UNIX Security Tools

Compiled by
Geoff Morrison
Division of Information Technology
for the
CSIRO Review of Computer Network Security

November 1993

CSIRO
AUSTRALIA

Table of Contents

1.0 Introduction 1

1.1 General 1
1.2 Intended Audience 1

2.0 Systems Security Tools 2

2.1 Npasswd 2
2.2 ANLpasswd 2
2.3 Passwd+ 3
2.4 COPS 3
2.5 Chkacct 4
2.6 Crack 4
2.7 Tripwire 5
2.8 Wuarchive ftpd 5
2.9 ISS - Internet Security Scanner 6
2.10 Local COPS 7

3.0 Network Security Tools 8

3.1 Tcp Wrapper (aka log_tcp) 8
3.2 Portmapper 8
3.3 SOCKS Library and sockd 9
3.4 Tcpdump 10
3.5 Etherfind 10
3.6 Etherfind decoder 10
3.7 Netstat 11
3.8 Texas A&M Network Security Package (tamu) 11
3.9 TIS Firewall Toolkit 12

4.0 Other Useful Tools/Techniques 13

4.1 Top 13
4.2 Routing Tables 13
4.3 Packet Filtering 13
4.4 Nfswatch 14
4.5 Ethertop 14
4.6 Gated 14
4.7 Xtr 14
4.8 Etherman, Interman, Packetman (Network Monitoring and Visualisation Tools) 14

5.0 Miscellaneous **16**
5.1 Kerberos 16
5.2 UCSF System Manager's Toolkit 16
5.3 Securelib - Kernel Wrap for SunOS via Shared Libraries 17
5.4 Swatch 17
5.5 CrackLib 17
5.6 Shadow Password Implementation 17
5.7 Obvious Password Detector 18
5.8 Data Encryption Standard Software 18

6.0 Summary **20**

Annex A Obtaining Tools **22**
A.1 Anonymous FTP 22
A.2 Finding Software - ARCHIE 24
A.3 UUNET 26
A.4 Berkeley 27
A.5 SlMTEL-20 27
A.6 SUN-SPOTS 27
A.7 comp.sources 27
A.8 Vendors 28
A.8.1 Sun Microsystems 28
A.8.2 Digital Equipment Corporation 28
A.8.3 Hewlett-Packard 28

Annex B References **29**
B.1 Books 29
B.2 Papers 30
B.3 Mailing Lists 31
B.4 Usenet Newsgroups 32

UNIX Security Tools

Compiled by
Geoff Morrison
Computing Infrastructure Manager
CSIRO Division of Information Technology
Canberra ACT
Geoff.Morrison@csis.dit.csiro.au

1.0 Introduction

1.1 General

A wealth of software has been developed for improving the security of UNIX systems. Much of this software has been developed at universities and other public institutions, and is freely available. This paper describes some of the more important programs available and how to obtain this software.

Wherever possible I have tried to provide a reference to the site of the original distribution as well as an Australian host site. Additional sources may be located by using *Archie* (Section A.2 on page 24).

The packages described require time to configure and install, and considerably more time to fully understand their strengths and weaknesses. There is no quick and easy answer to effectively maintain security.

If I have missed your favourite utility or there are more recent versions available please email me at the above address.

1.2 Intended Audience

This paper is technical in nature and as such is intended as a reference for UNIX System Managers.

2.0 Systems Security Tools

This section describes tools that are applied to host systems, this is where you are potentially at the greatest risk and includes workstations, file servers, data bases and other network services. This is also the point at which the user community sits at their desks and use the network.

2.1 Npasswd

The npasswd command, developed by Clyde Hoover at the University of Texas at Austin, is intended to be a replacement for the standard UNIX passwd command, as well as the SUN yppasswd command. The npasswd program makes passwords more secure by refusing to allow users to select insecure passwords. npasswd will work with NIS and C2 security.

The following capabilities are provided by npasswd:

- Configurable minimum password length
- Configurable to force users to use mixed case or digits and punctuation
- Checking for “simple” passwords such as a repeated letter
- Checking against the host name and other host-specific information
- Checking against the login name, first and last names, and so on
- Checking for words in various dictionaries, including the system dictionary.

Available from:

ftp.cc.utexas.edu	pub/npasswd

Recommended.

2.2 ANLpasswd

While other programs check for bad passwords after the fact, it is important to have good passwords at all times, not just after the latest Crack (Section 2.6 on page 4) run. To this end the Argonne National Laboratory have modified Larry Wall's Perl password program (perl-passwd2) and added;

- "ypsmarts" so it will work with NIS
- allows for gecos changes
- checks a sorted list of all "bad passwords".

The list of "bad passwords" are ALL the words that Crack will generate given all the dictionaries that they have been able to collect (approx. 107 Mb). The combination of improvements has turned publicly available code into a powerful tool that can aid sites in the maintenance of local security.

It currently runs on;
SUN, IBM, NeXt, SGI, Intel, Alliant, Encore, BBN, Solbourne, Sequent.

Current Version:	2.0
Available from:	
info.mcs.anl.gov	pub/systems/anlpasswd.tar.Z
ftp.uu.net	pub/security/anlpasswd-2.0.tar.Z

2.3 Passwd+

This proactive password program replacement suite written by Matt Bishop allows a system manager to enforce policies for selecting passwords. It replaces passwd, chfn, chsh. It is rule-based, easily configurable, prevents users from selecting weak passwords and provides logging information via syslog.

It does not work with NIS or C2 secured systems.

Available from:

dartmouth.edu	pub/security/passwd+.tar.Z
ftp.uu.net	pub/security/passwd+.tar.Z
archie.au	security/dartmouth/passwd+.tar.Z

2.4 COPS

The COPS (Computer Oracle and Password System) package (Farmer and Spafford, 1990), developed by Dan Farmer of Sun Microsystems, is a security tool for system administrators that checks for numerous common security problems on UNIX systems. A collection of shell scripts and C programs (a new version uses PERL instead of C), COPS can be easily run on almost any UNIX variant.

Among other things, it checks the following items and sends the results to the system administrator:

- Checks */dev/kmem* and other devices for world read/writability
- Checks special/important files and directories for "bad" modes (world-writable, etc.)
- Checks for easily-guessed passwords
- Checks for duplicate user ids, invalid fields in the password file, etc.
- Checks for duplicate group ids, invalid fields in the group file, etc.
- Checks all users' home directories and their .cshrc, .login, profile, and .rhosts files for security problems
- Checks all commands in the */etc/rc* files and cron files for world-writability
- Checks for bad root search paths, NFS file systems exported to the world, etc.

Includes an expert system that checks to see if a given user (usually root) can be compromised, given that certain conditions exist.

Checks for changes in the set-user-id (SUID) status of programs on the system.

