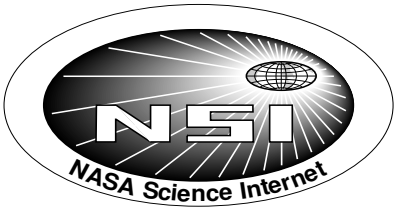


NASA Science Internet

Network Security Archive

Handbook

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-SEC1037.0

REVISION SHEET

Date	Section	Title and Instructions	Who
8/31/93	ALL	Initial Release of document Rev. 1.0	BGO

THIS PAGE INTENTIONALLY BLANK
(As are many others throughout this document)

1.0 Introduction

This document is intended for use by System and Network Administrators that are part of, or connected to, the NSI. This document provides an overview of the types of utilities, policies and useful things found in the security archive and is by no means all inclusive. See the appropriate README files in the archive for the latest information.

This handbook contains a description of each section of the archive, along with a summary about the files that are contained in each area. Helpful information, lessons learned and other interesting information about each of the files are also included. An attempt has been made to provide enough information about each of the files, however many of the tools contained in the archive have their own set of documentation.

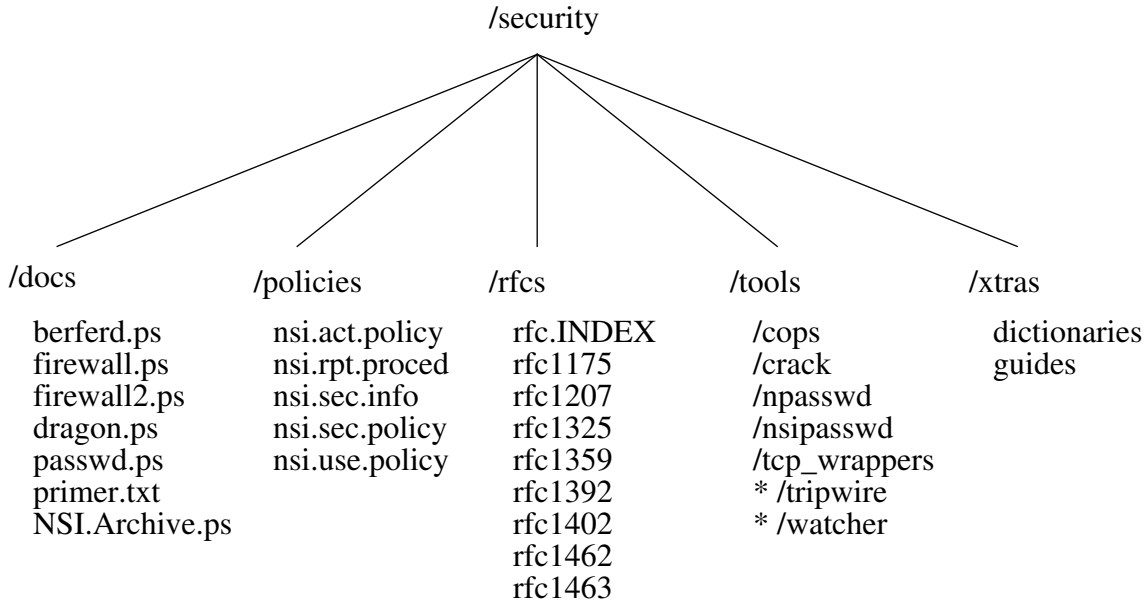
Any questions, comments or corrections should be forwarded to:

Brad Olive (bolive@nsipo.arc.nasa.gov)
Sterling Software
NASA Science Internet, Network Security Manager
+1-415-604-0670 voice
+1-800-998-6653 message/pager
+1-415-694-9970 pager

1.1 The NSI Network Security Archive Organization

The NSI Network Security Archive has been created to provide NSI systems and network administrators with a centralized location for policies, procedures, tools and other information that will be useful to them in maintaining secure systems.

The archive is maintained by the NSI Security Manager and consists of files that are available from various sources as well as custom tools created for the NSI community.



* Still under evaluation

This document is divided into sections corresponding to an area within the archive and describing the files contained in that section.

1.2 Accessing the Archive

The archive is available via anonymous ftp at nsipo.arc.nasa.gov. To access the system, ftp to nsipo.arc.nasa.gov and get the README.FIRST file out of the pub/security directory. To obtain access to the archive you must register with the security manager. Get the README.FIRST file for more details.

Each module or utility will also have its own README (or similarly named) file. Be sure to look at the README file for any instructions not contained in this document.

All of the files are in tar format and will have to be extracted and possibly compiled on your system. See the instructions that accompany each of the files (usually a README file).

2.0 /docs - Network Security Related Documents

The /docs archive contains documents covering various network security related issues.
As with any other issues related to network security, things are constantly changing. An attempt has been made to keep this document up to date, and to refer the reader to documents that are current and applicable. As documents become outdated or updated, this information will be changed.

2.1 berferd.ps - An Evening with Berferd In Which a Cracker is Lured, Endured and Studied
This is an excellent document by Bill Cheswick of AT&T Bell Laboratories about a cracker that believed that he had found the famous sendmail DEBUG hole on AT&T's Internet gateway. The hacker was led on for several months as he thought he was gaining access to the machine.

2.2 dragon.ps - There Be Dragons
This document was written by Steven M. Bellovin of AT&T Bell Laboratories and covers some of the things to look for in fighting off crackers. His examples come from actual experiences at AT&T and give insight into the various methods of tracking crackers.

2.3 firewall.ps - A Network Firewall
A description of the Internet gateway used by Digital Equipment Corporation/ Marcus J. Ranum.

2.4 firewall2.ps - Thinking About Firewalls
This document gives a brief introduction into firewalls and discusses several techniques for configuring a firewall system. This document was written by Marcus J. Ranum.

2.5 passwd.ps - Foiling the Cracker
This document by Daniel V. Klein of Carnegie Mellon University gives some actual statistics on their attempt to foil crackers with various tools. Of particular interest is the study of passwords and the probabilities presented of guessable passwords.

2.6 primer.txt - Coping with the Threat of Computer Security Incidents:
This document is a must for all security and systems personnel. As indicated by the title, this is a primer that discusses the most common areas that are vulnerable to security incidents. This document will introduce you to much of the terminology used in network security as well as provide a foundation for security administrators to build upon. There is also a section on incident handling and recovery.

