Forum of Incident Response and Security Teams
1994 Security Tools and Techniques CD-ROM

July, 1994

Introduction

Welcome to the FIRST 1994 Security Tools and Techniques CD-ROM. On this disc, you will find over 275 megabytes of information related to computer and data security, including over one hundred papers on various topics, over fifty software packages for UNIX systems, numerous virus scanners and similar tools for PCs and Macs, complete collections of the advisories issued by many of the FIRST member teams, password cracking dictionaries, summaries of computer-related laws by state and country, electronic ‘‘hacker’’ magazines, and more. The information contained on the FIRST CD-ROM has been collected from anonymous FTP sites around the world. Indeed, that is the primary purpose of the disc: to collect in a single place the information and tools that are scattered about the Internet, so that you, the user, can have a single place from which to obtain them.

THE MATERIAL ON THIS CD-ROM IS PROVIDED AS-IS

We (the Forum of Incident Response and Security Teams, the United States Government, Purdue University, and David A. Curry) disclaim all warranties with regard to the contents of this disc, including all implied warranties of merchantibility and fitness. In no event shall we be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of the contents of this disc.

USE OF THIS MATERIAL IS AT YOUR OWN RISK

The material on this disc has been collected via the Internet from anonymous FTP sites all over the world. No effort has been made to verify that the software thus obtained is free from viruses, Trojan horses, or other forms of malicious programming. No effort has been made to verify that the software performs as its authors claim, or that it even compiles. Before making use of any of this software, we recommend that you examine the source code, if available, and be sure that you believe it to be free of malicious code. Likewise, we recommend that you scan binary programs for viruses before installing or executing them on your system. In short, treat this material with the same caution and care you would use if you had FTPed it yourself.

Disk Format

This CD-ROM is formatted according to the ISO-9660 standard, which is based on a *de facto* industry standard format called ‘‘High Sierra.’’ The ISO-9660 format is very portable; nearly every system that supports CD-ROMs supports the ISO-9660 format in addition to any operating system specific formats the system offers. Most systems that support the ‘‘High Sierra’’ format (such as SunOS 4.1.*x*) will also support the ISO-9660 format. If you're not sure whether or not your system supports this format, the easiest way to find out is just to try it. Since the CD-ROM is a read-only media, you can't do any permanent damage.

Unfortunately, to obtain the maximum portability between operating systems, the designers of the ISO-9660 format had to impose rather serious constraints on the file and directory naming scheme that could be used. An ISO-9660 file system is very much like the one offered by MS-DOS:

- File and directory names may contain only upper-case letters, digits, and underscore characters.
- File names consist of a 0-8 character base name, a period ('.'), and a 0-3 character extension name. Either the base name or the extension name (but not both) may be missing.
- A version number, separated from the file name by a semi-colon (e.g., ``;1'') is required for all file names.
- Directory names consist of a 0-8 character base name, no period, and no extension name.
- A maximum of eight levels of directories are allowed, and only 510 files may appear in any directory. A path name (complete file name as specified from the top-level directory) is limited to a total length of 65 characters.
- No facilities are provided for file ownership, access permissions, links, and so forth.

When you use an ISO-9660 format disc on most UNIX systems, the CD-ROM driver typically makes some silent modifications to the ISO-9660 names so that they follow UNIX conventions. For example, many systems map alphabetic characters to lower case, hide the version numbers, and sometimes hide trailing periods. They typically give all files and directories a permission mode of 0555 (`r-xr-xr-x`).

In the table of contents on the following pages, all file and directory names are shown in lower case, and version numbers are not shown (all files have version number ``;1''). If your system displays upper case names and/or version numbers and does not map lower case letters into upper case or automatically append version numbers when needed, you will have to make these conversions yourself when accessing the disc. Within path names in the table of contents, the UNIX convention of using a slash (``/'') to separate path name components (e.g., */one/two/three/file.txt*) is used. If your system uses some other convention, such as the backslash (``\'') of MS-DOS, you will have to make this conversion yourself as well.