Current Version	1.04
Available from:	
cert.sei.cmu.edu	pub/tools/cops/1.04
archie.au	security/cert/tools/cops/1.04

It is also distributed periodically via the *comp.sources.unix* USENET newsgroup.

Note:
Sometimes the output from the COPS package can be misleading - YOU must be able to interpret the output to know what is correct for YOUR system

Recommended.

2.5 Chkacct

Chkacct is a COPS for the ordinary user. This tool is made available to the users to run, or it is run for them once per day. It will do an integrity check on the status of files in their own account and then mail them the results (such as "Dear user: Your *.rhosts* file is unsafe"). This package can help make your users more aware of security controls and raise their level of participation in the program.

Available from:

Chkacct is distributed with the COPS package.

ftp.cs.purdue.edu	pub/pcert/tools/chkacct.tar.Z

2.6 Crack

The crack program is a password cracking utility developed by Alec David Muffett of the University College of Wales. It comes with a fast version of the UNIX password encryption function, called *fcrypt*; this function is approximately 13 times faster than the standard UNIX *crypt* function. It also includes the ability to use multiple systems to parallelise the cracking. The general procedure used by crack is to first base guesses on the contents of the GECOS field, and then to use several preprocessed dictionaries. Additional dictionaries may be added.

Current Version	4.1
Available from:	
cert.sei.cmu.edu	pub/tools/crack
archie.au	security/cert/tools/crack

Additional dictionaries (Australian, Danish, Dutch, English, Finnish, French, German, Italian, Japanese, misc., names, Norwegian, Swedish) may be found on various other sites;

e.g. ftp.cs.purdue.edu	pub/pcert/dict
ftp.uu.net	doc/dictionaries

Note:
For crack to be really effective you should add additional dictionaries. Unfortunately giv-

ing crack a 26 Mbyte dictionary file, a full rule-set, testing against a password file of 115 users, running on a SUN SPARCstation 10/30, 24 hours a day, it ran for 27 days before going into limbo and having to be killed. During this time it cracked three passwords, but in the interim those users had changed their password!
The approach I recommend is to install a pro-active password program (npasswd or ANL-passwd) and use crack with the minimum set of dictionaries that you feel comfortable with (or have the processing power to effectively use).

2.7 Tripwire

Tripwire is an integrity monitor for UNIX systems. It uses several checksum/signature routines to detect changes to files, as well as monitoring selected items of system-maintained information. The system also monitors for changes in permissions, links and sizes of files and directories. It can be made to detect additions or deletions of files from watched directories.

The configuration of Tripwire is such that the system/security administrator can easily specify files and directories to be monitored or to be excluded from monitoring and to specify files which are allowed limited changes without generating a warning. Tripwire can also be configured with customised signature routines for site-specific checks.

Tripwire once installed on a "clean" system, can detect changes from intruder activity, unauthorised modification of files to introduce back-door or logic-bomb code, virus activity in a UNIX environment.

Current Version:	1.0.4
Available from:	
ftp.cs.purdue.edu	pub/spaf/COAST/Tripwire
cert.sei.cmu.edu	pub/tools/tripwire

There is a mailing list in support of this package, send mail to:
tripwire-request@cs.purdue.edu

with a body message consisting solely of the word *help*. The mail server will respond with instructions on how to get sources, patches, and how to join the mailing list.

Recommended.

2.8 Wuarchive ftpd

The wuarchive-ftpd is a modified FTP server. It was modified by Chris Myers of Washington University in September 1991. On SUN systems (SunOS) it is a replacement for */usr/etc/in.ftpd* and all of the features are incremental so it does everything in.ftpd does and more. In this respect it is completely compatible with the existing FTP clients.

Many of the features are not directly useful to the FTP user but provide improved capabilities for the system administrator including;

- Logging of file transfers inbound and/or outbound
- Access control for particular users, hosts, domains, time of day and number of simultaneous users
- User classification where users can be specified using a combination of users' types and addresses
- Informational messages can be displayed when a user cds into a directory to inform them about the nature of the contents of the directory
- Archiving and compression with tar and compress can be performed on-the-fly.

Available from:

wuarchive.wustl.edu	packages/wuarchive-ftpd
munnari.oz.au	pub/net/wu-ftpd-2.0.tar.Z

Note:
Ensure that the version is dated after 8 April 1993. See CERT advisory CA-93:06.

Recommended.

2.9 ISS - Internet Security Scanner

The Internet Security Scanner is a system that allows automated scanning of TCP/IP networked computers for security vulnerabilities. The software package, will interrogate all computers within a specified IP address range, determining the security posture of each with respect to several common system vulnerabilities. ISS does not attempt to gain access to a system being tested but is designed to provide the administrator with the information to fix obvious security misconfigurations.

The following vulnerabilities are currently tested for by ISS:

- Passwords on default accounts "guest", "bbs", "lp"
- Mail aliases "decode", "uudecode"
- Sendmail "wiz" and "debug" commands
- Anonymous FTP (see CERT Advisory CA-93:10)
- NIS (see CERT Advisory CA-92:13)
- NFS partitions world mountable
- rusers
- rexd.

Available from:

ftp.uu.net	usenet/comp.sources.misc/volume39/iss/part01.Z
archie.au	usenet/comp.sources.misc/volume39/iss/part01.Z

Reference:
CERT advisory CA-93:14.

Recommended.

2.10 Local COPS

Developed by Geoff Morrison and Peter Nikitser of CSIRO/DIT. This is a suite of scripts designed to overcome some of the (perceived) deficiencies of the current version of COPS. This package is customised for the DIT Canberra Laboratory and it assumes that the systems (workstations) are running tcp_wrappers (Section 3.1 on page 8) and the wuarchive in.ftpd (Section 2.8 on page 5). It is available for a heterogenous network of workstations (SUN, DEC and SGI) or a stand-alone system (e.g. UNIBIS). The system is designed to be run via "cron" and mail to "root" differences between yesterdays and todays syslog files, thus minimising the amount of data presented to the systems administrator. The basic design premise is that "no one has the time to read log files on a daily basis" so this presents to the administrator the daily differences in the system logs.

It currently checks:

- ftp transfer activity
- tcp connections (rshd, rlogind, telnetd, tftpd...)
- last login on all workstations
- current directory in "roots" path *(csh/sh)*
- changes to "roots" umask value
- cron usage
- modifications to important system files
  passwd, group, netgroup, login, sum, all NIS managed files
- bad su
- repeated login failures
- presence and content of *$HOME/.rhosts* files

The system is quite extensible, so that any facility may be monitored. In some ways it is a "poor-man's tripwire". It is certainly not designed to replace either tripwire or COPS.

3.0 Network Security Tools

The tools in this section relate to the physical network or "looking at what is happening on the wire" and are more "monitoring" in nature.