2.7 NSI.Archive.ps - NSI Network Security Archive Handbook
You are reading this document. Since the archive is constantly changing, please verify that the document number matches the one in the README file located in the security archive.

2.8 NSI_Security_Intro.ps - NSI Network Security Introduction
This document is intended for all NSI users and explains the basics of computer security.

2.9 NSI_Security_Intro.ps - NSI Network Security Introduction
This document is intended for all NSI users and explains the basics of computer security.

2.10. NSI_Security_Primer.ps - NSI Network Security, A Primer for System Administrators
This document is intended for all NSI System Administrators to educate them on their network security responsibilities.

3.0 /policies - Network Policies and Procedures

The /policies archive contains the official NSI policies, as well as information about the implementation, need and enforcement of policies.

3.1 nsi.act.policy - User Account Policy

This policy has been created by customizing policies that have been used by other organizations as to the responsibilities of all account holders. Publishing this policy will inform all account holders of their responsibilities as a user to uphold the NSI Acceptable Use Policy.

3.2 nsi.rpt.proced - Incident Reporting Procedures

This is a must for all personnel that may be handling any security-related incidents. The proper escalation procedure, contact list and other information is included.

3.3 nsi.sec.info - NSI Network Security Office Information

A copy of the document introducing the NSI Network Security Office and the services that are provided.

3.4 nsi.sec.policy - NSI Security Policy

A copy of the NSI security policy has been included for reference.

3.5 nsi.use.policy - NSI Acceptable Use Policy

A copy of the NSI acceptable use policy has been included for reference.

4.0 /rfcs

There are a number of RFCs that relate to security issues. An index to all of the RFCs has been included along with a collection of a few RFCs that may be of interest to anyone handing network security issues. All RFCs are available via anonymous ftp at *nis.nsf.net*. The collection of RFCs available from this archive will be continually updated as new articles are submitted. Information on how to obtain RFCs not archived at this site is included in the index file *rfc.INDEX*.

The following is a sampling of the RFCs contained in the NSI Network Security Archive:

RFC	Description
1175	FYI on Where to Start - A Bibliography of Internetworking Information
1207	FYI on Questions and Answers - Answers to Commonly Asked "Experienced Internet User" Questions
1244	Site Security Handbook
1325	FYI on Questions and Answers: Answers to Commonly asked "New Internet User" Questions
1359	Connecting to the Internet What Connecting Institutions Should Anticipate
1392	Internet Users' Glossary
1402	There's Gold in them thar Networks! Searching for Treasure in all the Wrong Places
1462	FYI on "What is the Internet?"
1463	FYI on Introducing the Internet - A Short Bibliography of Introductory Internetworking Readings for the Network Novice

5.0 /tools - Network Security Tools

The /tools archive contains a set of useful tools that have been collected from various archives, and some that have been created especially for NSI Network and Systems personnel. Unless noted otherwise, the tools are for systems running the Unix operating system. Each of the tools has been run and tested by the NSI Network Security Team. In many cases the code has been modified to accommodate the requirements of NSI.

Whenever possible, the appropriate programs should be run on all systems that have Internet access. Even though some of these programs may take awhile to configure and set up, most of them require little, if any, work as time goes on. A system that has never been checked by any of these utilities is considered more vulnerable than those which run the utilities. While none of these programs is foolproof, the use of these tools can greatly reduce the risk of an attack, and reduce the time required to restore a machine to the original state. To restore a system that has been running these utilities, a simple check will identify the corrupt files and holes. A system that was left unprotected will usually require a complete reinstallation. Taking a few moments now to set up a security plan may save days, or weeks, of work should the system be compromised.

The descriptions of the package and how it operates has either been taken from the actual tool documentation or created from the information contained in the tool documentation along with practical experience.

Since there are many different utilities, programs and scripts that all proclaim to be useful in helping identify security holes, this document will attempt to identify those that have been found to be worthwhile. As new utilities are found, or brought to the attention of the security team, they will be evaluated, tested and included as seen fit.

Network security problems exist in many areas. From the number of utilities that are available, it becomes obvious where the majority of the problems exist. The most obvious problem is access to the computer system using an account that is easily compromised. File permissions and easily broken passwords are by far the most common break-in points, and therefore have the largest collection of utilities to assist in the detection of these problems.

Packages that have been evaluated but not included in the archive are listed in Appendix B with comments as to the reason it was not included.

For these utilities to work, the system must be easily accessed by those authorized to use it. The utilities outlined in this document attempt to provide the proper level of security without restricting authorized users.

The utility collection COPS (Computer Oracle and Password System) has been revised several times since its introduction and contains a number of useful utilities. This collection will check most Unix systems for common file permission problems and to some extent password problems. COPS is a tool that should be run on a regular basis. By doing this, security problems are identified as they happen, and the reports generated will be smaller, thus freeing up your time for more important duties.

There are many password programs that attempt to break passwords. Easily guessed passwords are the most common point of compromise on any system. Programs such as *crack* will identify common password problems. For systems using shadowed password files, it is still important to run some sort of password checker to ensure that there are no accounts without passwords, or other easily guessed passwords. While *crack* is a useful tool, it will take hours or days to make its initial run. Subsequent runs are quicker since the program keeps track of the uncrackable entries, however there are easier ways to provide good password security.

The first step to password security is to prevent a user from picking an easily guessed password. Easily guessed passwords are names, words or other common identifying items. If the system were to assign a password, it would most likely get written down making it easy for someone to find. Allowing the user to select a password is the best method, however steps must be taken to ensure that the password is not easily cracked. There are several utilities included in the archive that will provide this checking. The program *crack* notifies the user after they have been using their password that it is not secure, while *npasswd* and *nsipasswd* prevent them from choosing an insecure password.

A common request that is received by any network provider is to isolate traffic from a given source. This can be done at the local host using wrapper utilities such as the tcp_wrapper program. With this package you can monitor nearly all incoming connections. The wrappers also log pertinent information about the connections, and allow the administrator to restrict what systems can connect to your network.

5.1 COPS - Computer Oracle and Password System

The COPS package is actually a collection of scripts that assist the system manager in finding potential security problems with their Unix system. Cops was written by Dan Farmer.

COPS will assist the Unix administrator with automated checks of common vulnerable areas.

