Operational Security - Occurrences and Defence

Danny Smith
Australian Computer Emergency Response Team
c/- Prentice Centre
The University of Queensland
Qld. 4072.
Australia
auscert@auscert.org.au
AUSCERT Hotline: +61 7 365 4417

Introduction

This paper is a discussion of computer security. Rather than detailing the standard weaknesses in computer security (which have been detailed many times in the past), this paper discusses a few recent vulnerabilities and details of where further information on computer security can be found. This information includes a large number of papers and books where more general discussions on computer security can be found.

UNIX Security - Basics

sendmail

sendmail(8) has recently been found to contain a vulnerability. This vulnerability allows anyone to execute arbitrary programs on your system from a remote location (without requiring an account on the system). This can allow anyone to gain access to the system as any account, except root. A number of approaches to this vulnerability have been advocated. See SERT Advisory SA-93.10 for further details.

accounts

The primary defence against intruders is the account and password mechanism. A poor choice of passwords will allow an intruder to gain access to the system. Once access is gained to the system, it then becomes easier to gain root access. The system security is only as strong as its weakest point. Therefore, password choice (and hence system security) is a community response - if one person fails to provide good security, then the security of the whole system may be compromised. See SERT Advisory SA-93.04 for further details.

File System Configurations

One of the easiest mistakes to make when configuring NFS results in allowing any system on the Internet to mount the file system. This typically applies to older UNIX systems. There are several mistakes that can be made, and they are usually silent in operation, which means that you may not be aware that it has happened. The easiest way to determine if your system is vulnerable to this form of attack, use the `showmount -e` command to verify that the exported file systems are appropriate.

The basic errors concern the content of the /etc/exports file. If the line exceeds 255 characters, it is possible that it will not be processed correctly. If any mistakes are made with the format of the export line (for example, referencing a non-existent group), then the line will not be processed correctly.

When configuring the exported file systems, be careful to only export file systems to known hosts. In addition, if possible export file systems read only, and nosuid.

Network Connections

Most of the attacks against a computer system will occur from a remote site, using various network services. Therefore, control of access to these services is essential. There is an excellent tool to do this called `tcp_wrapper`. When you use this tool, you should also verify the output logs, looking for any anomalous connections. These may indicate an attempt to access the system, which may indicate some antisocial behaviour. These connections should be investigated.

SERT was advised by the office of the Director of Public Prosecutions that the use of a login warning banner can help with any prosecution that may be required as the result of an intrusion. In addition, it also warns your legitimate users of their responsibilities and the penalties for misuse. This can be found in SERT Advisory SA-93.03.

The Berkeley "r" commands (such as rlogin, rsh, and so on) provide a convenient way to use networked systems without exposing the login password to network monitors. Unfortunately, many intrusions occur through "trusted systems" attacks - having one trusted system compromised, thus allowing all other trusted systems to be compromised. In addition, the .rhosts file represents a particular problem as the security of the computer system is out of the control of the system administrator, allowing any user access to their account from any system on the Internet. The only mechanisms to combat these weaknesses is to disable the "r" commands, or ensure good user education and responsibility.

UNIX Security - Tools

Megapatch

The Megapatch is for SunOS 4.1.2 and 4.1.3 systems only. It has been created in response to increasing security problems with these operating systems. Many security patches were required to both systems, and the number and order that they be applied became unmanageable. The Megapatch handles this problem. In addition, it installs a number of useful security tools (and gives them an initial configuration). The Megapatch can be obtained via anonymous ftp from ftp.sert.edu.au:/security/sert/tools.

Crack

Crack is a fast UNIX password cracking program designed to assist the site administrators in ensuring that user's use effective passwords. It is approximately 16 times faster than standard DES routines, enabling one to check more passwords in a given time. The dictionaries that are used can be supplied from a variety of sources, including generating them from information about the user's account.

Crack has the ability to automatically spread the load of password cracking to several machines on a network. The hosts are specified with a "power" rating which aids in determining how much of the password cracking load is passed to each networked machine. Whilst Crack is operating, it periodically saves its state, which helps with recovering from a known point if a host crashes, or Crack aborted.

Crack is available via anonymous ftp from ftp.sert.edu.au:/security/cert/tools.

COPS

COPS is a collection of shell scripts and programs that individually test an aspect of system security. These programs make no attempt to correct problems, but merely report them. Included in the COPS package is the Kuang rule based checker. This checker applies a number of set rules to determine if the system security can be compromised through a series of events, rather than just one. COPS is available via anonymous ftp from ftp.sert.edu.au:/security/cert/tools.

passwd+, npasswd

It has been shown in many studies that the security of the system is severely compromised if the choice of any password on the system is not secure. Increasing the space of possible passwords helps prevent against password guessing attacks. There are two mechanisms to preventing poor password choices: the first is to determine the poor password after it has been set (by using tools such as Crack), and the second is to test new passwords before they are changed against known poor passwords. The npasswd and passwd+ tools are proactive password changing programs that check passwords before they are accepted. These tools are available via anonymous ftp from ftp.sert.edu.au:/security/cert/tools.