3.1 Tcp Wrapper (aka log_tcp)

The tcpd program can be setup to monitor incoming requests for telnet, finger, ftp, exec, rsh, rlogin, tcpd, talk, spray, rusers, comstat and other services that have a one-to-one mapping onto executable files.

Optional features are:

- Access control based on pattern matching
- Remote username lookups with the RFC 931 protocol
- Protection against hosts that pretend to have someone elses host name.

Connections that are monitored by tcpd are reported through the syslog facility. Each record contains a time stamp, the remote host name and the name of the service requested. The information can be useful to detect unwanted activities, especially when logfile information from several hosts is merged.

TCP/IP daemon wrapper programs are not a substitute for *packet filtering* (Section 4.3 on page 13). They are an excellent tool to use until packet filtering is available. The additional syslog information can provide an early warning method of intrusion detection. An example would be numerous finger connections from one site in a short period of time.

Available from:

cert.sei.cmu.edu	pub/tools/tcp_wrappers
ftp.win.tue.nl	pub/security/tcp_wrappers_6.0.shar.Z
archie.au	security/cert/tools/tcp_wrappers
	security/eindhoven/tcp_wrappers_6.0.shar.Z

Recommended.

3.2 Portmapper

A *portmapper* replacement with access control in the style of the tcp wrapper (Section 3.1 on page 8) package. It provides a simple mechanism to discourage access to the NIS (YP), NFS, and other services registered with the portmapper.

In some cases, better or equivalent alternatives are available:
The SunOS portmap that is provided with *patch id 100482-04* should close the same security holes. In addition, it provides NIS daemons with their own access control lists. This is better than just portmapper access control.

The securelib shared library (Section 5.3 on page 17) implements access control for all kinds of (RPC) services, not just the portmapper.

Reportedly, Irix 4.0.x already has a secured portmapper. However, many vendors still ship portmap implementations that allow anyone to read or modify its tables and that will happily forward any request so that it appears to come from the local system.

Features:

- Optional host access control. The local host is always considered authorized. This feature requires the *libwrap.a* library that comes with recent tcp wrapper implementations.
- Requests to change the portmap tables are accepted only when they come from the local system.
- Optional requests to (un)register services on privileged ports (port < 1024) are accepted only when they come from a privileged port. This feature is optional because some RPC implementations still run all RPC daemons of an unprivileged port.
- Requests that are forwarded by the portmapper will be forwarded through an unprivileged port.
- The portmapper refuses to forward requests to rpc daemons that do (or should) verify the origin of the request: at present, the list includes most of the calls to the NFS mountd/nfsd daemons and the NIS daemons.

Restrictions:

Limiting access to the portmapper does not protect you from direct attacks on the rpc daemons; the main task of portmap is to maintain a table of available RPC services and the network ports that they are listening on. The securelib can be used to protect individual RPC daemons, and the latest SunOS portmap+NIS fix already protects the NIS daemons and implements limited forwarding.

On the other hand, even though a portmapper with access control only makes an attack more difficult, it still provides an excellent early warning system.

Available from:

ftp.win.tue.nl	pub/security/portmap.shar.Z
archie.au	security/eindhoven/portmap.shar.Z

3.3 SOCKS Library and sockd

The sockd and SOCKS Library (Ying-Da Lee - original version by David and Michelle Koblas) provide another way to implement a "TCP Wrapper". It is not intended to make the system it runs on secure, but rather to centralise ("firewall") all external internet services. The sockd process is started by inetd whenever a connection is requested for certain services (finger, whois, ftp, telnet, xgopher) and then only allows connections from approved hosts (listed in a configuration file). The sockd also will log information about the connection.

Available from:

ftp.inoc.dl.nec.com	pub/security/socks.cstc.4.0.tar.gz
ftp.uu.net	pub/security/socks.tar.Z
archie.au	security/misc/socks

3.4 Tcpdump

The tcpdump packet monitoring program prints the headers of packets on the ethernet that match a boolean expression. If no expression is given, all packets on the net will be dumped.

e.g. # tcpdump net *some-network-address*

will print all traffic between local hosts and hosts at the specified address.

tcpdump -x -q dst host *hostname* and dst port telnet

will print all packets destined for the telnet port on host *hostname*!

Available from:

ftp.ee.lbl.gov	tcpdump-2.2.1.tar.Z
munnari.oz.au	pub/net/tcpdump-2.2.1.tar.Z

Recommended.

3.5 Etherfind

Etherfind prints out information about packets on the ethernet that match a boolean expression.

e.g. # etherfind host hellsparc

will print all traffic either to or from the host "hellsparc"

Available from:

Included as part of Operating System (SunOS 4.1.x, Ultrix 4.x)

% man etherfind

3.6 Etherfind decoder

Unfortunately, most network monitors (e.g. etherfind, tcpdump, netstat) are not really designed for monitoring a network under attack, and so you have to capture more data than you need, and then sift through it manually. This is a time consuming procedure, but it is arguably better than nothing.

An etherfind decoder developed by Peter Campbell from the CSIRO Division of Fisheries in Hobart, is designed to take the output of etherfind monitoring and put it into a readable "human" form.

3.7 Netstat

You can use the netstat command to list all of the active and pending TCP/IP connections between your machine and every other machine on the Internet. This is very important if you suspect that somebody is breaking into your computer or using your computer to break into another one. netstat lets you see which machines your machine is talking to. The commands output includes the host and port number of each end of the connection, as well as the number of bytes in the receive and transmit queues. If a port has a name assigned in the */etc/services* file, netstat will print it instead of the port number.

Available from:

Included as part of Operating System (SunOS 4.1.x, Ultrix 4.x)
% man netstat

3.8 Texas A&M Network Security Package (tamu)

In August 1992, Texas A&M University UNIX computers came under extensive attack from a coordinated group of Internet crackers. This package of security tools represents the results of over seven months of development and testing of the software that they have been using to protect approx 12,000 Internet connected devices. The package includes three coordinated sets of tools;

- drawbridge
  An extremely powerful bridging filtering package
- tiger
  A set of convenient yet thorough machine checking programs
- netlog
  A set of intrusion detection network monitoring programs.

Current Version:	Beta Release
Available from:	
net.tamu.edu	pub/security/TAMU

Looks VERY interesting!

3.9 TIS Firewall Toolkit

The Trusted Information Systems (TIS) Toolkit is a software kit for building and maintaining internetwork firewalls. Included with the kit are complete sources for FTP, rlogin and telnet application proxies, user authentication management, compartmented SMTP and logging/log reduction. Components of the toolkit, while designed to work together, can be used in isolation or can be combined with other firewall components.

TIS maintains the electronic users group *fwall-users@tis.com* for discussion of the toolkit. To join, send email to *fwall-users- request@tis.com*.