Who should use COPS:

All Unix systems administrators should use COPS on a regular basis to ensure that their system has the most common vulnerable areas protected. This program can be launched by a cron entry and automatically deliver mail to the systems administrator on a regular basis.

How difficult / Time consuming is COPS:

COPS is fairly simple to install on most systems and will require under an hour to get the package installed and running in its basic mode. This time is well worth it to ensure that areas of vulnerability are covered.

Here is what the program currently checks:

- File, directory, and device permissions/modes.
- Poor passwords.
- Content, format, and security of password and group files.
- Programs and files run in /etc/rc* and cron(tab) files.
- Existence of root-SUID files, their permissions, and type.
- CRC checks against important binaries/key files to report changes.
- Writability of users home directories and startup files (.profile, .cshrc, etc.)
- Anonymous ftp setup.
- Unrestricted tftp, decode alias in sendmail, SUID uudecode problems.
- inetd.conf, rexd running in inetd.conf.
- Current directory in the search path, a "+" in /etc/host.equiv,
- Unrestricted NFS mounts, ensuring root is in /etc/ftpusers, etc.
- Dates of CERT advisories vs. key files.

5.2 crack - Password discovery program

Crack should be run by administrators who do not implement a program such as *npasswd* or *nsi-passwd*, or by systems that have installed one of these utilities and are ready to implement safe passwords. It is also a good idea to periodically run this on any system to ensure that the proactive password program is really functioning. Every administrator and security person has their own opinion on password selection which is a topic for another discussion, however it is important to make sure that your passwords are secure.

This program is a good starting point for administrators to use on any Unix system that uses the standard eight-character DES encrypted passwords. The first run of *crack* will take quite some time. If you do not change your dictionary file, the future *crack* runs will take less time since the encrypted passwords that have not been guessed are all stored in a file. This means that subsequent runs will only check passwords that have changed since the last run.

Crack has a set of rules that can be modified by the administrator. As *crack* runs, the program first identifies all of the salts used in your password file. Next, the program takes each word in the dictionary file and applies the rule to each word, encrypts it with the salt, and looks for a match with the encrypted passwords that use the same salt. Once it has completed a rule with all of the salts, it continues on to the next rule following the same method. If a password passes all of the tests, it will be saved in a file so that it is not tested the next time crack is run. If the dictionary is changed, all of the passwords will need to be tested again.

To set up and run crack, get the archive file off of the system.

Crack requires the password file that contains the encrypted passwords. This file is usually /etc/passwd, or if the system is using adjunct passwords, /etc/security/passwd.adjunct is the most likely location for this file.

The documentation that comes with the program is fairly complete, however we have included a larger dictionary for the crack runs. To install the program, set up the Crack script with the proper paths. Before running it, verify that the file Dicts/bigdict.Z exists and touch the file Dicts/.lockfile to ensure that the dictionary does not get rebuilt. If you want to create another dictionary, follow the instructions in the documentation, or add the words that you need to the file bigdict.Z by following these simple steps:

1) create a list of new words.
2) uncompress bigdict.
3) use comp to get the words from your new list that are not in bigdict.
4) cat these to the end of bigdict.
5) sort the file bigdict and recompress it.

5.3 npasswd - Proactive Password Changer

The npasswd password program is a replacement for passwd that checks passwords against a check similar to crack. The rules can be modified by the administrator, and site specific checks can be made. This prevents a user from selecting passwords that are contained in the dictionary, or are easily guessed. The program nsipasswd is more robust and recommended over this one for all sites. This program is included for sites that do not have perl, or other resources, to run the nsipasswd program.

Although this program does not provide any password history or aging, it is a simple program to install and will instill a fair amount of security for passwords.

npasswd was written by: Clyde Hoover <clyde@emx.utexas.edu>
This version includes a set of installation scripts that were created by Dan Kegel at JPL and modified by Brad Olive for the NSI.

This program will check against a set of rules that are created by the administrator, and uses a dictionary that can be modified. Additional dictionaries are also available in the NSI Network Security Archive.

Use this program only if you are unable to run nsipasswd.

Installation is simple since there is an installation script. Uncompress and extract the file npasswd.tar.Z and edit the compile_npasswd file with the proper DEST directory and verify all other paths in this file. You will also need to edit the install_npasswd script to identify the proper DEST and dictionary list. As an alternative, you can use the dictionary from crack (bigdict) which would require a minor change to the Makefile.

Once the files are edited, execute the compile_npasswd and install_npasswd scripts.

You are now ready to run the program. Before beginning, make sure that you have a window open as the super user, and that you have a copy of the password files:

> /etc/passwd
> /etc/security/passwd.adjunct (as appropriate)

This is in case a recovery is required due to something failing. The most common problem is to have the password file overwrite the adjunct file locking all users (including root) out of the system.

Once you have changed a password, verify that the only change is the encrypted portion of the proper password file (/etc/passwd or /etc/security/passwd.adjunct). If there are other changes, make a copy of the corrupt file and restore the original(s) before trying to determine the problem. If the adjunct file gets overwritten with the /etc/passwd file, the most likely cause is that the program cannot locate the password adjunct file in the /etc/security directory.

5.4 nsipasswd - Proactive Password Changer & Aging Perl Script Version 1.0

The nsipasswd program is a proactive password changing program that runs a number of tests on a password that a user enters. These rules can be modified by the administrator to make them stricter or milder. The combination that is included by default is fairly secure when used with the dictionaries that are included in the distribution.

This program will work with adjunct passwords, but there is no Sun NIS support at this time.

One feature of this program is the password memory. This will prevent a user from reusing a password that they have used before. Currently, this program remembers forever, however a utility for aging the file will be available shortly. Password expiration is also possible, and a separate utility will be created to provide aging capability.

This script is an adaptation of the script found in Chapter 6 of *Programming perl,* by Larry Wall and Randall Schwartz. Several modifications were taken from the program anlpasswd, which is the same script modified by Argonne National Laboratory. Thanks to Mark Henderson and his organization for the ideas.

In addition to allowing the user to change their password, nsipasswd allows the user to change their default shell and gecos information. The gecos information is usually ignored by the current versions of *finger* for security reasons, however a local finger script can be created to read this information for users of the local system.

The NSI modifications to this script were made by Brad Olive. If you have any comments or questions, send them to Brad at bolive@nsipo.arc.nasa.gov.

