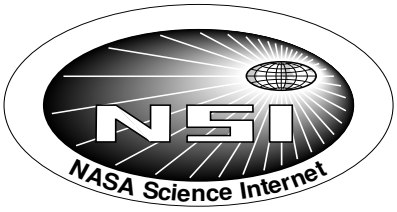

NASA Science Internet

Network Security Basics

A Primer for System Administrators

August 1993

Brad Olive,
NSI Network Security Manager

Prepared for the
NASA Science Internet Project Office
NASA Ames Research Center
By Sterling Software, Inc.
NAS2-13210-648

DO-SEC1043.0

NASA Science Internet

Network Security Basics

A Primer for System Administrators

Brad Olive, NSI Network Security Manager

INTRODUCTION

This document provides a quick overview of the NSI Network Security guidelines. All sites that are connected to the NASA Science Internet are required to follow the NSI Acceptable Use Policy and the NSI Network Security Policy. This document is intended to give the system administrators an overview of what is expected from their sites. Additional information on NSI Network Security can be found in the NSI Network Security Archive Handbook which describes the NSI Network Security Archive and the tools available there. The handbookt is available from the NAIC as well as the NSI anonymous ftp server. Please forward any comments or suggestions about this document to: *bolive@nsipo.arc.nasa.gov.*

The main focus of this document is the protecting systems connected to the NSI. Intruders obtain access to systems and use them to introduce worms, trojans or viruses to the system they have accessed and any other hosts that are trusted by that system. Over 90% of the recorded intrusions are due to poor password protection.

SCOPE OF PROTECTION

Computers connected to the Internet have to be protected from users on the local system and users on the thousands of other computers on the network. The Internet is a collection of millions of users worldwide. Each of these users potentially has access to the entire network, and not all of them are responsible network citizens. NSI has a responsibility to all sites connected to the NSI network, including users connected through other network providers, to prevent malicious activity from originating within, or causing problems on the NSI network.

REPORTING INTRUSIONS

If an intrusion is detected from the network, it should be reported immediately to the NSI Computer Emergency Response Team. The NSI-CERT can be contacted through the NOC 24-hour hotline. For problems that do not involve an intruder, the NSI-CERT can also be reached via e-mail at *nsi-cert@nsipo.arc.nasa.gov* . Intruders always read e-mail to see if they have been detected, so it is important to contact the NSI-CERT off-line to make sure that the intruder does not get scared and cause major damage to the system. Instructions for reporting an incident are available via the NSI anonymous ftp server.

INCIDENT HANDLING

When an intrusion (or other security problem) is detected within the NSI network, an attempt will be made by the NSI-CERT to contact the administrator at the originating site as well as the attacked site to discuss the problem. In serious cases, the connection to the site may be turned off until a resolution has been found. This connection may be terminated indefinitely in serious cases.

The site administrator needs to be aware of the security risks associated with running the system. Basic security includes user education, proper system monitoring and continual maintenance. When security is applied properly there is no decrease in accessibility, performance or increased maintenance time. In fact, secure systems are often easier to maintain.

SECURITY PLAN

An attack plan has to be made to help prevent intrusions from occurring. The first check should be for accounts with no password, or default passwords. These accounts are often used by service personnel and sometimes have system privileges. Lock open accounts and make sure that there are no default or easy passwords. Accounts that use the same name for the login as the password (or “Joe” accounts) should also be removed.

Many intruders *finger* systems to find account names and then attempt to log in with simple passwords. The NSI Security Archive Handbook has details on how to train users on passwords. If intruders can get a copy of the password file, they can run a program such as *crack* to try to guess passwords. It is important to make sure that all passwords on a system are changed if it appears that anyone has obtained a copy of the password file. System passwords should be changed immediately if there is a possibility that the password file has been taken.

All users should be educated on password privacy. Encourage them to pick a hard to guess password that they can remember without writing it down. A pro-active password checker (like *nsipasswd*) can be used to prevent easily guessed passwords.

Check all permission levels periodically though the system to make sure that system files are protected. If intruders change a system file they will have complete control over the system.

Install all patches and fixes distributed by the manufacturer or recommended by the nsi-cert. These fixes usually correct security holes in addition to the obvious bug that they claim. The security fixes are usually not mentioned to prevent panic and to keep the security problem quiet.

The Trivial File Transfer Protocol (TFTP) has also been a source of breakins on UNIX systems. There is a quick test that will show if a system is vulnerable to these attacks. The procedure is to connect to the system via *tftp* and try to " *get /etc/passwd* ". If the file is transferred, the system is weak. To correct a system that has the *tftp* vulnerability, disable *tftpd* , or install *tftpd* with restricted access.

Check file and directory permissions. System files and binary directories should have appropriate permissions. There are many utilities that are available to check these permissions for you.

On systems that allow secure ttys, the */etc/ttytab* or */etc/ttys* file needs to be checked for tty lines that are allowed to be secure. There should be no secure ttys other than a console or physically secure location. For tracking purposes, any user that needs root access should use the " *su* " command.

The *sendmail* bug has been corrected on many systems, however there are still some versions that have not been fixed. Verify that the system is running Berkeley version 5.65 or later of sendmail, or that the vendor's version has been fixed. Using " *telnet <host> 25* " will identify the vendor and version of sendmail running on that machine.

FTP is also a known source for intruder attacks. The Berkeley version 5.60 of July 22, 1990 corrected the known problems. The anonymous FTP service must be configured properly. This is done by verifying that the anonymous FTP root directory and the bin and etc subdirectories should not be owned by ftp.

The Morris Internet Worm used a *fingerd* hole. This is one of the most widely known bugs, and one that has been fixed on most every system. Versions of *finger* with a date after November 1988 contain the fix.

The */etc/hosts.equiv* , */etc/hosts.lpd* and all *~/.rhost* files should not contain a'+' entry. These files should not be world writeable. The */etc/inetd.conf* file should not contain the following entries unless they are required:

port 11 - systat
port 69 - tftp
port 87 - link

Support of *uucp* requires that the *L.cmds* file has only the commands that are required in it. The file should be owned by root, and world-readable. The *L.sys* file should be owned by *uucp* and protected to mode 600.

This covers the basic areas of system security, and is only the beginning. The NSI Network Security Archive Handbook will cover many of the tools available and provide additional insight into network security. A suggested reading list is also included for system administrators that have a desire to seek more information about systems and network security.