made up of a myriad of platform configurations. Most of our servers run Novell software, but the versions of the software vary. A portion of the LAN is run on an OS/2 platform and currently is running an OS/2 based virus protection package. The OS/2 LAN was not included in the scope of the review in that it will be replaced in the near future and current protection techniques that are being performed at a server level are adequate.

The NLM review team was comprised of individuals that could represent the

different environments throughout Public Debt. The team members are as follows:

OAIS/AIS Security Branch: Kim Clancy (team leader), Jim Heikkinen, Mary Clark, Joe Kordella

OA/TSS: Dee Atwell, Bill Scroggs

OAIS/Communications Branch: Rick Montalbano

OA/OAB: Jeff Schaff, Chris Murnahan

SBOO/OAB: David Earley

OAIS/SEAS: Conrad Sterling

The test plan was the process that was developed and followed by the team to ensure that consistent testing was accomplished. The steps that were agreed upon are as follows:

1. Requirements for the software were agreed upon. A rating sheet was developed and utilized in the evaluation of the anti-virus software.

2. A market survey was conducted and a list of products was presented to the team.

The team selected several software packages for evaluation that appeared to best fit the needs of the Bureau.

3. A procurement for the software was initiated and assignments were made to team members defining the product they would be responsible for demonstrating.

4. Software was received and distributed to team members who were given time to utilize the products, become familiar with them and able to demonstrate them against the testing criteria developed.

5. The team met, reviewed and rated the software and agreed upon recommendations.

All software packages that meet the Bureau's requirements will be submitted as acceptable for purchase. After a tool has been procured, the NLM review team will develop configuration standards and implement the product Bureau wide.

Story #5

Dear Clyde

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

Story #6

Page 4

Story #7

Page 3

Story #8

ISSM

Story #9
Information

Story #10
Systems

Story #11
Security

Story #12
Monitor

Story #13
Dedicated to

Story #14
the pursuit

Story #15
of security

Story #16
awareness

Story #17
April 1993 ISSM

Story #18
Send your comments or questions to Clyde c/o the AIS Security Branch in Parkersburg, Room 1011, or leave them in Clyde's mailbox located on the Security bulletin boards throughout the Parkersburg office.

Story #19 -- "NWSLTR04.03"
In the not too distant future, Public Debt will be providing Password Generating Tokens to its mainframe computer users. These tokens will provide an additional level of computer security access control to help insure that the Bureau's computer systems are kept secure. We will be publishing various articles regarding tokens so that you can become aware of what these tokens are, how you use them, etc. The first of these articles "A decade of experience with password tokens" follows. It is an excellent ar

ticle that appeared in the January/February 1993 issue of the Infosecurity News. This article by Ben Miller, who is editor/publisher of Personal Identification Newsletter in Rockville, Md. He chairs the annual CardTech / SecurTech Conference. This article is reprinted by permission of Infosecurity News.

It is hard to believe that 10 years have passed since password tokens were first introduced to the information security world. At the start, the technology was too complicated for most users to understand, the tokens were notoriously unreliable and only a few operating environments supported the technology.

Somewhere along the line, however, tokens took off. Now, more than 2,000 organizations use these personal authentication devices and some have more than 10,000 units in circulation.

In the U.S. alone, more than half a million people use tokens to access computers. This adds up to a lot of experience, which is increasingly reflected in the sophistication of the newest hardware and software offered by suppliers.

At first glance, a typical password token looks like a pocket calculator (although it may have only a few keys) and has about the same dimensions as a stack of three or four credit cards. The device generates and displays a different password each time its owner logs on.

Industry structure

There are two major components to what is called the enhanced user authentication market--the tokens themselves and the host interfaces that support them. Unfortunately, vendors do not neatly fall into these two categories. While firms that produce tokens offer host support for their own devices, not all support competitors' tokens. Other companies, including some suppliers of host access control packages, offer hostsoftware or hardware front-ends only. In most cases, these companies can also sell tok

ens.

In the view of many, it is the hardware and/or software program that resides on the hosts that is the most important element of enhanced authentication technology. Tokens are viewed simply as an enabling hardware component of the system. The host interface is in fact very important because it does much more than execute cryptographic authentication schemes. An important point to remember is that a special version of the host interface is required for each operating system environment. Today, almost e

very computing platform is supported, from PCs to supercomputers, but not by every vendor. The major token suppliers are Security Dynamics Inc. (SecurID), Enigma Logic Inc. (DES Silver/Gold and MultiSync), Racal-Guardata (Watch-Word), Digital Pathways Inc. (SecurNet Key), ThumbScan Inc. (Access Key), Datamedia Corp. and CryptoCard Corp. (CryptoCard).

There are also a number of "quasi-tokens" on the market. For instance, several companies offer a software version of a token on a floppy disk and MicroFrame Inc. offers a feature for sending one-time passwords to beepers.

In addition to the host interfaces from token vendors, a growing number of third-party software packages support tokens. Among the most established are MicroFrame, Inc.'s hardware front-end. CKS NA's NC-Pass and the Blockade network access control package from Uti-Maco Safeguard Systems, USA.