Where to start:

Once you have the file nsipasswd.tar.Z, uncompress and extract the tar file.(This can be done with zcat) This will create the subdirectory nsipasswd with all of the required files located in the directory. You will need to decide where the dictionary is going to be stored and where the program executables are going to be placed. The program creates 1 dictionary that has been compiled from dozens of dictionaries. This dictionary includes the standard */usr/dict/words* dictionary, and all words have been truncated at 8 characters to speed up processing. Edit the *Makefile* and the *nsipasswd.pl* script. The variables that point to the dictionaries are:

passwd.perl - $dictdir
Makefile - $DICTLOC

You also need to determine the location of the program nsipasswd.pl. This is specified in the makefile and in the c-wrapper program suidwrap.c:

Makefile - $PROGLOC
suidwrap.c - Line 20 - eargv[2] = “(Expand $PROGLOC)/nsipasswd.pl”;
i.e. - eargv[2] = “/var/local/nsipasswd.pl”;

The file *passhist* is created in */etc.* If you need to change the location of the password history file, you will need to change the *nsipasswd.pl* script. Make sure this file is *chmod* 600. This file contains the user-id, the last encrypted password and the date the password was used. This file is used to prevent re-use of passwords and will also be consulted by the expiration script.

Once you have made these changes, you are ready to begin the installation.

Installation:

From the nsipasswd directory that contains the files, as the super user, execute the makefile by typing:

make all

This will compile the c-wrapper program, install the wrapper and the perl script, uncompress the dictionaries and set the proper permissions.

If you wish to use the perl finger program, *finger.pl*, *chmod* the file 755, change it's name to whatever you want to call the program (e.g. lfinger) and place it in a location that will be in everyone's path.

You are now ready to run the program. Before beginning, make sure that you have a window open as the super user, and that you have a copy of the password files:

/etc/passwd
/etc/security/passwd.adjunct (as appropriate)

This is in case a recovery is required due to something failing. The most common problem is to have the password file overwrite the adjunct file locking all users (including root) out of the system.

Once you have changed a password, verify that the only change is the encrypted portion of the proper password file (*/etc/passwd or /etc/security/passwd.adjunct*). If there are other changes, make a copy of the corrupt file and restore the original(s) before trying to determine the problem.

5.5 tcp_wrappers - TCP/IP access control

Wrapper programs can be an effective way to monitor all incoming connections to your system. These wrappers can also limit access and provide other security features. Using a wrapper can increase the administrators awareness as to what services are being accessed, and by whom. If the standard logs are reviewed, intruder attempts can be seen and dealt with.

For the beginner, it is suggested that the wrappers be installed and run without adding any of the restrictions to familiarize them with the logs. Once the logs have been reviewed and analyzed, a decision can be made to set up proper access controls. Failing to do this may result in the system being unaccessible to the network.

This package includes tiny daemon wrapper programs that can be installed without any changes to existing software or to existing configuration files. The wrappers report the name of the remote host and of the requested service; the wrappers do not exchange information with the remote client process, and impose no overhead on the actual communication between the client and server applications.

With this package you can monitor incoming connections to the SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, TALK, and other network services.

Early versions of the programs were tested with Ultrix >= 2.2, with SunOS >= 3.4 and ISC 2.2. Later versions have been installed on a wide variety of platforms such as SunOS 4.x and 5.x, Ultrix 3.x and 4.x, DEC OSF/1 T1.2-2, HP-UX 8.x, AIX 3.1.5, Apollo SR10.3.5, Sony, NeXT, SCO UNIX, DG/UX, Cray, and an unknown number of other ones.

Requirements are that the network daemons are spawned by a super server such as the inetd, a 4.3BSD-style socket programming interface, and the availability of a syslog(3) library and of a syslogd(8) daemon. The wrappers should run without modification on any system that satisfies these requirements. Workarounds have been implemented for several common bugs in systems software.

6.0 /xtras - Extras

dictionaries

This directory contains the dictionaries that are used by crack, nsipasswd or any other utility requiring large dictionaries. There are many different dictionaries, however the nsidict.tar file contains a unique set of words that have all be truncated at 8 characters. This file has no duplicates. The other files contain the raw data that was used to generate nsidict.tar.

Dictionaries other than nsidict.tar may be removed as disk space requires.

guides

This section contains guides that will be helpful to systems and security personnel. They are included here because they are not specifically security related, but cover more general topics related to systems administration, network use or other helpful ideas.

Appendix A - References

This section contains a list of reference books with annotated bibliographies from RFC1244 for your reference.

A.1 Computer Law

[ABA89] American Bar Association, Section of Science and Technology, "Guide to the Prosecution of Telecommunication Fraud by the Use of Computer Crime Statutes", American Bar Association, 1989.

[BENDER] Bender, D., "Computer Law: Evidence and Procedure", M. Bender, New York, NY, 1978-present. Kept up to date with supplements. Years covering 1978-1984 focuses on: Computer law, evidence and procedures. The years 1984 to the current focus on general computer law. Bibliographical references and index included.

[BLOOM] Bloombecker, B., "Spectacular Computer Crimes", Dow Jones- Irwin, Homewood, IL. 1990.

[CCH] Commerce Clearing House, "Guide to Computer Law", (Topical Law Reports), Chicago, IL., 1989. Court cases and decisions rendered by federal and state courts throughout the United States on federal and state computer law. Includes Case Table and Topical Index.

[CONLY] Conly, C., "Organizing for Computer Crime Investigation and Prosecution", U.S. Dept. of Justice, Office of Justice Programs, Under Contract Number OJP-86-C-002, National Institute of Justice, Washington, DC, July 1989.

[FENWICK] Fenwick, W., Chair, "Computer Litigation, 1985: Trial Tactics and Techniques", Litigation Course Handbook Series No. 280, Prepared for distribution at the Computer Litigation, 1985: Trial Tactics and Techniques Program, February-March 1985.

[GEMIGNANI] Gemignani, M., "Viruses and Criminal Law", Communications of the ACM, Vol. 32, No. 6, Pgs. 669-671, June 1989.

[HUBAND] Huband, F., and R. Shelton, Editors, "Protection of Computer Systems and Software: New Approaches for Combating Theft of Software and Unauthorized Intrusion", Papers presented at a workshop sponsored by the National Science Foundation, 1986.