TCP Wrapper

`tcp_wrapper` (previously known as LOG TCP) is a package that is used to monitor incoming IP connections, log them, and provide a number of add-on services including a limited form of access control and some sanity checks.

The first function is to log connections. Any connection to an IP service that has `tcp_wrapper` enabled for it will write a connection record to the syslog daemon, containing the time and the source of the connection. If access control has been enabled, the list will be checked to see if the source of this connection has been allowed or denied access to that IP service. If the service is denied, then the connection is aborted. If the service is allowed, then the normal daemon is executed.

If the name checking has been turned on, the wrapper will verify that the name to address mapping is the same as the address to name mapping. If there is any discrepancy, the wrapper concludes that it is dealing with a host that is pretending to have someone else's name (as in an attack on the "r" commands). If this is detected, the connection is logged, and then aborted.

`tcp_wrapper` is an extremely simple, and yet effective tool. It is very useful in preventing connections from outside an organisation from approaching the systems. It is possible to allow certain connections (for example, mail) to the systems, while restricting others. Even if an intruder learns an account and password for the system, they must first penetrate a "trusted" system before they can gain access to the system. It is therefore imperative that users do not use the same password on all systems.

Tripwire

Tripwire is a file integrity checker using a number of cryptographic checksumming algorithms in parallel for added security. Algorithms such as CRC-16 and CRC-32, commonly used to checksum data packets for transmission across a network, do not provide sufficient strength to protect the integrity of files against a determined intruder. There are public domain tools that will help "recreate" a valid checksum on files while still maintaining file size. This is especially true of system binaries.

Tripwire makes use of several message digesting algorithms. These are:

- MD5
- MD4
- MD2
- Snefru
- CRC-32
- CRC-16

The use of more than one of these algorithms in parallel greatly reduces the chances of an intruder being able to modify a monitored file without detection. To run Tripwire, a reference database of results needs to be built, immediately after the installation of the operating system and any products, and prior to reconnecting to the network. In this way, it is possible to be sure that the files have not already been modified. The output from Tripwire (as well as Tripwire itself) should ideally be kept on a hardware write protected disk to prevent modification. Tripwire should then be run at regular intervals to verify the integrity of key system files. Another alternative to using hardware protected media is to print out a copy of Tripwire's results. In this way, an intruder must gain physical access to the premises to adjust the original data from Tripwire. This also helps if there is any suspicion on the integrity of the Tripwire database.

Tripwire is available via anonymous ftp from ftp.sert.edu.au:/security/cert/tools.

Vendor Supplied

Some vendor's provide add-on security packages which should be investigated. The advantage of a vendor supplied package is that it is supported by contract, and there is a mechanism for getting updates to the package if it does not perform correctly. It is also more likely to be compatible with the specified version of the operating system than a generic security tool. One example of a vendor supplied product is Sun Microsystems' SunShield package. Contact the vendors for further information.

Vendor C2

A particular security package worth investigating relates to C2 security. Some vendors supply this by default, other vendors have it available as an add-on package. C2 security provides a number of different features which help to improve the security of the system. This might include shadow passwords, increased logging, and discretionary access control.

socks

The socks package is a firewall enhancer which allows users to pass out through the firewall transparently. Many networks are now moving towards the concept of firewall systems - systems designed to act as an entry portal to the network. Using a firewall system means that no other systems are directly connected to the global network. To access the global network requires accounts on the firewall system, and a two hop process. Granting a large number of users access to the firewall system reduces its effective security, and therefore its performance as a security tool.

Socks automates the process of having a firewall host which is utilised as a transient point for global network access. From the point of view of a user behind the firewall host, there is no apparent difference between running socks and the regular client software on a host. The difference is that all traffic is passing through a daemon on the firewall host.

Socks also maintains a security configuration file, which can filter connections based upon host address and service. This is very similar to what `tcp_wrapper` does, except `tcp_wrapper` operates on a host by host basis, and the socks package is designed to filter all connections to the local network that pass through a firewall system.

Kerberos

Kerberos is a distributed authentication service developed as part of Project Athena at MIT. The greatest advantage of Kerberos is that the password is not transmitted across the network in plain text, therefore helping to defeat network monitoring attacks. In addition, the use of an "authenticator" helps to prevent replay attacks. Since Kerberos is a distributed system, it is now possible to use a single password for accessing the network, and then access is granted to all network services supporting Kerberos.