File Name Extensions

For each file on the disc, the file name extension is used to indicate the format of the file. The extensions in use on this edition of the disc are:

.hqx A BinHex'd file for the Macintosh. Use BinHex or StuffIt to debinhex the file.

.ps PostScript, the page description language from Adobe. You can send this to a laser printer that understands PostScript, such as any Apple LaserWriter, or most of the newer Hewlett-Packaer LaserJet printers. You can also preview it on the screen using a PostScript previewer such as `ghostscript`.

.sea A BinHex'd self-extracting Compact Pro archive for the Macintosh. Use Compact Pro, BinHex, or StuffIt to debinhex the files, then double click on the debinhexed files to extract the files from the compactor archives.

.tar A UNIX ''tar'' (tape archive) file. This file contains an archive of other files and directories. It can be extracted into the current directory on a UNIX system by using the command `tar -xvf` *`filename`*, or a table of contents of the archive can be listed by using the command `tar -tvf` *`filename`*. For PC and Macintosh users, some public-domain programs that can read UNIX ''tar'' archives have been supplied in the ***archprog*** directory on the disc.

.txt Plain ASCII text. May contain backspaces for underlining or bold face, and may occasionally contain non-ASCII (but usually ISO Latin-1) symbols such as letters with diacritical marks.

.zip A ''zip'' archive file. This file contains an archive of other files and directories, and is in a format that is commonly used on MS-DOS systems. It can be extracted into the current directory using the command `unzip` *`filename`*. For UNIX and Macintosh users, some public-domain programs that can read ''zip'' archives has been supplied in the ***archprog*** directory on the disc.

1. The Top-Level Directory

At the top level of the CD-ROM directory tree, the collection of software, papers, and so forth has been subdivided into several categories. Each category is contained in its own directory; most of the categories have been further subdivided into subdirectories. The rest of this document provides a detailed listing of each file on the disc, and a brief description of its contents.

At the top level, the following subdirectories are available:

archprog Software for various platforms to read the archive files stored on the rest of the disc.

ethics A collection of ''ethics'' documents and computer usage policies, maintained by Dave Grisham of the University of New Mexico.

maillist Archives of various security-related mailing lists and electronically distributed journals and magazines.

papers Research papers, journal articles, documentation, and other information on a wide variety of computer and data security-related topics.

passdict A collection of password cracking dictionaries.

policies A collection of policies on vaious topics, maintained as part of the Computers and Academic Freedom archives of the Electronic Freedom Foundation.

software Public domain (or freely available) software tools that are releated to computer security or incident response. Some of these programs are directed at computer security, others have primary purposes doing other things, but can be useful in the security field as well. Where possible, source code is provided. In cases where binaries only are provided, use them at your own risk.

teaminfo Information about and provided by the FIRST member teams. Includes advisories, articles, etc.

1.1. */archprog*

The ***/archprog*** directory contains software for various platforms to read the archive files stored on the rest of the disc. The files in this directory are:

dostar.zip An MS-DOS implementation of the `tar` command, for extracting ''tar'' format archive files.

mactar.hqx A Macintosh implementation of the `tar` command, for extracting ''tar'' format archive files. Version 4.0b.

macunzip.hqx The Info-ZIP Macintosh implementation of the `unzip` command, for extracting ''zip'' format archive files. Version 5.1.

unxunzip.tar The Info-ZIP UNIX implementation of the `unzip` command, for extracting ''zip'' format archive files. Version 5.1.

1.2. */ethics*

The ***/ethics*** directory contains a collection of ''ethics'' documents and computer usage policies, maintained by Dave Grisham of the University of New Mexico.

1.3. */maillist*

The ***/maillist*** directory contains the archives of various security-related mailing lists and electronically distributed journals and magazines. The subdirectories in this directory are:

bugtraq	The archives of the `bugtraq@crimelab.com` full-disclosure security hole mailing list.
cud	The Computer Underground Digest electronic magazine.
firewall	The archives of the `firewalls@greatcircle.com` mailing list.
nia	The Network Information Access electronic magazine.
phrack	The Phrack electronic magazine.
surfpunk	The SURFPUNK Technical Journal electronic magazine.
virus_l	The archives of the `virus-l@lehigh.edu` mailing list.