[MCEWEN] McEwen, J., "Dedicated Computer Crime Units", Report Contributors: D. Fester and H. Nugent, Prepared for the National Institute of Justice, U.S. Department of Justice, by Institute for Law and Justice, Inc., under contract number OJP-85-C-006, Washington, DC, 1989.

[PARKER] Parker, D., "Computer Crime: Criminal Justice Resource Manual", U.S. Dept. of Justice, National Institute of Justice, Office of Justice Programs, Under Contract Number OJP-86-C-002, Washington, D.C., August 1989.

[SHAW] Shaw, E., Jr., "Computer Fraud and Abuse Act of 1986, Congressional Record (3 June 1986), Washington, D.C., 3 June 1986.

[TRIBLE] Trible, P., "The Computer Fraud and Abuse Act of 1986", U.S. Senate Committee on the Judiciary, 1986.

A.2 Computer Security

[CAELLI] Caelli, W., Editor, "Computer Security in the Age of Information", Proceedings of the Fifth IFIP International Conference on Computer Security, IFIP/Sec '88.

[CARROLL] Carroll, J., "Computer Security", 2nd Edition, Butterworth Publishers, Stoneham, MA, 1987.

[COOPER] Cooper, J., "Computer and Communications Security: Strategies for the 1990s", McGraw-Hill, 1989.

[BRAND90] Brand, R., "Coping with the Threat of Computer Security Incidents: A Primer from Prevention through Recovery", R. Brand, 8 June 1990. As computer security becomes a more important issue in modern society, it begins to warrant a systematic approach. The vast majority of the computer security problems and the costs associated with them can be prevented with simple inexpensive measures. The most important and cost effective of these measures are available in the prevention and planning phases. These methods are presented in this paper, followed by a simplified guide to incident handling and recovery. Available on-line from: cert.sei.cmu.edu:/pub/info/primer.

[CHESWICK] Cheswick, B., "The Design of a Secure Internet Gateway", Proceedings of the Summer Usenix Conference, Anaheim, CA, June 1990. Brief abstract (slight paraphrase from the original abstract): AT&T maintains a large internal Internet that needs to be protected from outside attacks, while providing useful services between the two. This paper describes AT&T's Internet gateway. This gateway passes mail and many of the common Internet services between AT&T internal machines and the Internet. This is accomplished without IP connectivity using a pair of machines: a trusted internal machine and an untrusted external gateway. These are connected by a private link. The internal machine provides a few carefully-guarded services to the external gateway. This configuration helps protect the internal internet even if the external machine is fully compromised. This is a very useful and interesting design. Most firewall gateway systems rely on a system that, if compromised, could allow access to the machines behind the firewall. Also, most firewall systems require users who want access to Internet services to have accounts on the firewall machine. AT&T's design allows AT&T internal internet users access to the standard services of TELNET and FTP from their own workstations without accounts on the firewall machine. A very useful paper that shows how to maintain some of the benefits of Internet connectivity while still maintaining strong security.

[CURRY] Curry, D., "Improving the Security of Your UNIX System", SRI International Report ITSTD-721-FR-90-21, April 1990. This paper describes measures that you, as a system administrator can take to make your UNIX system(s) more secure. Oriented primarily at SunOS 4.x, most of the information covered applies equally well to any Berkeley UNIX system with or without NFS and/or Yellow Pages (NIS). Some of the information can also be applied to System V, although this is not a primary focus of the paper. A very useful reference, this is also available on the Internet in various locations, including the directory cert.sei.cmu.edu:/pub/info.

[FITES] Fites, M., Kratz, P. and A. Brebner, "Control and Security of Computer Information Systems", Computer Science Press, 1989. This book serves as a good guide to the issues encountered in forming computer security policies and procedures. The book is designed as a textbook for an introductory course in information systems security. The book is divided into five sections: Risk Management (I), Safeguards: security and control measures, organizational and administrative (II), Safeguards: Security and Control Measures, Technical (III), Legal Environment and Professionalism (IV), and CICA Computer Control Guidelines (V). The book is particularly notable for its straight-forward approach to security, emphasizing that common sense is the first consideration in designing a security program. The authors note that there is a tendency to look to more technical solutions to security problems while overlooking organizational controls which are often cheaper and much more effective. 298 pages, including references and index.

[GARF] Garfinkel, S, and E. Spafford, "Practical Unix Security", O'Reilly & Associates, ISBN 0-937175-72-2, May 1991. Approx 450 pages, $29.95. Orders: 1-800-338-6887 (US & Canada), 1-707-829-0515 (Europe), email: nuts@ora.com This is one of the most useful books available on Unix security. The first part of the book covers standard Unix and Unix security basics, with particular emphasis on passwords. The second section covers enforcing security on the system. Of particular interest to the Internet user are the sections on network security, which address many of the common security problems that afflict Internet Unix users. Four chapters deal with handling security incidents, and the book concludes with discussions of encryption, physical security, and useful checklists and lists of resources. The book lives up to its name; it is filled with specific references to possible security holes, files to check, and things to do to improve security. This book is an excellent complement to this handbook.

[GREENIA] Greenia, M., "Computer Security Information Sourcebook", Lexikon Services, Sacramento, CA, 1989. A manager's guide to computer security. Contains a sourcebook of key reference materials including access control and computer crimes bibliographies.

[HOFFMAN] Hoffman, L., "Rogue Programs: Viruses, Worms, and Trojan Horses", Van Nostrand Reinhold, NY, 1990. (384 pages, includes bibliographical references and index.)

[JOHNSON] Johnson, D., and J. Podesta, "Formulating A Company Policy on Access to and Use and Disclosure of Electronic Mail on Company Computer Systems". A white paper prepared for the EMA, written by two experts in privacy law. Gives background on the issues, and presents some policy options. Available from: The Electronic Mail Association (EMA) 1555 Wilson Blvd, Suite 555, Arlington, VA, 22209. (703) 522-7111.

[KENT] Kent, Stephen, "E-Mail Privacy for the Internet: New Software and Strict Registration Procedures will be Implemented this Year", Business Communications Review, Vol. 20, No. 1, Pg. 55, 1 January 1990.

[LU] Lu, W., and M. Sundareshan, "Secure Communication in Internet Environments: A Hierachical Key Management Scheme for End-to-End Encryption", IEEE Transactions on Communications, Vol. 37, No. 10, Pg. 1014, 1 October 1989.