S/Key

S/Key is a software system designed to implement a secure one-time password scheme. It uses 64 bits of information transformed by the MD4 message digest algorithm. The 64 bits of information are supplied by the user in the form of six short English words that are generated by a secure computer. Ultimately, this computer could be a pocket sized smart card, a standalone PC or Macintosh, or a secured machine at work. A list of passwords is generated, and each time a user authenticates to the system, the next password on the list is prompted for. Once this is successfully used, it is no longer valid. Password lists may be changed in a secure manner across an insecure network.

Interfaces for UNIX and VMS have been developed or are currently under final testing. S/Key is available via anonymous ftp from thumper.bellcore.edu:/pub/nmh.

Secure Programming

Whilst some of the problems with security on computer systems are related to design, the proliferation of third party software packages has opened up a new world of security vulnerabilities. Often here, the problems relate to either inexperienced programmers or inadequate care when coding the system. The problem of how to write secure systems has been analysed for many years now, and it is possible to write secure systems if a number of basic mistakes are avoided.

Many of the solutions and programming styles simply come down to being as conservative as possible with programming, and never trusting the environment the program is operating in. Matt Bishop wrote an excellent paper which can also be found as an Appendix in Rik Farrow's book. His advice included:

Close all file descriptors before calling exec()
Checking the environment
Never using relative filenames
Catching all signals
Making only safe assumptions about error recovery
Verifying all input data and its source
Not coding in race conditions (i.e., not allowing the environment to be ever be vulnerable, not even between two instructions).

UNIX Security - Publications

De Alvare A., How Crackers Crack Passwords or What Passwords to Avoid, Proceedings of the UNIX Security Workshop II, Portland, August 1990

Arnold N., UNIX Security: A Practical Tutorial, McGraw-Hill Inc., 1993

Bishop M., How to Write a Setuid Program, ;login, Volume 12, Number 1, January/February 1987

Bellovin S. and Merrit M., Limitations of the Kerberos Authentication System, Proceedings of the USENIX Winter 1991

Cheswick W., An evening with Berferd in which a Cracker is Lured, Endured, and Studied, Proceedings of the Winter USENIX Conference, San Francisco, January 1992

Curry D., Improving the Security of your UNIX System, ITSTD-721-FR-90-21, SRI International, April 1990

Farrow R., UNIX System Security: How to Protect your Data and Prevent Intruders, Addison-Wesley, April 1991

Grottola M., The UNIX Audit: Using UNIX to Audit UNIX, McGraw-Hill Inc., 1993

Garfinkel S. and Spafford E. Practical UNIX Security, O'Reilley and Associates Inc., 1991

Koblas D. and Koblas M., SOCKS, Proceedings of the USENIX Security Symposium, 1992

Klein D.,	"Foiling the Cracker": A Survey of, and Improvements to, Password Security, Proceedings of the UNIX Security Workshop II, Portland, August 1990
Tanenbaum A.,	Computer Networks, Prentice-Hall International Inc., 1989
SA-93.03	SERT Advisory SA-93.03, Suggested Login Banner
SA-93.04	SERT Advisory SA-93.04, Guidelines for Developing a Sensible Password Policy
SA-93.06	SERT Advisory SA-93.06, UNIX Computer Security Checklist
SA-93.10	SERT Advisory SA-93.10, sendmail vulnerability

VMS Security - Basics

VMS contains a number of useful security features that help protect the system from intrusion. These should be studied (by reading the manuals), and then enabled and configured to the needs of the system. "Generally", an intruder must be able to login to the system before further damage can be done, provided a number of services are disabled.

DECnet Wrapper

Rob McMillan (SERT) is developing a DECnet Wrapper (similar in operation to the `tcp_wrapper`) which can control access to DECnet objects based upon remote nodename and username. It will be an extremely useful tool, and is hoped to be available in the new year.

System Password

VMS has the concept of a "system password". This is not the password to the SYSTEM account, but a password used to gain initial access to the system. When the system password is enabled, any enabled interactive connections to the system will connect, but be met with no prompt at all. This generally confuses the intruder who is at least expecting some identification for the system. If the general access password is entered correctly, then the normal `Username:` prompt is supplied. Else, the connection is aborted. This is only really useful for small community systems. Large general access systems would not find the system password scheme very effective.

SYSGEN Parameters

A number of SYSGEN parameters can be adjusted to affect the security of the VMS system. The Security manuals contain details of the parameters and their effect.

Access to the SYSTEM Account

The account "SYSTEM" is a general privileged account that is well known by intruders (similar to root for UNIX). Therefore, access to this account should be tightly controlled through the use of the UAF fields.

Disable the TASK Object

The DECnet TASK object allows anyone to run a command file on the system. If this is not required, it should be disabled by removing it (setting a default account and password is not sufficient as any valid account and password may still be supplied).