Available from:

ftp.tis.com	pub/firewalls/toolkit

Note:
Worthy of a look just for the documentation on *firewall* construction.

4.0 Other Useful Tools/Techniques

4.1 Top

Top displays the top 10 (or user defined) processes on a system and periodically updates this information. Raw cpu percentage is used to rank processes. This is not specifically a security related package but it is an extremely useful tool to see where and by whom your cpu is being used.

Available from:

eecs.nwu.edu	pub/top/top-3.2.tar.Z

4.2 Routing Tables

One of the simplest approaches to preventing unwanted network connections is to simply remove certain networks from a gateway's routing tables. This makes it impossible (or nearly impossible) for a host to send packets to those networks. Most protocols require bi-directional packet flow even for unidirectional data flow; thus breaking one side of the route is usually sufficient.

This approach is commonly taken in firewall systems, by preventing the firewall from advertising local routes to the outside world.

Manual manipulation of a hosts routing tables can cause return packets to "get lost". If *dynamic* routing is not required than *static* routing may be configured with specific routes to wanted hosts/networks. Obviously this technique is only feasible if access to a specific host is limited to a few known networks but combined with the tcp_wrapper software can be a very useful technique.

Further information:

```
% man routed
```

4.3 Packet Filtering

Many commercially available gateway systems (more commonly called routers) provide the ability to filter packets based not only on sources and destinations but also on source-destination combinations. This mechanism can be used to deny access to a specific host, network, or subnet from any other host, network or subnet.

Gateway systems from Cisco Systems support an even more complex scheme, allowing finer control over source and destination addresses. Via the use of address masks, one can deny access to all but one host on a particular network. The Cisco systems also allow packet filtering based on IP protocol type and TCP or UDP port numbers.

Recommended.

4.4 Nfswatch

The nfswatch program, developed by the David Curry of SRI, monitors all NFS packets by host, network, or file system. This is not specifically a security related package but it is an extremely useful tool to see where NFS traffic is coming from/going to and which filesystem it is accessing.

Available from:

harbor.ecn.purdue.edu	pub/davy/nfswatch4.0.tar.Z
ftp.erg.sri.com	pub/software
icarus.riacs.edu	pub/programs/nfswatch.tar.Z
ftp.adelaide.edu.au	pub/4.3/nfswatch4.0.tar.Z

Recommended.

4.5 Ethertop

Ethertop is a program which displays network usage in the same form as top (above) and is intended for quick diagnosis of network problems e.g. who is accessing the file server.

Available from:

archie.au	usenet/comp.sources.unix/volume25

4.6 Gated

The gated program, which has a more configurable implementation of the Routing Information Protocol (RIP). The current gated implementation also contains support for the HELLO, BGP, and OSPF routing protocols.

Available from:

gated.cornell.edu	pub/gated
munnari.oz.au	pub/net/gated-R3_0_1.tar.Z

4.7 Xtr

Xtr is an X front to Suns' rpc.etherd network monitor (/bin/traffic). Again, not strictly a security tool it is very useful to be able to see from whom and where traffic on the local network is coming from.

Available from:

ftp.uu.net	usenet/comp.sources.x/volume12
archie.au	usenet/comp.sources.x/volume12

4.8 Etherman, Interman, Packetman (Network Monitoring and Visualisation Tools)

These tools may be used to monitor and "display" network communications. Two of the tools provide a real-time picture of network communications. These tools are designed to allow network managers to passively monitor a network and diagnose common network problems as quickly and efficiently as possible.

- Etherman
  An X11 based tool which displays a representation of real-time Ethernet communications. Network data is promiscuously received via a system "network tap" and summarised into useful statistics. These statistics are displayed in a graphical manner, as to allow both experienced network managers and novices an insight as to how a network is being used. Etherman will also provide protocol summaries, usage statistics and postscript snapshots of network activity.
- Interman
  Focuses on IP connectivity within a single segment. As with Etherman, this tool allows a real-time representation of network communications to be displayed. Interman employs the same methods of network data capture as Etherman, except only IP traffic is considered. Since IP is a network-level protocol, Interman will display multiple networks - both local and remote. Protocol summaries, usage statistics and postscript snapshots are also available.
- Packetman
  A retrospective Ethernet packet analyser. This tool allows the capture and analysis of an Ethernet packet trace.

Available from:

At present, only binaries for SUN Sparc (SunOS 4.1.x) and DEC-mips (ULTRIX 4.2a and above) are available.

ftp.cs.curtin.edu.au pub/netman/sun4c|dec-mips/[etherman|interman|-packetman].tar.Z

you will also need:

pub/netman/hershey-[sun4c|dec-mips].tar.Z

5.0 Miscellaneous

The packages in this section are unknowns, if you have tried these systems or can provide any additional information please contact the author.

5.1 Kerberos

Kerberos is a DES-based encryption scheme that encrypts sensitive information, such as passwords, sent via the network from client software to the server daemon process. The network services will automatically make requests to the Kerberos server for permission "tickets". You need the source to your client/server programs so that you can use the Kerberos libraries to build new applications. Since Kerberos tickets are cached locally in */tmp*, if there is more than one user on a given workstation, then a possibility for a collision exists. Kerberos also relies upon the system time to operate, therefore it should be enhanced in the future to include a secure time server (timed is not appropriate).

The Kerberos package, developed by the Massachusetts Institute of Technology's Project Athena is available for anonymous FTP from the host *athena-dist.mit.edu* in the directory *pub/kerberos*. The other software developed by Project Athena, as well as various conference papers describing the project and its software, are available from this host as well.

5.2 UCSF System Manager's Toolkit

The UCSF System Manager's Toolkit (SMT), developed at the University of California, is a collection of software to automate routine administrative functions on a network of UNIX machines. It includes software to manage accounting, security audits, unattended file system backups, file system clean-up, user account installation and deletion, as well as other major components. It was developed on SUN systems, and should work with only minor modification on other Berkeley-based systems. System V systems are not supported.

The SMT is available for a modest license fee (?). For more information, contact:

Claire LeDonne, Manager
Campus Software Office
2320 Shattuck Avenue, Suite B
Berkeley, CA 94704

(415)643-7201
ledonne@garnet.berkeley.edu

Note:
The author has tried to obtain additional information on this package but has yet been unsuccessful.

5.3 Securelib - Kernel Wrap for SunOS via Shared Libraries

This is a wrapper for SunOS daemons that use RPC (Remote Procedure Calls), such as portmap, ypserv, ypbind, ypupdated, mountd, pwdauthd etc. To utilise this, you must have SunOS 4.1 or higher and must have the capability to rebuild your shared libraries. Essentially, you modify the function calls that the kernel uses to establish RPC connections, such as *accept(), recvfrom() and recvmsg()*. Since these calls are maintained in the shared libraries, you have access to modify them without rewriting the kernel.