[LU1] Lu, W., and M. Sundareshan, "A Model for Multilevel Security in Computer Networks", IEEE Transactions on Software Engineering, Vol. 16, No. 6, Page 647, 1 June 1990.

[NSA] National Security Agency, “Information Systems Security Products and Services Catalog”, NSA, Quarterly Publication. NSA’s catalogue contains chapter on: Endorsed Cryptographic Products List; NSA Endorsed Data Encryption Standard (DES) Products List; Protected Services List; Evaluated Products List; Preferred Products List; and Endorsed Tools List. The catalogue is available from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. One may place telephone orders by calling: (202) 783-3238.

[OTA] United States Congress, Office of Technology Assessment, “Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information”, OTA-CIT-310, October 1987. This report, prepared for congressional committee considering Federal policy on the protection of electronic information, is interesting because of the issues it raises regarding the impact of technology used to protect information. It also serves as a reasonable introduction to the various encryption and information protection mechanisms. 185 pages. Available from the U.S. Government Printing Office.

[PALMER] Palmer, I., and G. Potter, “Computer Security Risk Management”, Van Nostrand Reinhold, NY, 1989.

[PFLEEGER] Pfleeger, C., “Security in Computing”, Prentice-Hall, Englewood Cliffs, NJ, 1989. A general textbook in computer security, this book provides an excellent and very readable introduction to classic computer security problems and solutions, with a particular emphasis on encryption. The encryption coverage serves as a good introduction to the subject. Other topics covered include building secure programs and systems, security of database, personal computer security, network and communications security, physical security, risk analysis and security planning, and legal and ethical issues. 538 pages including index and bibliography.

[SHIREY] Shirey, R., “Defense Data Network Security Architecture”, Computer Communication Review, Vol. 20, No. 2, Page 66, 1 April 1990.

[SPAFFORD] Spafford, E., Heaphy, K., and D. Ferbrache, “Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats”, ADAPSO, 1989. (109 pages.) This is a good general reference on computer viruses and related concerns. In addition to describing viruses in some detail, it also covers more general security issues, legal recourse in case of security problems, and includes lists of laws, journals focused on computers security, and other security-related resources. Available from: ADAPSO, 1300 N. 17th St, Suite 300, Arlington VA 22209. (703) 522-5055.

[STOLL88] Stoll, C., “Stalking the Wily Hacker”, Communications of the ACM, Vol. 31, No. 5, Pgs. 484-497, ACM, New York, NY, May 1988. This article describes some of the technical means used to trace the intruder that was later chronicled in “Cuckoo’s Egg” (see below).

[STOLL89] Stoll, C., “The Cuckoo’s Egg”, ISBN 00385-24946-2, Doubleday, 1989. Clifford Stoll, an astronomer turned UNIX System Administrator, recounts an exciting, true story of how he tracked a computer intruder through the maze of American military and research networks. This book is easy to understand and can serve as an interesting introduction to the world of networking. Jon Postel says in a book review, “[this book] ... is absolutely essential reading for anyone that uses or operates any computer connected to the Internet or any other computer network.”

[VALLA] Vallabhaneni, S., “Auditing Computer Security: A Manual with Case Studies”, Wiley, New York, NY, 1989.

A.3 Ethics

[CPSR89] Computer Professionals for Social Responsibility, "CPSR Statement on the Computer Virus", CPSR, Communications of the ACM, Vol. 32, No. 6, Pg. 699, June 1989. This memo is a statement on the Internet Computer Virus by the Computer Professionals for Social Responsibility (CPSR).

[DENNING] Denning, Peter J., Editor, "Computers Under Attack: Intruders, Worms, and Viruses", ACM Press, 1990. A collection of 40 pieces divided into six sections: the emergence of worldwide computer networks, electronic breakins, worms, viruses, counterculture (articles examining the world of the "hacker"), and finally a section discussing social, legal, and ethical considerations. A thoughtful collection that addresses the phenomenon of attacks on computers. This includes a number of previously published articles and some new ones. The previously published ones are well chosen, and include some references that might be otherwise hard to obtain. This book is a key reference to computer security threats that have generated much of the concern over computer security in recent years.

[ERMANN] Ermann, D., Williams, M., and C. Gutierrez, Editors, "Computers, Ethics, and Society", Oxford University Press, NY, 1990. (376 pages, includes bibliographical references).

[FORESTER] Forester, T., and P. Morrison, "Computer Ethics: Tales and Ethical Dilemmas in Computing", MIT Press, Cambridge, MA, 1990. (192 pages including index.) From the preface: "The aim of this book is two-fold: (1) to describe some of the problems created by society by computers, and (2) to show how these problems present ethical dilemmas for computers professionals and computer users. The problems created by computers arise, in turn, from two main sources: from hardware and software malfunctions and from misuse by human beings. We argue that computer systems by their very nature are insecure, unreliable, and unpredictable -- and that society has yet to come to terms with the consequences. We also seek to show how society has become newly vulnerable to human misuse of computers in the form of computer crime, software theft, hacking, the creation of viruses, invasions of privacy, and so on." The eight chapters include "Computer Crime", "Software Theft", "Hacking and Viruses", "Unreliable Computers", "The Invasion of Privacy", "AI and Expert Systems", and "Computerizing the Workplace." Includes extensive notes on sources and an index.

[GOULD] Gould, C., Editor, "The Information Web: Ethical and Social Implications of Computer Networking", Westview Press, Boulder, CO, 1989.

[IAB89] Internet Activities Board, "Ethics and the Internet", RFC 1087, IAB, January 1989. Also appears in the Communications of the ACM, Vol. 32, No. 6, Pg. 710, June 1989. This memo is a statement of policy by the Internet Activities Board (IAB) concerning the proper use of the resources of the Internet. Available on-line on host ftp.nisc.sri.com, directory rfc, filename rfc1087.txt. Also available on host nis.nsf.net, directory RFC, filename RFC1087.TXT-1.

[MARTIN] Martin, M., and R. Schinzinger, "Ethics in Engineering", McGraw Hill, 2nd Edition, 1989.

