CERT Advisory CA-1994-01 Ongoing Network Monitoring Attacks

Original issue date: February 3, 1994
Last revised: September 19, 1997
Updated copyright statement

A complete revision history is at the end of this file.

In the week before we originally issued this advisory, the CERT/CC staff observed a dramatic increase in reports of intruders monitoring network traffic. Systems of some service providers have been compromised, and all systems that offer remote access through rlogin, telnet, and FTP are at risk. Intruders have already captured access information for tens of thousands of systems across the Internet.

The current attacks involve a network monitoring tool that uses the promiscuous mode of a specific network interface, /dev/nit, to capture host and user authentication information on all newly opened FTP, telnet, and rlogin sessions.

In the short-term, we recommend that all users on sites that offer remote access change passwords on any network-accessed account. In addition, all sites having systems that support the /dev/nit interface should disable this feature if it is not used and attempt to prevent unauthorized access if the feature is necessary. A procedure for accomplishing this is described in Section III.B.2 below. Systems known to support the interface are SunOS 4.x (Sun3 and Sun4 architectures) and Solbourne systems; there may be others. Sun Solaris systems do not support the /dev/nit interface. If you have a system other than Sun or Solbourne, contact your vendor to find if this interface is supported.

While the attack is specific to /dev/nit, the short-term workaround does not constitute a solution. The best long-term solution currently available for this attack is to reduce or eliminate the transmission of reusable passwords in clear-text over the network.

I. Description

Root-compromised systems that support a promiscuous network interface are being used by intruders to collect host and user authentication information visible on the network.

The intruders first penetrate a system and gain root access through an unpatched vulnerability. Solutions and workarounds for these vulnerabilities have been described in previous CERT advisories, which are available from
ftp://ftp.cert.org/pub/cert_advisories

The intruders then run a network monitoring tool that captures up to the first 128 keystrokes of all newly opened FTP, telnet, and rlogin sessions visible within the compromised system's domain. These keystrokes usually contain host, account, and password information for user accounts on other systems; the intruders log these for later retrieval. The intruders typically install Trojan horse programs to support subsequent access to the compromised system and to hide their network monitoring process.

II. Impact

All connected network sites that use the network to access remote systems are at risk from this attack.

All user account and password information derived from FTP, telnet, and rlogin sessions and passing through the same network as the compromised host could be disclosed.

III. Approach

There are three steps in our recommended approach to the problem:

- Detect if the network monitoring tool is running on any of your hosts that support a promiscuous network interface.
- Protect against this attack either by disabling the network interface for those systems that do not use this feature or by attempting to prevent unauthorized use of the feature on systems where this interface is necessary.
- Scope the extent of the attack and recover in the event that the network monitoring tool is discovered.

A. Detection

The network monitoring tool can be run under a variety of process names and log to a variety of filenames. Thus, the best method for detecting the tool is to look for

1. Trojan horse programs commonly used in conjunction with this attack,
2. any suspect processes running on the system,
3. the unauthorized use of /dev/nit,
4. unexpected ASCII files in the /dev directory, and
5. modifications to /etc/rc* files and /etc/shutdown

1) Trojan horse programs:

The intruders have been found to replace one or more of the following programs with a Trojan horse version in conjunction with this attack:

/usr/etc/in.telnetd
and /bin/login (Used to provide back-door access for the intruders to retrieve information)
/bin/ps (Used to disguise the network monitoring process)
netstat
ifconfig

su
ls
find
du
df
libc
sync
binaries referred in /etc/inetd.conf

Because the intruders install Trojan horse variations of standard UNIX commands, we recommend not using other commands such as the standard UNIX *sum(1)* or *cmp(1)* commands to locate the Trojan horse programs on the system until these programs can be restored from distribution media, run from read-only media (such as a mounted CD-ROM), or verified using cryptographic checksum information.

In addition to the possibility of having the checksum programs replaced by the intruders, the Trojan horse programs mentioned above may have been engineered to produce the same standard checksum and timestamp as the legitimate version. Because of this, the standard UNIX *sum(1)* command and the timestamps associated with the programs are not sufficient to determine whether the programs have been replaced.

We recommend that you use both the /usr/5bin/sum and /bin/sum commands to compare against the distribution media and assure that the programs have not been replaced. The use of *cmp(1)*, MD5, Tripwire (only if the baseline checksums were created on a distribution system), and other cryptographic checksum tools are also sufficient to detect these Trojan horse programs, provided these programs were not available for modification by the intruder. If the distribution is available on CD-ROM or other read-only device, it may be possible to compare against these volumes or run programs off these media.