Available from:

eecs.nwu.edu	pub/securelib.tar
archie.au	security/eindhoven/securelib.tar.Z

5.4 Swatch

Swatch (Stephen E. Hansen and E. Todd Atkins) is really two things, it is a program used to parse through the myriad of log data generated by the various security programs, in particular syslog. But it's more than that. It is fully configurable with triggers (actions), so that while it is continuously monitoring the log in real-time, it can take actions based upon high-priority events that you tell it to watch for. To get full use of this, you will need to modify your network service daemons such as ftpd and telnetd so that enhanced logging is added to syslog, to feed swatch.

Available from:

sierra.stanford.edu	pub/sources/swatch-1.8.6.tar.Z
ftp.cs.purdue.edu	pub/pcert/tools/unix/swatch-1.8.2.tar.Z

5.5 CrackLib

CrackLib is a library containing a number of C functions which may be used in a "passwd"-like program. The basic idea is to try and prevent users from choosing passwords that could be guessed by crack by filtering them out at the source.

Note:
CrackLib is NOT a replacement passwd program. CrackLib is a LIBRARY that enables YOU to write such as replacement.

Available from:

cert.sei.cmu.edu	pub/tools/cracklib
archie.au	security/eindhoven/cracklib.tar.Z

5.6 Shadow Password Implementation

John F. Haugh has written a set of routines to implement shadow password files and password aging. The distribution also includes replacement versions of login, passwd, and sin, a program to be run when booting in single-user mode to prompt for the root password before invoking a shell, and several other utilities. Version 3 of the distribution was posted in Volume 26 of the *comp.sources.misc* newsgroup in November 1991 and is available from the *comp.sources* archive sites.

Available from:

ftp.uu.net	pub/security/shadow-3.1.4.tar.Z
archie.au	usenet/comp.sources.misc/volume26

5.7 Obvious Password Detector

John Nagle of Stanford University has developed a library routine that can be used to detect "obvious" passwords by searching for English language triples (such as "ing," "the", and so on). Although a complete password changing program is not included in the distribution, the routine may still prove useful as a tool to allow users to verify that their password choices are secure. The software was posted in Volume 16 of the *comp.sources.unix* newsgroup in November 1988 and is available from the *comp.sources* archive sites *(archie.au:/usenet/*).*

5.8 Data Encryption Standard Software

Several implementations of the Data Encryption Standard (DES), are available from sites on the Internet. Many UNIX vendors include implementations of DES with their products, at least in the United States. Current U.S. export restrictions prevent the distribution of DES software outside the United States.

Phil Karn, author of the popular KA9Q implementation of TCP/IP for packet radio and personal computers, offers a freely distributable implementation of DES as part of this package. It is available for anonymous FTP from *ucsd.edu* in the file */hamradio/packet/tcpip/crypto/des.tar* (ftp.adelaide.edu.au:/pub/ka9q/crypto/des.tar.Z)

Dave Barrett of the University of Colorado at Boulder has written a fast DES-compatible encipherment program, along with material to send enciphered material through electronic mail. It is available for anonymous FTP from the host *ftp.uu.net* in the file */pub/fast-des.shar.S*.

To counter the U.S. export restrictions, Antti Louko of the Helsinki University of Technology in Finland has created an implementation of DES suitable for use with Kerberos. Because this implementation was not created in the U.S., the export restrictions do not apply. This implementation was posted in Volume 18 of the *comp.sources.unix* newsgroup in March 1989, and may be obtained from any of the *comp.sources* archive sites. It is also available for anonymous FTP from the site *kampi.hut.fi* in */alo/des-dist.tar.Z* (archie.au:/usenet/comp.sources.unix/volume18/des-no-usa).

A public domain implementation of DES suitable for use with Kerberos has been written by Eric Young of Bond University in Queensland. It is available for anonymous FTP from the host *gondwana.ecr.mu.oz.au* in the file */pub/athena/eBones-p9-des.tar*.Z. He has a newer version in the works which can be retrieved from *ftp.psy.uq.oz.au* in the file */pub/DES/libdes.tar.93-06-29.Z.*

The next version of Berkeley UNIX (following 4.3 Reno) will probably have a copyrighted but freely available implementation of DES.

There are several other versions of DES available, but many of them are designed explicitly for speed, for use in research on password crackers and the like. These versions are not typically available via anonymous sources, and must be obtained from the authors.

6.0 Summary

The large amount of software development on the Internet as a whole has made it possible to find a program for almost any purpose. Several pieces of software have been developed that can help you increase the security of your system; it is important that you investigate the distribution sources of these programs.

One caution about obtaining software from the Internet bears mentioning, however. It is important to realize that most of the software out there is offered on an as-is basis, and that there are unethical people who will create versions of these programs that contain viruses, Trojan horses, or other problems. Before installing and executing any program obtained from the network, either via anonymous FTP or from one of the source newsgroups, carefully examine the code to be sure it does only what you expect it to, and try and obtain it from the original site.

Use a combination of tools, DO NOT place your faith in one tool alone, they should be used to compliment each other.

TABLE 1. Summary - UNIX Security Tools

Name	Classification	Comments
ANLpasswd	passwd replacement	Recommended
Chkacct	"User" integrity check	Part of COPS
COPS	System integrity check	Recommended
Crack	Weak password detection program	Use with a pro-active passwd program
CrackLib	Write your own passwd program	
Data Encryption Standard Software	Public Domain DES implementations	
Drawbridge	Packet bridging/filtering software (PC based)	See Texas A&M, Recommended
Etherfind	Ethernet packet monitoring	Included in Operating System
Etherfind decoder	etherfind packet decoder	
Etherman	Network monitoring and visualisation tool	
Ethertop	Network usage analyser/monitor	
Gated	routed replacement ("dynamic" routing)	
Interman	Network monitoring and visualisation tool	
Internet Security Scanner (ISS)	System vulnerability checker	Recommended
Kerberos	Authentication system	
Kernel Wrap for SunOS	Daemon wrapper for RPC calls	
Local COPS	Scan and summarise syslog files	