[MIT89] Massachusetts Institute of Technology, “Teaching Students About Responsible Use of Computers”, MIT, 1985-1986. Also reprinted in the Communications of the ACM, Vol. 32, No. 6, Pg. 704, Athena Project, MIT, June 1989. This memo is a statement of policy by the Massachusetts Institute of Technology (MIT) on the responsible use of computers.

[NIST] National Institute of Standards and Technology, “Computer Viruses and Related Threats: A Management Guide”, NIST Special Publication 500-166, August 1989.

[NSF88] National Science Foundation, “NSF Poses Code of Networking Ethics”, Communications of the ACM, Vol. 32, No. 6, Pg. 688, June 1989. Also appears in the minutes of the regular meeting of the Division Advisory Panel for Networking and Communications Research and Infrastructure, Dave Farber, Chair, November 29-30, 1988. This memo is a statement of policy by the National Science Foundation (NSF) concerning the ethical use of the Internet.

[PARKER90] Parker, D., Swope, S., and B. Baker, “Ethical Conflicts: Information and Computer Science, Technology and Business”, QED Information Sciences, Inc., Wellesley, MA. (245 pages).

A.4 The Internet Worm

[BROCK] Brock, J., "November 1988 Internet Computer Virus and the Vulnerability of National Telecommunications Networks to Computer Viruses", GAO/T-IMTEC-89-10, Washington, DC, 20 July 1989. Testimonial statement of Jack L. Brock, Director, U. S. Government Information before the Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce, House of Representatives.

[EICHIN89] Eichin, M., and J. Rochlis, "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988", Massachusetts Institute of Technology, February 1989. Provides a detailed dissection of the worm program. The paper discusses the major points of the worm program then reviews strategies, chronology, lessons and open issues, Acknowledgments; also included are a detailed appendix on the worm program subroutine by subroutine, an appendix on the cast of characters, and a reference section.

[EISEN89] Eisenberg, T., D. Gries, J. Hartmanis, D. Holcomb, M. Lynn, and T. Santoro, "The Computer Worm", Cornell University, 6 February 1989. A Cornell University Report presented to the Provost of the University on 6 February 1989 on the Internet Worm.

[GAO] U.S. General Accounting Office, "Computer Security - Virus Highlights Need for Improved Internet Management", United States General Accounting Office, Washington, DC, 1989. This 36 page report (GAO/IMTEC-89-57), by the U.S. Government Accounting Office, describes the Internet worm and its effects. It gives a good overview of the various U.S. agencies involved in the Internet today and their concerns vis-a-vis computer security and networking.Available on-line on host nnsc.nsf.net, directory pub, filename GAO_RPT; and on nis.nsf.net, directory nsfnet, filename GAO_RPT.TXT.

[REYNO89] The Helminthiasis of the Internet, RFC 1135, USC/Information Sciences Institute, Marina del Rey, CA, December 1989. This report looks back at the helminthiasis (infestation with, or disease caused by parasitic worms) of the Internet that was unleashed the evening of 2 November 1988. This document provides a glimpse at the infection,its festering, and cure. The impact of the worm on the Internet community, ethics statements, the role of the news media, crime in the computer world, and future prevention is discussed. A documentation review presents four publications that describe in detail this particular parasitic computer program. Reference and bibliography sections are also included. Available on-line on host ftp.nisc.sri.com directory rfc, filename rfc1135.txt. Also available on host nis.nsf.net, directory RFC, filename RFC1135.TXT-1.

[SEELEY89] Seeley, D., "A Tour of the Worm", Proceedings of 1989 Winter USENIX Conference, Usenix Association, San Diego, CA, February 1989. Details are presented as a "walk thru" of this particular worm program. The paper opened with an abstract, introduction, detailed chronology of events upon the discovery of the worm, an overview, the internals of the worm, personal opinions, and conclusion.

[SPAFF88] Spafford, E., “The Internet Worm Program: An Analysis”, Computer Communication Review, Vol. 19, No. 1, ACM SIGCOM, January 1989. Also issued as Purdue CS Technical Report CSD-TR-823, 28 November 1988. Describes the infection of the Internet as a worm program that exploited flaws in utility programs in UNIX based systems. The report gives a detailed description of the components of the worm program: data and functions. Spafford focuses his study on two completely independent reverse-compilations of the worm and a version disassembled to VAX assembly language.

[SPAFF89] Spafford, G., “An Analysis of the Internet Worm”, Proceedings of the European Software Engineering Conference 1989, Warwick England, September 1989. Proceedings published by Springer-Verlag as: Lecture Notes in Computer Science #387. Also issued as Purdue Technical Report #CSD-TR-933.

A.5 National Computer Security Center (NCSC)

All NCSC publications, approved for public release, are available from the NCSC Superintendent of Documents. NCSC was formerly known as the CSC, Compter Security Center.

National Computer Security Center
9800 Savage Road
Ft Meade, MD 20755-6000

National Telecommunications and Information Systems Security (NTISS)
NTISS Committee,
National Security Agency
Ft Meade, MD 20755-6000

[CSC] Department of Defense, "Password Management Guideline", CSC-STD-002-85, 12 April 1985, 31 pages. The security provided by a password system depends on the passwords being kept secret at all times. Thus, a password is vulnerable to compromise whenever it is used, stored, or even known. In a password-based authentication mechanism implemented on an ADP system, passwords are vulnerable to compromise due to five essential aspects of the password system: 1) a password must be initially assigned to a user when enrolled on the ADP system; 2) a user's password must be changed periodically; 3) the ADP system must maintain a 'password database'; 4) users must remember their passwords; and 5) users must enter their passwords into the ADP system at authentication time. This guideline prescribes steps to be taken to minimize the vulnerability of passwords in each of these circumstances.

[NCSC1] NCSC, "A Guide to Understanding AUDIT in Trusted Systems", NCSC-TG-001, Version-2, 1 June 1988, 25 pages. Audit trails are used to detect and deter penetration of a computer system and to reveal usage that identifies misuse. At the discretion of the auditor, audit trails may be limited to specific events or may encompass all of the activities on a system. Although not required by the criteria, it should be possible for the target of the audit mechanism to be either a subject or an object. That is to say, the audit mechanism should be capable of monitoring every time John accessed the system as well as every time the nuclear reactor file was accessed; and likewise every time John accessed the nuclear reactor file.