Authentication schemes

In the beginning, two types of authentication schemes were offered: time-synchronized and challenge- response. Because of the success of the easy-to-use, time-based SecurID, a third scheme, called transaction-synchronized authentication was introduced.

Time-synchronized authentication was pioneered by Security Dynamics, which holds patents on the technique. The token calculates a dynamic password every 60 seconds based on the unique key in the device and the current time. The dynamic password, displayed on a liquid crystal display, is entered into the computer during the log-on routine. The basic SecurID token has no pushbuttons and is the easiest of all devices to use. In recent years, new versions with one or more keys have been introduced for en

tering personal identification numbers (PIN) and that can support up to three hosts.

Challenge-response tokens are a little more sophisticated. The host transmits a pseudo-random number, or challenge. The user enters the number into a keypad on the token and a response is calculated based on the token's key and the challenge. This number is entered into the terminal by the user and the host compares it to the expected value. The challenge- response approach requires more actions on the part of the user and results in a slightly longer sign-on. Watchword, SecurNet Key, Access Key, Mu

ltiSync, and CryptoCard are among the leading brands of challenge-response tokens.

Transaction-synchronized tokens rely on the host and token to keep track of successful sign-ons, using the most recent one-time password in calculating the next. A single button is used to tell the token to make its calculation. This type of token was available as early as 1986, but implementation was crude and tokens and hosts would often get out of synch. The technique has recently been revived, because it is very simple to use. Enigma Logic's DES Silver and Gold products use the transaction-synchr

onized approach, although the Gold version also supports challenge-response and multiple hosts.

As with all tokens, log-on procedures become more complex when multiple hosts or user PINs are used.

PINs and static passwords

Passwords generated by tokens are usually referred to as "dynamic" or "one-time" passwords. While tokens significantly enhance access control security, they do not completely eliminate the need for user ID numbers, static passwords and personal identification numbers.

Security administrators can mix and match memorized identification techniques to gain higher and higher levels of security. A basic token log-on routine asks for a user ID number, followed by the one-time password generated by the token. At the next level of security, a static password is also entered into the terminal keyboard. This is usually in response to a separate prompt by the software, but it can be appended to the dynamic password displayed on the token. Some software packages even support d

uress codes using the password function. Here, a special password is entered that tells the system that the session is compromised.

The highest level of security, short of using biometrics, requires entering a PIN into the token before it will operate. This is called the "user-to-token handshake." Most token supplies offer versions of their devices with keypads for this purpose. While this is the most secure approach, it has not been popular because tokens with keypads cost more and the log-on process becomes more complicated. Most tokens that support PINs allow users to select their own numbers. For security reasons, no one els

e knows this code and there is no superuser back door. Therefore, if the PIN is forgotten the token must be re-initialized.

Algorithms

Many of today's tokens use the Data Encryption Standard (DES) to calculate passwords. In fact, most challenge-response and transaction-synchronized devices use the DES X9.9 Financial Institutions Message Authentication Code standard to generate their one-time passwords. A number of offerings use proprietary algorithms and some devices include both DES and a proprietary formula. It is believed that no one has compromised any of the algorithms used in tokens. However, only DES has withstood over 20 yea

rs of scrutiny at the hands of the world's best cryptographers.

Multiple hosts

A decade ago, computer systems were much simpler and tokens were generally used to protect a single, sensitive activity. By 1990, the token industry heard clearly that the growth of PCs, LANs, and interconnected networks demanded support of multiple hosts. This posed a number of problems for tokens with a single key and especially severe problems for time- or transaction-synchronized devices. For instance, transaction-based tokens could easily get out of sync if a user moved from host to host. A time

-synchronized password could be compromised if it was valid for more than one host at a time.

Fortunately, there are many solutions to the multihost challenge. If just two hosts are involved, the first few digits of the one-time password can be used for one host and the last few digits for the second. Or, different static passwords can

also be used to differentiate hosts. Hardware or software front-ends can also be established to act as gateways passing authentications off to other systems. The least attractive option is to require users to carry more than one token.

Most vendors have introduced tokens with multiple keys to support up to nine different hosts. Some products can even apply different algorithms for each host. Token suppliers especially like multihost applications because they derive significant revenue from license fees on the host interface, which can cost up to $10,000 a copy. Generally, multiple host tokens are more complicated: log-on procedures require selecting the proper host via keys on the token. It is also important to plan for the future

because tokens may have to be reinitialized and reregistered if a new host is added.
Administrative add-ons

Adopting tokens adds to the organization's administrative chores -- tokens must be issued and kept track of and employees need to be trained to use them.

When tokens are first issued they need to be registered in a database: some have to be initialized. These steps are unavoidable and procedures must be established for distributing tokens to users. Security administrators will see the tokens again when their batteries expire.

Inevitably, users lose or break the devices. This calls for procedures to allow users, whose tokens are lost or out of commission to get onto the system. Fortunately, most host interfaces now have built-in procedures for granting temporary access.