TABLE 1. Summary - UNIX Security Tools

Name	Classification	Comments
Log TCP	Monitor and log tcp requests	See Tcp Wrappers
Netlog	Intrusion detection, network monitoring	See Texas A&M, Recommended
Netstat	Monitor TCP/IP port connections	Included in Operating System
Nfswatch	NFS traffic analyser/monitor	
Npasswd	passwd/yppasswd replacement	Recommended
Obvious Password Detector	Write your own passwd program	
Packet Filtering	"Router" operation (e.g. Cisco)	Recommended
Packetman	Network monitoring and visualisation tool	
Passwd+	passwd replacement	
Portmapper	Tcp wrapper for portmapper	Apply SunOS patch 100482
Routing Tables	Manipulate "static" routes	
Securelib	Daemon wrapper for RPC calls	See Kernel Wrap for SunOS
Socks Library & sockd	Proxy (logging) server daemon	Similar to tcp_wrappers
Shadow Password	Implement shadow password and password aging	
Swatch	Scan syslog files	Appears similar to "Local COPS"
Tcpdump	Ethernet packet monitoring/analysis	Recommended
Tcp Wrappers (log_tcp)	Monitor and log tcp requests	Recommended
Texas A&M Network Security Package (tamu)	Comprehensive security system	See "drawbridge, tiger, netlog", Recommended
Tiger	Machine checking programs	See Texas A&M, Recommended
TIS Firewall Toolkit	Tools for building Internet firewalls (proxy agents)	
Top	Interactive "ps"	
Tripwire	System integrity monitor	Recommended
UCSF System Managers Toolkit	System Administration tools	
Wuarchive ftpd	Logging ftp daemon	Recommended
Xtr	Network monitoring tool	

Annex A Obtaining Tools

A.1 Anonymous FTP

Several sites on the Internet maintain large repositories of public-domain and freely distributable software, and make this material available for “anonymous” FTP. A host which allows anonymous FTP allows anyone to connect to the host using the login *anonymous*, and transfer files from a restricted directory. A sample anonymous FTP session is shown below.

```
geoff@lyra% ftp ftp.uu.net
Connected to ftp.uu.net.
220 ftp.UU.NET FTP server (Version 2.0WU(13) Fri Apr 9 20:44:32 EDT 1993) ready.
Name (ftp.uu.net:geoff):    anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:                   enter your complete email address, yourname@site.csiro.au here
230-
230-            Welcome to the UUNET archive.
230-   A service of UUNET Technologies Inc, Falls Church, Virginia
230-   For information about UUNET, call +1 703 204 8000, or see the files
230-   in /uunet-info
230-
230-   Access is allowed all day. Local time is Mon Aug 9 23:11:51 1993.
230-
230-   All transfers are logged with your host name and email address.
230-   If you don't like this policy, disconnect now!
230-
230-   If your FTP client crashes or hangs shortly after login, try using a
230-   dash (-) as the first character of your password. This will turn off
230-   the informational messages which may be confusing your ftp client.
230-
230-Please read the file /info/README.ftp
230- it was last modified on Mon Jan 18 13:53:56 1993 - 203 days ago
230-Please read the file /info/README
230- it was last modified on Wed Aug 5 21:10:26 1992 - 368 days ago
230 Guest login ok, access restrictions apply.
ftp> cd vendor/sun/sun-fixes
250 CWD command successful.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 2784

-rw-r--r--   1   76   120      4566   Nov   18   1991   README
-rw-r--r--   1   76   120    484687   Dec   14   1988   ddn.tar.Z
-rw-r--r--   1   76   120    140124   Jan   13   1989   gated.sun3.Z
-rw-r--r--   1   76   120     22646   Dec   14   1988   in.ftpd.sun3.Z
-rw-r--r--   1   76   120     30463   Dec   14   1988   in.ftpd.sun4.Z
-rw-r--r--   1   76   120      1138   Jul    8   1989   lib.msg.Z
-rw-r--r--   1   76   120    252837   Jul    8   1989   libc_pic.a.sun3.Z
-rw-r--r--   1   76   120    246605   Jul    8   1989   libc_pic.a.sun4.Z
```

```
-rw-r--r--   1  76   120    245149  Jul   8  1989  libc_resolv.so.sun3.Z
-rw-r--r--   1  76   120    235129  Jul   8  1989  libc_resolv.so.sun4.Z
-rw-r--r--   1  76   120     17403  May  25  1989  rcp.sun3.Z
-rw-r--r--   1  76   120     20315  May  25  1989  rcp.sun4.Z
-rw-r--r--   1  76   120      6859  Feb   3  1989  rpc.yppasswdd.sun3.Z
-rw-r--r--   1  76   120      7779  Feb   3  1989  pc.yppasswdd.sun4.Z
-rw-r--r--   1  76   120    618703  Aug  21  1990  selection_svc.tar.Z
-rw-r--r--   1  76   120     86753  Aug  31  1989  sendmail.mx.sun3.Z
-rw-r--r--   1  76   120    110163  Aug  31  1989  sendmail.mx.sun4.Z
-rw-r--r--   1  76   120     72119  Aug  31  1989  sendmail.sun3.Z
-rw-r--r--   1  76   120     99147  Aug  31  1989  sendmail.sun4.Z
drwxr-sr-x   2  76   120      1024  Dec  22  1991  unofficial
-rw-r--r--   1  76   120      3673  Jul  11  1989  wall.sun3.Z
-rw-r--r--   1  76   120      4099  Jul  11  1989  wall.sun4.Z
-rw-r--r--   1  76   120      7955  Jan  18  1989  ypbind.sun3.Z
-rw-r--r--   1  76   120      9237  Jan  18  1989  ypbind.sun4.Z
226 Transfer complete.
1723 bytes received in 1.1 seconds (1.5 Kbytes/s)
ftp> type image
200 Type set to I.
ftp> get ypbind.sun4.Z
200 PORT command successful.
150 Opening BINARY mode data connection for ypbind.sun4.Z (9237 bytes).
226 Transfer complete.
local: ypbind.sun4.Z remote: ypbind.sun4.Z
9237 bytes received in 2.7 seconds (3.3 Kbytes/s)
ftp> bye
221 Goodbye.
geoff@lyra%
```

After connecting to the host, log in with the special login *anonymous*. As a password, enter your electronic mail address. The *cd* command can be used to change directories; most sites place their distributions in a subdirectory called *pub*. The *dir* command lists the current directory. Many sites compress their distributions to conserve disk space; files which have been compressed have names which end in ".Z". These files must be transferred in "binary" mode to avoid corruption; the *type image* FTP command tells FTP to perform binary transfers instead of ASCIl transfers (ASCII files may usually be transferred in binary mode also, at least between systems of the same type). The *get* command copies a remote file to a local file of the same name. Finally, the *bye* command closes the connection. For more information on the use of FTP, consult the manual page for the ftp command on your system.