1.4. */papers*

The ***/papers*** directory contains research papers, journal articles, documentation, and other information on a wide variety of computer and data security-related topics. Within the ***/papers*** directory, the following subdirectories are available:

authent	Documents related to authentication of users, communications, and hosts.
criteria	Documents related to security evaluation criteria for computer systems and protocols.
crypto	Documents related to cryptograhic protocols and methods.
firewall	Documents related to the construction and use of network firewalls.
general	Documents that cover computer security in general and other miscellaneous topics.
legal	Documents related to computer security, the law, and ethics.
password	Documents related to passwords.
protocol	Documents related to the design of secure network protocols, and to the security analysis of existing protocols.
unix	Documents related to the security of the UNIX operating system.
virus	Documents related to computer viruses, worms, etc. The Internet Worm papers are in this directory.

1.4.1. */papers/authent*

The ***/papers/authent*** directory contains documents related to authentication of users, communications, and hosts. The files in this directory are:

kerberos.ps	Steiner, Jennifer G., Clifford Neuman, Jeffrey I. Schiller. ‘‘Kerberos: An Authentication Service for Open Network Systems.’’ A description of the Kerberos authentication system.
kerbdial.ps	Bryant, Bill. ‘‘Designing an Authentication System: A Dialogue in Four Scenes.’’ A ‘‘play’’ in which the characters end up designing an authentication system much like Kerberos. Provides an easy-to-understand description of why Kerberos is the way it is.

kerblim.ps Bellovin, Steven M. and Michael Merritt. ''Limitations of the Kerberos Authentication System.'' A description of some limitations and weaknesses in the Kerberos authentication system.

kknight.ps Molva, Refik, Gene Tsudik, Els Van Herreweghen, Stefano Zatti. ''KryptoKnight Authentication and Key Distribution System.'' An authentication and key distribution system that provides facilities for secure communication in any type of network environment.

longjobs.ps Rubin, A. D. and P. Honeyman. ''Long Running Jobs in an Authenticated Environment.'' A system for running batch jobs in an environment in which users must have tokens or tickets to run.

ntn.ps Neuman, B. Clifford and Stuart G. Stubblebine. ''A Note on the Use of Timestamps as Nonces.'' A note on the use of timestamps in authentication protocols.

1.4.2. */papers/criteria*

The ***/papers/criteria*** directory contains documents related to security evaluation criteria for computer systems and protocols. The files in this directory are:

ctcpec1.ps ''Canadian Trusted Computer Product Evaluation Criteria, Part 1.'' The Canadian ''Orange Book.''

ctcpec2.ps ''Canadian Trusted Computer Product Evaluation Criteria, Part 2.'' The Canadian ''Orange Book.''

exeguide.txt Helsing, Cheryl, Marianne Swanson, and Mary Anne Todd. ''Executive Guide to the Protection of Information Resources.'' A U.S. National Institute of Standards and Technology publication.

fcvol1.ps ''Federal Criteria for Information Technology Security, Volume 1.'' The new ''Orange Book.''

fcvol2.ps ''Federal Criteria for Information Technology Security, Volume 2.'' The new ''Orange Book.''

greenbk.txt ''Green Book on the Security of Information Systems.'' A document that sets out the development of a consistent approach to Information Security in Europe, taking into account common interests with other countries.

harmony.ps ''Foundations for the Harmonization of Information Technology Security Standards.'' An analysis of the differences between the U.S., Canadian, and European Information Technology Security efforts, and discussions of how to make them more similar.

horses.ps Hambridge, Sally and Jeffrey C. Sedayao. ''Horses and Barn Doors: Evolution of Corporate Guidelines for Internet Usage.'' A description of how Intel Corp.'s Internet usage policies were developed.