2) Suspect processes:

Although the name of the network monitoring tool can vary from attack to attack, it is possible to detect a suspect process running as root using *ps(1)* or other process-listing commands. Until the *ps(1)* command has been verified against distribution media, it should not be relied upon--a Trojan horse version is being used by the intruders to hide the monitoring process. Some process names that have been observed are sendmail, es, and in.netd. The arguments to the process also provide an indication of where the log file is located. If the "-F" flag is set on the process, the filename following indicates the location of the log file used for the collection of authentication information for later retrieval by the intruders.

3) Unauthorized use of /dev/nit:

If the network monitoring tool is currently running on your system, it is possible to detect this by checking for unauthorized use of the /dev/nit interface. We have created a minimal tool, cpm, for this purpose.

We urge you to use the cpm tool on every machine at your site (where applicable). Some sites run this as a cron job at regular intervals, such as every 15 minutes, to report any result that indicates a possible compromise.

cpm (version 1.2) can be obtained from

ftp://ftp.cert.org/pub/tools/cpm/ ftp://ftp.uu.net/pub/security/cpm/

Below are the MD5 checksums for the tarfiles and the contents of the cpm.1.2 directory, when created.

MD5 (cpm.1.2.tar) = 5f0489e868fbf213c026343cca7ec6ff
MD5 (cpm.1.2.tar.Z) = b76285923ad17d8dbfffd9dd0082ce5b
MD5 (cpm.1.2.tar.gz) = e689ca1c663e4c643887245f41f13a84
MD5 (cpm.1.2/MANIFEST) = ed6ec1ca374113c074547eb0580d9240
MD5 (cpm.1.2/README) = 34713d2be42b434a117165a5002f0a27
MD5 (cpm.1.2/cpm.1) = 84df06d9c6687314599754f3515c461b
MD5 (cpm.1.2/cpm.c) = 3da08fe657b96a75697a41e2700d456e
MD5 (cpm.1.2/cpm.txt) = 5860bfb9c383f519e494a38c682c22fb

This archive contains a readme file, also included as Appendix C of this advisory, containing instructions on installing and using this detection tool.

Note that some sites have reported intruders gaining root access then reinstalling a kernel with /dev/nit functionality.

4) Unexpected ASCII files in /dev

Look for unexpected ASCII files in the /dev directory. Some of the Trojan binaries listed above rely on configuration files, which are often found in /dev.

5) Modifications to /etc/rc* files and /etc/shutdown

Check for modifications to /etc/rc* files and /etc/shutdown. Some intruders have modified /etc/rc files to ensure that the sniffer restarts after a shutdown or reboot. Others have modified the shutdown sequence to remove all traces of compromise.

B. Prevention

There are two actions that are effective in preventing this attack. A long-term solution requires eliminating transmission of clear-text passwords on the network. For this specific attack, however, a short-term workaround exists. Both of these are described below.

1) Long-term prevention:

We recognize that the only effective long-term solution to prevent these attacks is by not transmitting reusable clear-text passwords on the network. We have collected some information on relevant technologies. This information is included as Appendix B in this advisory. Note: These solutions will not protect against transient or remote access transmission of clear-text passwords through the network.

Until everyone connected to your network is using the above technologies, your policy should allow only authorized users and programs access to promiscuous network interfaces. The tool described in Section III.A.3 above may be helpful in verifying this restricted access.

2) Short-term workaround:

Regardless of whether the network monitoring software is detected on your system, we recommend that ALL SITES take action to prevent unauthorized network monitoring on their systems. You can do this either by removing the interface, if it is not used on the system or by attempting to prevent the misuse of this interface.

For systems other than Sun and Solbourne, contact your vendor to find out if promiscuous mode network access is supported and, if so, what is the recommended method to disable or monitor this feature.

For SunOS 4.x and Solbourne systems, the promiscuous interface to the network can be eliminated by removing the /dev/nit capability from the kernel. The procedure for doing so is outlined below (see your system manuals for more details). Once the procedure is complete, you may remove the device file /dev/nit since it is no longer functional.

Procedure for removing /dev/nit from the kernel:

1. Become root on the system.
2. Apply "method 1" as outlined in the System and Network Administration manual, in the section, "Sun System Administration Procedures," Chapter 9, "Reconfiguring the System Kernel." Excerpts from the method are reproduced below:

```
# cd /usr/kvm/sys/sun[3,3x,4,4c]/conf
# cp CONFIG_FILE SYS_NAME

[Note that at this step, you should replace the CONFIG_FILE
with your system specific configuration file if one exists.]

# chmod +w SYS_NAME
# vi SYS_NAME

   #
   # The following are for streams NIT support.  NIT is used by
   # etherfind, traffic, rarpd, and ndbootd.  As a rule of thumb,
   # NIT is almost always needed on a server and almost never
   # needed on a diskless client.
   #
   pseudo-device   snit            # streams NIT
   pseudo-device   pf              # packet filter
   pseudo-device   nbuf            # NIT buffering module

[Comment out the preceding three lines; save and exit the
editor before proceeding.]

# config SYS_NAME
# cd ../SYS_NAME
# make

# mv /vmunix /vmunix.old
# cp vmunix /vmunix

# /etc/halt
< b
```

[This step will reboot the system with the new kernel.]