A.2 Finding Software - ARCHIE

Archie is a system that allows searching of indexes of what files are available on public servers on the Internet. It's the place you should start if you are searching for programs, data or text files. You ask it either to find filenames which contain a certain search string or suggest files whose description contains a certain word. It returns the actual filenames that meet the search criteria, and the name of the servers containing those files. Once you decide which of the files most likely meets your needs, you can easily move the file to your computer with anonymous FTP.

e.g.

```
geoff@lyra% telnet archie.au
Trying 139.130.4.6 ...
Connected to archie.au.
Escape character is '^]'.

            Welcome to Archie.AU (aka plaza.AARNet.EDU.AU)

Public access services provided on this machine are
      archie        The Archie System
      de            Directory Service
      netfind       Network Search Utility

Unauthorized access to any other account is prohibited.

Local time is 10:08AM on Wednesday, 11 August 1993

login: archie
Last login: Wed Aug 11 10:07:35 from maristb.marist.e
SunOS Release 4.1.3 (PLAZA) #11: Sun Aug 8 06:31:49 EST 1993

. . . . . . . . . .

# 'search' (type string) has the value 'regex'.
Archie.AU> set search sub
Archie.AU> prog diction

Host alice.fmi.uni-passau.de    (132.231.1.180)
Last updated 12:31 8 Aug 1993

   Location: /pub
     DIRECTORY    drwxrwxr-x 512 bytes 21:00 4 Jun 1992 dictionaries

Host alice.fmi.uni-passau.de    (132.231.1.180)
Last updated 12:31 8 Aug 1993

   Location: /pub/unix/misc
     FILE    -rw-rw-r-- 485521 bytes 21:00 3 Jun 1992 dictionaries.tar.Z

. . . . . . . . . .

Host binkley.cs.mcgill.ca    (132.206.51.9)
```

```
Last updated 08:47 28 Jul 1993

   Location: /hutch/pub
     DIRECTORY    drwxr-xr-x 512 bytes 13:21 24 Jun 1993 Dictionaries

Host ftp.cs.purdue.edu    (128.10.2.1)
Last updated 13:25 18 Jul 1993

   Location: /pub/ygz
     DIRECTORY    drwxrwxr-x 1024 bytes 05:14 29 Jun 1993 cxterm-dictionary

Host ftp.cs.purdue.edu    (128.10.2.1)
Last updated 13:25 18 Jul 1993

   Location: /pub/ygz/cxterm-dictionary
     FILE    -rw-r--r-- 3405 bytes 23:11 29 May 1993 00DICTIONARY.readme

Host ftp.uu.net    (192.48.96.9)
Last updated 13:41 19 Jul 1993

   Location: /doc/literary/obi/BSD/doc/usd
     DIRECTORY    drwxr-xr-x 512 bytes 00:00 27 Jul 1992 32.diction

Archie.AU> bye
# Bye.
Connection closed by foreign host.
geoff@lyra%
```

After *telneting* to the host *archie.au*, log in with the special login *archie*. The *set search* command is used to specify that the search string will match a filename that contains it as a substring, the case is ignored when doing the matching. The *prog searchstring* (diction) command is used to start a search for anything that contains the substring "diction" (looking for additional dictionaries for crack). After the search is complete, the server returns a list of servers and filenames that fit the search criteria. Finally, the *bye* command closes the connection. For more information on the use of *Archie*, consult the references at the end of this paper, or telnet to *archie.au* and type *help*.

A.3 UUNET

UUNET Communications Services, Inc. makes large volumes of software and other information available for anonymous FTP. Some of the directories which may be of interest;

- *networking/athena*
  The MIT Project Athena software distribution, including Kerberos.
- *systems/unix/bsd-sources*
  The sources to much of 4.3BSD, including most of the utility programs, and the TCP/IP networking code. If you want to make a modified version of a standard program such as login for your site, the sources here are often a good place to start.
- *usenet/comp.sources.**
  The USENET newsgroups *comp sources.** are all archived here. There are directories for several varieties of home computer and workstations, as well as more general directories such as *comp.sources.unix* and *comp.sources.misc*. The software in these directories is divided into volumes; indexes are contained in the top-level directories.
- *inet/ietf*
  Minutes of meetings of the various working groups of the Internet Engineering Task Force, which is responsible for adopting new Internet standard protocols. Working groups exist for almost any topic imaginable, including several on security-related subjects.
- *inet/internet-drafts*
  Copies of all Internet Drafts, which are the predecessors to Request for Comments. These documents specify proposed protocols and policies, and are available for public review and comment.
- *inet/rfc*
  Copies of all Internet Request for Comments documents, which specify the protocols and procedures used on the Internet. The protocol specifications for all "official" Internet services, including IP, TCP, UDP, SMTP, FTP, and TELNET are contained here. The file *rfc-index* contains an index to the documents.
- *vendor/sun/sun-dist*
  Official security-related patches from Sun Microsystems. Other patches (non-security-related) must be obtained through the normal Sun channels.
- *systems/unix/ucb-fixes*
  Official patches (both security-related and non-security-related) for 4.3BSD from the University of California at Berkeley.

The above list is only a small fraction of the material available from UUNET; the best way to find out what is available is to log in via FTP and browse around.

To connect to UUNET via anonymous FTP, contact the host *ftp.uu.net*. The file *Is-lR.Z* contains a complete list of files available and is updated daily.

Note:

You should check *archie.au* first before going to overseas archives as the response times will be faster.

A.4 Berkeley

The University of Califomia at Berkeley makes fixes available for anonymous FTP. These fixes pertain primarily to the current release of BSD UNIX (currently release 4.3-Reno). However, even if you are not running their software, these fixes are still important, since many vendors (Sun Microsystems, Digital Equipment, Hewlett Packard, etc.) base some or most of their software on the Berkeley releases.

The Berkeley fixes are available for anonymous FTP from the host *vangogh.cs.berkeley.edu* in the directory *4.3/ucb-fixes*. The file *INDEX* in this directory describes what each fix contains.

A.5 SlMTEL-20

The host *wsmr-simtel20.army.mil* is a TOPS-20 system operated by the U.S. Army at White Sands Missile Range, New Mexico. Its primary purpose is to make repositories of UNIX, MS-DOS, and Ada software available to the military organizations connected to the MILNET, although access is open to anyone, military or not.

The directory *PD6:<UNIX-C>* contains a large amount of UNIX software, primarily taken from the USENET *comp.sources* newsgroups. The file *000-MASTER-INDEX. TXT* contains a description of each file contained in the repository. The file *000-INTRO-UNIX-SW.TXT* contains information on the mailing list used to announce new software in the repository, and also contains detailed instructions for transferring the software with FTP. Because the TOPS-20 file formats differ from those of UNIX-systems, this file should be consulted before transferring any software.

A.6 SUN-SPOTS

The SUN-SPOTS mailing list, and the USENET newsgroup *comp.sys.sun* are used for discussing software and hardware issues associated with workstations from Sun Microsystems, Inc. A repository of software for Sun workstations, including security related software, is accessible for anonymous FTP from the host *relay.cs.toronto.edu.*

A.7 comp.sources

The USENET newsgroups *comp.sources.unix* and *comp.sources.misc* provide a wealth of UNIX software for every conceivable purpose. The sources posted to these groups are archived in several places around the Internet, including *archie.au*. A related group, *alt.sources*, also contains some useful software.