Login Banner

A login banner should be displayed each time a user connects to the system. See the SERT Advisory SA-93.03 for further details. SERT Advisories can be obtained via anonymous ftp from ftp.sert.edu.au:/security/sert/sert-advisory.

ACLs

Access Control Lists can be used to further tune the VMS entity protection to individual users. These are a good idea if tight control is required to system resources. Consult the VMS Security manuals for more information.

Proxies

Proxies represent a "trust" relationship, and care must be taken to ensure that the trust chain cannot be broken or tampered with. If there is any doubt, then proxies should not be used. This unfortunately exposes the password to network monitoring.

VMS Security - Tools

Supervisor

Supervisor displays all input and output to a terminal device on another terminal device. Supervisor offers two modes of monitoring: Observer and Advisor.

Observer mode allows a privileged user to view every character typed and printed at another user's terminal. The effect is that both users, initiator and target, see the same screen at the same time.

Advisor mode allows a terminal user to type command lines, comments, and program input into the target user's terminal process. The effect is the same as if the user had typed the characters.

Photo is a similar utility that allows users to log their own terminal sessions into a file. While Photo is running, each character sent to and received from the terminal is recorded in a file and may be redisplayed later using the `playback` command.

DECnet Wrapper

The DECnet Wrapper is similar in functionality as that provided by the `tcp_wrapper` on UNIX systems. The DECnet wrapper also provides access to services based upon remote has and remote username. This is in contrast to the `tcp_wrapper` which can only provide access based upon the remote hostname. More details can be obtained from the author (R.McMillan@itc.gu.edu.au).

Audit Server

The audit server is an effective tool at determining breakin attempts. It should be used judiciously to provide the maximum amount of useful information. The audit server has the ability to flood the system administrator with irrelevant information, and therefore must be configured appropriately. Note, it is possible to adjust the level of audit logging from time to time (for example, by using a regular batch job). In this way audit logging may be increased for the quieter hours, and decreased during busy times.

ACLs

As described in the previous section, Access Control Lists may help to provide finer grain control over access to system objects and resources. If ACLs are to be used, careful thought must be given to the order that they will be processed in, so that the appropriate behaviour is attained. Consult the Access Control List Editor Manual for further details.

S/Key

S/Key is a software based one time password scheme. It was described in the section on UNIX Tools. A VMS based implementation is currently under development and testing within SERT and is expected to be available early in the new year.

VMS Security - Publications

Various VMS Manuals:

- DEC TCP/IP Services for VMS System Management
- Guide to VAX/VMS System Security
- Access Control List Editor Utility
- Accounting Utility
- Audit Analysis Utility
- Authorize Utility
- Guide to Maintaining a VMS System
- Network Control Program Manual
- Networking Manual

McMillan, R. A Practical Exercise in Securing an OpenVMS System, Proceedings DECUS Symposium, 1993, available via anonymous ftp from ftp.sert.edu.au:/security/sert/papers/VMS-Security.txt

X Security - Basics

X security is a difficult problem because many users are unaware that they are vulnerable. If a user can connect to an X server, they are then able to access a number of the facilities provided by the server, including monitoring every keystroke, or viewing what is on the screen. Therefore, X security is becoming an important issue, even if it does not represent a "flaw" in the security of the system.

If extra security is required, then the packets may be filtered by the firewall or router, to prevent them travelling outside of the local network. This does not provide a complete solution as the X servers are still vulnerable to local users, and it may be desirable to use X across the wider network.

The file `/etc/Xn.hosts` (e.g., `X0.hosts`) can be used to provide host based security. Note that any user on that host still has access to the X server.

The use of the MIT-MAGIC-COOKIE-1 allows per-user based security. This system creates a "magic cookie" which must be current and available in the $HOME/.Xauthority file for access to take place. If the correct magic cookie is not supplied, then access is denied. Note that this system is not available across all X platforms. In addition, how the magic cookie is securely obtained and moved to different systems is a local matter, and may be somewhat cumbersome. This usually means that this form of security is not viewed favourably, and may be abandoned as too difficult.

Finally, the CERT Coordination Centre released an Advisory recently detailing a vulnerability in the xterm package. Details on this can be found in CERT Advisory CA-93:17 on ftp.sert.edu.au:/security/cert/cert-advisories.

X Security - Tools

A number of public domain programs exist that will connect to the X server and capture keystrokes, input events, or even a copy of the entire displayed screen. Whilst these are not technically "tools", they do represent the style of program in use that is affected by the security of the X server. These programs are not available from SERT.

X Security - Publications

Mui L. and Pearce E., X Window System Administrator's Guide, O'Reilley and Associates Inc., 1992.

Manual pages for:

- X(1)
- Xsecurity(1)
- twm(1)
- mwm(1)
- olwm(1)
- chmod(1)
- screendump(1)
- xloadimage(1)
- xauth(1)
- xinit(1)
- sh(1)
- fbtab(5)