[NOTE that even after the new kernel is installed, you need to take care to ensure that the previous vmunix.old , or other kernel, is not used to reboot the system.]

C. Scope and recovery

If you detect the network monitoring software at your site, we recommend following three steps to successfully determine the scope of the problem and to recover from this attack.

1. Restore the system that was subjected to the networkmonitoring software.

The systems on which the network monitoring and/or Trojan horse programs are found have been compromised at the root level; your system configuration may have been altered. See Appendix A of this advisory for help with recovery.

2. Consider changing router, server, and privileged account passwords due to the wide-spread nature of these attacks.

Since this threat involves monitoring remote connections, take care to change these passwords using some mechanism other than remote telnet, rlogin, or FTP access.

3. Urge users to change passwords on local and remote accounts.

Users who access accounts using telnet, rlogin, or FTP either to or from systems within the compromised domain should change their passwords after the intruder's network monitor has been disabled.

4. Notify remote sites connected from or through the local domain of the network compromise.

Encourage the remote sites to check their systems for unauthorized activity. Be aware that if your site routes network traffic between external domains, both of these domains may have been compromised by the network monitoring software.

Appendix A: RECOVERING FROM A UNIX ROOT COMPROMISE

A. Immediate recovery technique

a. Disconnect from the network or operate the system in single- user mode during the recovery. This will keep users and intruders from accessing the system.
b. Verify system binaries and configuration files against the vendor's media (do not rely on timestamp information to provide an indication of modification). Do not trust any verification tool such as *cmp(1)* located on the compromised system as it, too, may have been modified by the intruder. In addition, do not trust the results of the standard UNIX *sum(1)* program as we have seen intruders modify system files in such a way that the checksums remain the same. Replace any modified files from the vendor's media, not from backups.

   -- or --

   Reload your system from the vendor's media.
c. Search the system for new or modified setuid root files.

```
find / -user root -perm -4000 -print
```

   If you are using NFS or AFS file systems, use ncheck to search the local file systems.

```
ncheck -s /dev/sd0a
```

d. Change the password on all accounts.
e. Don't trust your backups for reloading any file used by root. You do not want to re-introduce files altered by an intruder.

More detailed advice can be found in

ftp://ftp.cert.org/pub/tech_tips/root_compromise

B. Improving the security of your system

a. CERT Security Technical Tips
   The CERT/CC staff has developed technical tips and checklists based on information gained from computer security incidents reported to us. These tips are available from

   ftp://ftp.cert.org/pub/tech_tips

b. Security Tools
   Use security tools such as COPS and Tripwire to check for security configuration weaknesses and for modifications made by intruders. We suggest storing these security tools, their configuration files, and databases offline or encrypted. TCP daemon wrapper programs provide additional logging and access control. These tools are available

   ftp://ftp.cert.org/pub/tools

c. CERT Advisories
   Review past CERT advisories (both vendor-specific and generic) and install all appropriate patches or workarounds as described in the advisories. CERT advisories and other security-related information are available from

   http://www.cert.org/

   ftp://ftp.cert.org/pub/

To join the CERT Advisory mailing list, send a request to:
cert-advisory-request@cert.org

Please include contact information, including a telephone number.

Appendix B: ONE-TIME PASSWORDS

Given today's networked environments, CERT recommends that sites concerned about the security and integrity of their systems and networks consider moving away from standard, reusable passwords. CERT has seen many incidents involving Trojan network programs (e.g., telnet and rlogin) and network packet sniffing programs. These programs capture clear-text hostname, account name, password triplets. Intruders can use the captured information for subsequent access to those hosts and accounts. This is possible because 1) the password is used over and over (hence the term "reusable"), and 2) the password passes across the network in clear text.

Several authentication techniques have been developed that address this problem. Among these techniques are challenge-response technologies that provide passwords that are only used once (commonly called one-time passwords). This document provides a list of sources for products that provide this capability. The decision to use a product is the responsibility of each organization, and each organization should perform its own evaluation and selection.