[NCSC2] NCSC, "A Guide to Understanding DISCRETIONARY ACCESS CONTROL in Trusted Systems", NCSC-TG-003, Version-1, 30 September 1987, 29 pages. Discretionary control is the most common type of access control mechanism implemented in computer systems today. The basis of this kind of security is that an individual user, or program operating on the user's behalf, is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control. [...] Discretionary controls are not a replacement for mandatory controls. In any environment in which information is protected, discretionary security provides for a finer granularity of control within the overall constraints of the mandatory policy.

[NCSC3] NCSC, “A Guide to Understanding CONFIGURATION MANAGEMENT in Trusted Systems”, NCSC-TG-006, Version-1, 28 March 1988, 31 pages. Configuration management consists of four separate tasks: identification, control, status accounting, and auditing. For every change that is made to an automated data processing (ADP) system, the design and requirements of the changed version of the system should be identified. The control task of configuration management is performed by subjecting every change to documentation, hardware, and software/ firmware to review and approval by an authorized authority. Configuration status accounting is responsible for recording and reporting on the configuration of the product throughout the change. Finally, though the process of a configuration audit, the completed change can be verified to be functionally correct, and for trusted systems, consistent with the security policy of the system.

[NTISS] NTISS, “Advisory Memorandum on Office Automation Security Guideline”, NTISSAM CONPUSEC/1-87, 16 January 1987, 58 pages. This document provides guidance to users, managers, security officers, and procurement officers of Office Automation Systems. Areas addressed include: physical security, personnel security, procedural security, hardware/software security, emanations security (TEMPEST), and communications security for stand-alone OA Systems, OA Systems used as terminals connected to mainframe computer systems, and OA Systems used as hosts in a Local Area Network (LAN). Differentiation is made between those Office Automation Systems equipped with removable storage media only (e.g., floppy disks, cassette tapes, removable hard disks) and those Office Automation Systems equipped with fixed media (e.g., Winchester disks). Additional NCSC Publications:

[NCSC4] National Computer Security Center, “Glossary of Computer Security Terms”, NCSC-TG-004, NCSC, 21 October 1988.

[NCSC5] National Computer Security Center, “Trusted Computer System Evaluation Criteria”, DoD 5200.28-STD, CSC-STD-001-83, NCSC, December 1985.

[NCSC7] National Computer Security Center, “Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments”, CSC-STD-003-85, NCSC, 25 June 1985.

[NCSC8] National Computer Security Center, “Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements”, CSC-STD-004-85, NCSC, 25 June 85.

[NCSC9] National Computer Security Center, “Magnetic Remanence Security Guideline”, CSC-STD-005-85, NCSC, 15 November 1985. This guideline is tagged as a “For Official Use Only” exemption under Section 6, Public Law 86-36 (50 U.S. Code 402). Distribution authorized of U.S. Government agencies and their contractors to protect unclassified technical, operational, or administrative data relating to operations of the National Security Agency.

[NCSC10] National Computer Security Center, “Guidelines for Formal Verification Systems”, Shipping list no.: 89-660-P, The Center, Fort George G. Meade, MD, 1 April 1990.

[NCSC11] National Computer Security Center, “Glossary of Computer Security Terms”, Shipping list no.: 89-254-P, The Center, Fort George G. Meade, MD, 21 October 1988.

[NCSC12] National Computer Security Center, “Trusted UNIX Working Group (TRUSIX) rationale for selecting access control list features for the UNIX system”, Shipping list no.: 90-076-P, The Center, Fort George G. Meade, MD, 1990.

[NCSC13] National Computer Security Center, “Trusted Network Interpretation”, NCSC-TG-005, NCSC, 31 July 1987.

[NCSC14] Tinto, M., “Computer Viruses: Prevention, Detection, and Treatment”, National Computer Security Center C1 Technical Report C1-001-89, June 1989.

[NCSC15] National Computer Security Conference, “12th National Computer Security Conference: Baltimore Convention Center, Baltimore, MD, 10-13 October, 1989: Information Systems Security, Solutions for Today - Concepts for Tomorrow”, National Institute of Standards and National Computer Security Center, 1989.

A.6 Security Checklists

[AUCOIN] Aucoin, R., “Computer Viruses: Checklist for Recovery”, Computers in Libraries, Vol. 9, No. 2, Pg. 4, 1 February 1989.

[WOOD] Wood, C., Banks, W., Guarro, S., Garcia, A., Hampel, V., and H. Sartorio, “Computer Security: A Comprehensive Controls Checklist”, John Wiley and Sons, Interscience Publication, 1987.

A.7 Additional Publications

Defense Data Network's Network Information Center (DDN NIC)
The DDN NIC maintains DDN Security bulletins and DDN Management bulletins online on the machine: NIC.DDN.MIL. They are available via anonymous FTP. The DDN Security bulletins are in the directory: SCC, and the DDN Management bulletins are in the directory: DDN-NEWS.

For additional information, you may send a message to: NIC@NIC.DDN.MIL, or call the DDN NIC at: 1-800-235-3155.

[DDN88] Defense Data Network, "BSD 4.2 and 4.3 Software Problem Resolution", DDN MGT Bulletin #43, DDN Network Information Center, 3 November 1988. A Defense Data Network Management Bulletin announcement on the 4.2bsd and 4.3bsd software fixes to the Internet worm.

[DDN89] DCA DDN Defense Communications System, "DDN Security Bulletin 03", DDN Security Coordination Center, 17 October 1989. IEEE Proceedings

[IEEE] "Proceedings of the IEEE Symposium on Security and Privacy", published annually. IEEE Proceedings are available from:

Computer Society of the IEEE
P.O. Box 80452 Worldway Postal Center
Los Angeles, CA 90080

Appendix B - Other Programs

This section lists other programs that have been evaluated by the NSI Network Security Team but are not included in the archive. A brief explanation of the program and the reason for its exclusion is included.

anlpasswd - This program is an excellent adaptation of the perl script that was used for nsipasswd. Many of the features of nsipasswd were taken from the anlpasswd program.

spi - Security Profile Imspector package. This is a toolkit of commands to help security ifficers perform security checks on a system. This is currently under evaluation.

tripwire - System Modification Watcher
Not included at this time - still under evaluation

watcher - System Modification Watcher
Not included at this time - still under evaluation

Copyrights and Affiliations

UNIX(r) is a registered trademark of UNIX System Laboratories, Inc.