The most secure approach is to issue a new token. This is only practical where there are decentralized token inventories and no remote computing. However, most organizations maintain central token stocks and have many remote users, often including customers. Re-issuing tokens may take at least a day and procedures must be designed to ensure that the correct person receives the token.

For the immediate problem of letting the user work for the day, a help desk that can issue a temporary password is a must. Some organizations keep a special token at the help desk that the security administrator uses to generate a password. Others generate a 10-character password on host software that is only valid for 24 hours. Still another has the user call the system administrator and simply read a challenge number from the terminal display.

Whatever method is used for temporary access and reissue, there must be procedures to deactivate a lost, stolen or damaged token. An adequate supply of replacement tokens will prevent having to rely on less-secure methods for too long. Many organizations hold users financially liable for lost or abused tokens.

Even the most sophisticated tokens can seem easy to use if you have just spent a few months selecting and installing your system. However, from the user's perspective, tokens are often just another inconvenience. Training may make the difference between a smooth implementation and an administrative disaster. How training is structured depends on several factors. Will users come to the security department to get their tokens or will the devices be distributed by local administrators, or even via couri

er? What types of people will be using the devices--programmers, sales people, customers, etc.? How many people will be using them, a few dozen or a few thousand?

Written materials, seminars, posters and videos can help. All have been used by other organizations, and vendors should be willing to identify customers whose programs have been effective.

Story #20
CLYDE'S
Computer Security
Hall of Fame

Story #21
Tokens from Page 2

Story #22 -- "ISSMHOF"

The Office of Securities and Accounting Services (OSAS), Division of Securities and Accounts (DSA) has been inducted to the Computer Security Hall of Fame.

The OSAS/DSA's dedication to Public Debt's computer sercurity program has earned it recognition for its efforts with an induction to the Computer Security Hall of Fame.

OSAS/DSA ISSM's Deloris Vance and Delores Craddolph have promoted computer security awarness issues beyond the normal distribution and reader tracking of the ISSM newsletter. They have provided in-house training to their Division, also they have published their own computer security awareness newsletter (See this issues insert for a copy of their publication). They also arrange for meeting space for Washington based ISSMs whenever ISSM meetings are scheduled. These "extra" efforts have been evident in

all aspects of their computer security administration.

OSAS/DSA's dedication, interest and "going the extra mile" attitude to all aspects of the Bureau's computer security program is of the type that will make Public Debt's computer security program exceptional.
Submitted by Kim Clancy, Manager of the AIS Security Branch.

Story #23
In the January issue of the ISSM we reported that free diskettes distributed by the Cobb Group at the Federal Computer Conference December 8, 9, or 10, may have contained a virus which is very difficult to detect. We later received information, after we had gone to print, that the advisory we received was a false alarm. (Lesson learned from group releasing notice - verify positive reports with multiple

scanning software.)

Story #24 -- "CLYDE"
Dear Clyde,
I really enjoy playing games on my PC at home. Can I bring any of these games to work and use them on my PC here at Public Debt?
Ima Funlover
Dear Ima,
PC games should not be brought in and used on any Public Debt PC. There are a number of reasons why, such as:
PDI 85-02 Microcomputer Security, on Page 6, Section II, Information Security, Software Security states that:
1. "In order to guard against invasive or destructive programming, unsolicited software or software borrowed from outside of Public Debt will not be used prior to the testing of the software on a microcomputer isolated by user management for this purpose".
2. "Public Debt managers must ensure that copyright laws governing the misuse of vendor software, as well as the unauthorized duplication or use of software for other than stipulated back-up purposes, is not condoned either actively or passively" Software that is brought in to the workplace from home or school has been considered one of the leading type of carriers of computer virus infections.
I like to play games on my PC that I have at home too. Let's both leave that type of fun for home.

Story #25
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.

Story #26
Continued on Page 4

Story #27
from Page 3

Story #28
Password tokens

Story #29
Continued on Page 3

Story #30

Virus Alert Retraction

Story #31
Tokens

Story #32
NLM Anti-virus From Page 1

Story #33
Continued on Page 4

Story #34
by Mary Clark

Story #35
Testing Product Reactions to Viruses

Story #36

How does a reseach team test a product's reaction to live viruses? A product claims it reacts a certain way, but until it actually detects something and performs the test, you really don't know how it will react in your environment. Public Debt's NLM test team wanted to test products in their real world environment but was not comfortable with letting live viruses loose on the production servers. After a bit of research with an expert in virus writing and detection - a virus writer and editor of CRYPT

newsletter virus magazine - Urnst Kouch, we discovered at his recommendation a tool called Rosental. Rosental is a program that generates virus signatures, but not live viruses. It provides a method for checking scanners and ensuring they operate as suggested. Rosental program is a shareware program and can be found on the AIS BBS. It should be noted that Urnst warned against using the Rosental generated signatures as a test to determine the accuracy of a product. He did state it would provide a metho

d of testing product behavior.

Story #37
by Kim Clancy