I. Publicly Available Packages

S/KEY(TM)

The S/KEY package is publicly available (no fee) via anonymous FTP from:

```
thumper.bellcore.com            /pub/nmh directory
```

```
There are three subdirectories:

               skey            UNIX code and documents on S/KEY.
                               Includes the change needed to login,
                               and stand-alone commands (such as "key"),
                               that computes the one-time password for
                               the user, given the secret password and
                               the S/KEY command.

               dos             DOS or DOS/WINDOWS S/KEY programs.  Includes
                               DOS version of "key" and "termkey" which is
                               a TSR program.

               mac             One-time password calculation utility for
                               the Mac.
```

II Commercial Products:

Secure Net Key (SNK) (Do-it-yourself project)
Digital Pathways, Inc.
201 Ravendale Dr.
Mountainview, Ca. 94043-5216
USA
Phone: 415-964-0707
Fax: (415) 961-7487

Products:
handheld authentication calculators (SNK004) serial line auth interruptors (guardian)

Note: Secure Net Key (SNK) is des-based, and therefore restricted from US export.

Secure ID (complete turnkey systems)
Security Dynamics
One Alewife Center
Cambridge, MA 02140-2312
USA
Phone: 617-547-7820
Fax: (617) 354-8836

Products:
SecurID changing number authentication card
ACE server software

SecureID is time-synchronized using a 'proprietary' number generation algorithm

WatchWord and WatchWord II
Racal-Guardata
480 Spring Park Place
Herndon, VA 22070
703-471-0892
1-800-521-6261 ext 217

Products:
Watchword authentication calculator
Encrypting modems

Alpha-numeric keypad, digital signature capability

SafeWord
Enigma Logic, Inc.
2151 Salvio #301
Concord, CA 94520
510-827-5707
Fax: (510)827-2593

Products:
DES Silver card authentication calculator
SafeWord Multisync card authentication calculator

Available for UNIX, VMS, MVS, MS-DOS, Tandum, Stratus, as well as other OS versions. Supports one-time passwords and super smartcards from several vendors.

Appendix C: cpm 1.0 README FILE

cpm - check for network interfaces in promiscuous mode.

Thursday Feb 3 1994
CERT Coordination Center
Software Engineering Institute

Carnegie Mellon University
Pittsburgh, PA 15213-3890

This program is free software; you can distribute it and/or modify it as long as you retain the Carnegie Mellon copyright statement.

It can be obtained via anonymous FTP from ftp.cert.org:pub/tools/cpm.tar.Z.

This program is distributed WITHOUT ANY WARRANTY; without the IMPLIED WARRANTY of merchantability or fitness for a particular purpose.

This package contains:

README
MANIFEST
cpm.1
cpm.c

To create cpm under SunOS, type:

```
% cc -Bstatic -o cpm cpm.c
```

On machines that support dynamic loading, such as Sun's, CERT recommends that programs be statically linked so that this feature is disabled.

CERT recommends that after you install cpm in your favorite directory, you take measures to ensure the integrity of the program by noting the size and checksums of the source code and resulting binary.

The following is an example of the output of cpm and its exit status.

Running cpm on a machine where both the le0 and le2 interfaces are in promiscuous mode, under *csh(1)*:

```
% cpm
le0
le2
% echo $status
2
%
```

Running cpm on a machine where no interfaces are in promiscuous mode, under *csh(1)*:

```
% cpm
% echo $status
0
%
```

The CERT Coordination Center thanks the members of the FIRST community as well as the many technical experts around the Internet who participated in creating this advisory. Special thanks to Eugene Spafford of Purdue University for his contributions.

UPDATES

- We have seen sniffers for other platforms, i.e., Solaris.
- Sites have reported intruders using sniffers to capture authentication to routers. Using that data, they compromise the routers and modify the configuration file.

Revision History

```
Sept. 19, 1997  Updated Copyright statement
Apr. 03, 1997  Appendix B - corrected "Public Domain" to read "Publicly
                Available"
Oct. 09, 1996  Sentence 1 - Clarified the time of the increase in the reports.
               Appendix A - Added the URL for our tech tip on root compromises.
Aug. 30, 1996  Information previously in the README was inserted
               into the advisory. Updated URLs.
July 31, 1996  Appendix B - referred to new tech tips, which replace the single
               security checklist
Mar. 20, 1996  Sec.III.A.3 - additional information concerning cpm (v. 1.2)
Sept. 21, 1995 Sec. III.A.3 - suggestions regarding cpm
Feb. 02, 1995  Sec. III - additional information on Trojan binaries (III.A),
               use of the /dev directory (III.A.3), and two more
               activities (III.A.4 & III.A.5)
Feb. 02, 1995  Updates section - additional information about sniffer activity
```