A.8 Vendors

Some UNIX vendors make bug fixes for their systems available over the Intemet. These fixes are announced through various channels.

A.8.1 Sun Microsystems

Security problems in Sun's operating system are reported through the *cert-advisory* mailing list, as well as via Sun's Customer Warning System.

Fixes for security-related bugs in Sun Microsystems' version of UNIX can be obtained via anonymous FTP from UUNET Communications Services (Section A.3 on page 26) in the directory *sun-dist*. Each file contains instructions for installing the fix, and files for all Sun architectures affected by the fix. The fixes usually apply only to Sun's most recent operating system releases.

SUN Microsystems in conjunction with the University of North Carolina operate an anonymous ftp and WAIS server at ***sunsite.unc.edu*** as an archive for public-domain software, shareware and technical documentation. The original *"sunflash"* notification about this site is available from *ftp.csis.dit.csiro.au* in *pub/sunsite.unc.edu.ANNOUNCE*.

A.8.2 Digital Equipment Corporation

Digital Equipment Corporation makes software for its version of UNIX, such as new versions of sendmail, available for anonymous FTP from the host ***gatekeeper.dec.com*** in the directory *pub/DEC*. These are unofficial distributions provided as a service by DEC's Western Research Laboratory.

For official patches to Ultrix, contact your Digital sales representative.

A.8.3 Hewlett-Packard

At the end of 1990, Hewlett-Packard announced that it would be making its support service available over the Internet for its customers with support contracts. Contact your sales representative for information on how to obtain this service.

Annex B References

B.1 Books

- How to Protect Your Data and Prevent Intruders: UNIX System Security
  Rik Farrow
  Addison-Wesley Publishing Company, 1991
- Managing NFS and NIS
  Hal Stern
  O'Reilly and Associates, Inc. 1991
- Practical UNIX Security
  Simon Garfinkel and Gene Spafford
  O'Reilly and Associates, Inc. 1992
- TCP/IP Network Administration
  Craig Hunt
  O'Reilly & Associates, Inc. 1992
- UNIX System Administration Handbook
  Evi Nemeth, Garth Snyder, Scott Seebass
  Prentice-Hall, 1989
- UNIX System Security
  Patrick H. Wood and Stephen G. Kochan
  Hayden Books, 1985
- UNIX System Security A Guide for Users and System Administrators
  David A. Curry
  Addison-Wesley Publishing Company, 1992
- X/Open Security Guide, 2nd Edition
  X/Open Company Limited, 1990
- The Whole Internet Users Guide & Catalog
  Ed Krol
  O'Reilly & Associates, Inc. 1992
- The Cuckoo's Egg
  Cliff Stoll
  Doubleday, 1989

B.2 Papers

The following papers are available via anonymous FTP from *ftp.csis.dit.csiro.au* in */pub/security/papers*.

- "Limitations of the Kerberos Authentication System"
  Steve Bellovin, Michael Merritt
- "Security Problems in the TCP/IP Protocol Suite"
  Steve Bellovin, AT&T Bell Laboratories
- "There Be Dragons"
  Steve Bellovin, AT&T Bell Laboratories, 1992
- "Coping with the Threat of Computer Security Incidents - A Primer from Prevention through Recovery"
  Russell L. Brand, 1990
- "Network (In)Security Through IP Packet Filtering"
  D. Brent Chapman, Great Circle Associates 1992
- "An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied"
  Bill Cheswick, AT&T Bell Laboratories, 1992
- "The Design of a Secure Internet Gateway"
  Bill Cheswick, AT&T Bell Laboratories, 1992
- "Improving the Security of Your UNIX System"
  David A. Curry, SRI International
- "A High-Speed Software DES Implementation"
  David C. Feldmeier
- "UNIX Password Security - Ten Years Later"
  David C. Feldmeier and Philip R. Karn
- "A Unix Network Protocol Security Study: Network Information Service"
  David K. Hess, David R. Safford, Udo W. Pooch, Texas A&M University
- "Hijacking AFS"
  P. Honeyman, L.B. Huston, M.T. Stolarchuk
- "Foiling the Cracker - A Survey of, and Improvements to, Password Security"
  Daniel V. Klein
- "A Weakness in the 4.2 BSD UNIX TCP/IP Software"
  Robert T. Morris, AT&T Bell Laboratories
- "Kerberos: An Authentication Service for Open Network Systems"
  Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller
- "A Network Firewall"
  Marcus J. Ranum, Digital Equipment Corporation
- "Thinking about Firewalls"
  Marcus J. Ranum, Trusted Information Systems, Inc., 1993

- "X Through the Firewall, and Other Application Relays"
  G. Winfield Treese and Alec Wolman, Digital Equipment Corporation
- Internet RFC Series
  1244 - Site Security Handbook
  1281 - Guidelines for the Secure Operation of the Internet
- Internet Security for UNIX System Administrators
  CERT Coordination Centre 1992
- CERT FAQ, Information Sheets and recommendations
- CISCO Security

B.3 Mailing Lists

- CERT-Advisory
  Mailing list for CERT-published (US -Computer Emergency Response Team) advisories of security problems, fixes and workarounds. Send requests to *cert@-cert.org*. Past advisories and other information is available for anonymous FTP from *cert.org*.
- CERT-tools
  Mailing list for discussion of computer security tools. Send requests to *cert@cer-t.org.*
- SERT-public
  Mailing list for SERT-published (Australian - Security Emergency Response Team) advisories of security problems, fixes and workarounds. Send requests to *sert@sert.edu.au*. Past advisories and other information is available for anonymous FTP from *ftp.sert.edu.au.*
- Sun-managers
  Mailing list for Managers of SUN systems, designed for a quick turn around for specific problems. To subscribe, send a request to *sun-managers-request@eecs.n-wu.edu*, the request should contain simply one line *"add"*.
- Firewalls
  Mailing list for people interested in discussing design, construction and maintenance of Internet firewalls. To subscribe, send *"subscribe firewalls"* in the body of a message to *Majordomo@GreatCircle.COM*. Archives available for anonymous FTP from *FTP.GrearCircle.COM.*

B.4 Usenet Newsgroups

• alt.security	Security issues on computer systems.
• comp.admin.policy	Discussions of site administration polocies.
• comp.protocols.kerberos	The Kerberos authentication server.
• comp.protocols.tcp-ip	TCP and IP network protocols.
• comp.security.announce	Announcements from CERT.
• comp.security.misc	Security issues of computers and networks.
• comp.security.unix	Discussion of UNIX security.
• comp.sources.misc	Miscellaneous software postings.
• comp.sources.unix	UNIX oriented sources.
• comp.sys.sun.admin	SUN system administration issues and questions.
• comp.unix.admin	Administering a UNIX bases system.
• comp.unix.wizards	Questions for only true UNIX wizards.
• news.answers	(security FAQ)