internet.txt Pethia, R., S. Crocker, and B. Fraser. ''Guidelines for the Secure Operation of the Internet – RFC 1281.'' Provides a set of guidelines to aid in the secure operation of the Internet.

itsec.txt ''Information Technology Security Evaluation Criteria.'' The European ''Orange Book.''

mgtguide.txt Helsing, Cheryl, Marianne Swanson, and Mary Anne Todd. ‘‘Management Guide to the Protection of Information Resources.’’ A U.S. National Institute of Standards and Technology publication.

oss Karila, Arto T. This subdirectory contains the PostScript files that make up ‘‘Open Systems Security: An Architectural Framework.’’ Thesis dissertation presenting an architecture for building secure open systems communication via untrusted global data networks.

psfos.ps Neuman, B. Clifford. ‘‘Protection and Security Issues for Future Systems.’’ An examination of the problems of protection and security as applied to future computer systems.

relate.ps ‘‘Relating Functionality Class and Security Sub-Profile Specifications.’’ A discussion of various alternatives for associating functionality class and security sub-profiile specifications, such as those presented in the Federal Criteria (***fcvol1.ps*** and ***fcvol2.ps***).

tcsec.txt ‘‘Department of Defense Trusted Computer System Evaluation Criteria.’’ The ‘‘Orange Book.’’

1.4.3. */papers/crypto*

The ***/papers/crypto*** directory contains documents related to cryptographic protocols and methods. The files in this directory are:

acmcrypt.ps Landan, Susan, et al. ‘‘Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy.’’ A report of a special panel of the ACM (Association for Computing Machinery) U.S. Public Policy Committee.

aeke.ps Bellovin, Steven M. and Michael Merritt. ‘‘Augmented Encrypted Key Exchange: A Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise.’’ An extension of the protocol described in ***neke.ps*** that removes the requirement that the host store passwords in cleartext.

cfs.ps Blaze, Matt. ‘‘A Cryptographic File System for Unix.’’ A description of a UNIX file system implementation that provides transparent encryption and decryption of files stored on the disk.

cfskey.ps Blaze, Matt. ‘‘Key Management in an Encrypting File System.’’ A description of how ‘‘smart cards’’ can be used to manage the keys used by the encryption file system described in ***cfs.ps***.

des.ps Feldmeier, David C. ‘‘A High-Speed Software DES Implementation.’’ Describes a high-speed software implementation of the Data Encryption Standard.

desbreak.ps Wayner, Peter C. ‘‘Using Content-Addressable Search Engines to Encrypt and Break DES.’’ A very simple parallel architecture using a modifed version of content-addressable memory can be used to cheaply and efficiently encipher and decipher data with DES-like systems. Describes how to implement these systems, and also how to construct a large scale engine for exhaustively searching the keyspace of DES.

eesproto.ps Blaze, Matt. ''Protocol Failure in the Escrowed Encryption Standard.'' A description of some protocol weaknesses in the Clinton administration's Escrowed Encryption Standard, also known as the Clipper Chip.

fail.ps Anderson, Ross. ''Why Cryptosystems Fail.'' A survey of the failure modes of retail banking systems, the second largest application of cryptography.

neke.ps Bellovin, Steven M. and Michael Merrit. ''Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks.'' A combination of public- and private-key cryptography that allows two parties sharing a common password to exchange confidential and authenticated information over an insecure network. The protocol is secure against active attack, and also against off-line ''dictionary'' attacks.

pkcs This subdirectory contains the complete family of Public-Key Cryptography Standards from RSA Laboratories. They cover RSA encryption, Diffie-Hellman key agreement, password-based encryption, extended-certificate syntax, cryptographic message syntax, private-key information syntax, and certification request syntax, as well as selected attributes. The files in this subdirectory are:

- ***examples.ps*** ''Some Examples of the PKCS Standards.''
- ***layman.ps*** ''A Layman's Guide to a Subset of ASN.1, BER, and DER.''
- ***overview.ps*** ''An Overview of the PKCS Standards.''
- ***pkcs_1.ps*** ''RSA Encryption Standard.''
- ***pkcs_2.ps*** Deprecated.
- ***pkcs_3.ps*** ''Diffie-Hellman Key-Agreement Standard.''
- ***pkcs_4.ps*** Deprecated.
- ***pkcs_5.ps*** ''Password-Based Encryption Standard.''
- ***pkcs_6.ps*** ''Extended-Certificate Syntax Standard.''
- ***pkcs_7.ps*** ''Cryptographic Message Syntax Standard.''
- ***pkcs_8.ps*** ''Private-Key Information Syntax Standard.''
- ***pkcs_9.ps*** ''Selected Attribute Types.''
- ***pkcs_10.ps*** ''Certifcation Request Syntax Standard.''

privkey.ps Davis, Don and Ralph Swick. ''Network Security via Private-Key Certificates.'' Some practical security protocols that use private-key encryption in the public-key style.

rsafaq.ps Fahn, Paul. ''Answers to Frequently Asked Questions About Today's Cryptography.''

scfaq.txt Readers of *sci.crypt*. ''Cryptography FAQ.''

skipjack.txt Brickell, Ernest F., Dorothy E. Denning, Stephen T. Kent, David P. Maher, and Walter Tuchman. ''SKIPJACK Review: Interim Report: The SKIPJACK Algorithm.'' The report from the group of non-government cryptologists who reviewed the classified SKIPJACK encryption algorithm used in the Clinton administration's Clipper and Capstone chips.

swipe.ps Ioannidis, John and Matt Blaze. ‘‘The Architecture and Implementation of Network Layer Security Under Unix.’’ A description of a network-layer security protocol for the IP protocol suite that provides authentication, integrity, and confidentiality of IP datagrams.

visa.ps Estrin, Deborah, Gene Tsudik, and Jeffrey Mogul. ‘‘Visa Protocols for Controlling Inter-Organizational Datagram Flow.’’ A cryptographic method for authenticating and authorizing a flow of datagrams.

visaext.ps Estrin, Deborah, Gene Tsudik, and Jeffrey Mogul. ‘‘Visa Protocols for Controlling Inter-Organizational Datagram Flow: Extended Description.’’ A cryptographic method for authenticating and authorizing a flow of datagrams.

1.4.4. */papers/firewall*

The ***/papers/firewall*** directory contains documents related to the construction and use of network firewalls. The files in this directory are:

cslater.ps Corbridge, Bruce, Robert Henig, and Charles Slater. ‘‘Packet Filtering in an IP Router.’’ A description of how the packet filtering facility in the Telebit NetBlazer was designed and developed.

dec.ps Ranum, Marcus J. ‘‘A Network Firewall.’’ A description of Digital Equipment Corporation’s network firewall between its corporate network and the Internet.

fwalls.ps Ranum, Marcus J. ‘‘Thinking About Firewalls.’’ A description of some of the considerations and tradeoffs in designing network firewalls.

gatekeep.ps Schauer, Hervé and Christphe Wolfhugel. ‘‘An Internet Gatekeeper.’’ A description of how to construct an Internet firewall.

gateway.ps Cheswick, Bill. ‘‘The Design of a Secure Internet Gateway.’’ A description of the design of the firewall used by AT&T to protect their corporate network from the Internet.

isoc94.ps Avolio, Frederick M. and Marcus J. Ranum. ‘‘A Network Perimeter With Secure External Access.’’ A description of the firewall in use at *whitehouse.gov*.

packets.ps Bellovin, Steven M. ‘‘Packets Found on an Internet.’’ A description of the types of packets, particularly the anomalous ones, that appeared at the AT&T firewall.

pktfilt.ps Chapman, D. Brent. ‘‘Network (In)Security Through IP Packet Filtering.’’ A description of how to use the packet filtering features of commercial routers as a security tool.

screen.ps Mogul, Jeffrey C. ‘‘Simple and Flexible Datagram Access Controls for Unix-based Gateways.’’ A description of the `screend` packet filtering system.

tcpwrap.ps Venema, Wietse. ‘‘TCP Wrapper: Network Monitoring, Access Control, and Booby Traps.’’ A description of the author’s `tcpwrapper` software.

toolkit.ps Ranum, Marcus J. and Frederick M. Avoilio. ‘‘A Toolkit and Methods for Internet Firewalls.’’ A description of the Trusted Information Systems Firewall Toolkit.

unixnet.ps Reinhardt, Robert B. ‘‘An Architectural Overview of UNIX Network Security.’’ A description of a number of UNIX-related components of network security, particularly as they pertain to firewalls.

xthrufw.ps Treese, G. Winfield and Alec Wolman. ‘‘X Through the Firewall, and Other Application Relays.’ A description of how to create application-specifc relays to pass traffic through a network firewall.

1.4.5. */papers/general*

The ***/papers/general*** directory contains documents that cover computer security in general, and some other miscellaneous topics. The files in this directory are:

berferd.ps Cheswick, Bill. ‘‘An Evening With Berferd: In Which a Cracker is Lured, Endured, and Studied.’’ A description of how the author kept an attacker ‘‘on the line’’ for several months in order to learn his methods.

certresp.ps Pethia, Richard D. and Kenneth R. van Wyk. ‘‘Computer Emergency Response – An International Problem.’’ A call for international cooperation between computer emergency response teams, and suggested methods for achieving it.

compro.txt Klaus, Christopher William. ‘‘Compromise: What if Your Machines are Compromised by an Intruder.’’ Suggestions for securing a system after it has already been compromised.

dragons.ps Bellovin, Steven M. ‘‘There Be Dragons.’’ A description of the wide variety of attacks attempted on the AT&T Internet firewall.

estcsirc.ps Wack, John P. ‘‘Establishing a Computer Security Incident Response Capability.’’ Procedures and issues for establishing a computer security incident response team.

faq.txt Muffett, Alec. ‘‘Almost Everything You Wanted To Know About Security.’’

forensic.ps Spafford, Eugene H. ‘‘Software Forensics: Can We Track Code to its Authors?’’ An idea that it may be possible to identify the authors of malicious software by the style and features of their programs.

ftpfaq.txt Klaus, Christopher William. ‘‘How to Set Up a Secure Anonymous FTP Site.’’ Methods for numerous different operating systems.

fuat.ps Baran, Fuat, Howard Kaye, and Margarita Suarez. ‘‘Security Breaches: Five Recent Incidents at Columbia University.’’ A detailed account of five break-ins at Columbia University, and the steps taken to stop them.

hacker.txt Meyer, Gordon R. ‘‘The Social Organization of the Computer Underground.’’ The author’s thesis for a master’s degree in sociology.

handbook.txt Holbrook, P. and J. Reynolds. ‘‘Site Security Handbook – RFC 1244.’’ The product of the Site Security Policy Handbook Working Group of the Internet Engineering Task Force.

holland.ps Van Doorn, Leendert. ''Computer Break-ins: A Case Study.'' A study of multiple break-in attempts at Vrije Universiteit in Amsterdam.

netcash1.ps Medvinsky, Gennady and B. Clifford Neuman. ''Electronic Currency for the Internet.'' A framework for electronic currency for the Internet that provides a real-time electronic payment system.

netcash2.ps Medvinsky, Gennady and B. Clifford Neuman. ''NetCash: A Design for Practical Electronic Currency on the Internet.'' A framework for electronic currency for the Internet that provides a real-time electronic payment system.

nist.txt Helsing, Cheryl, Marianne Swanson, and Mary Anne Todd. ''Computer User's Guide to the Protection of Information Resources.'' A report from the U.S. National Institute of Standards and Technology.

nistbook Roback, Edward and Barbara Guttman. ''An Introduction to Computer Security: The NIST Handbook.'' A publication of the U.S. National Institute of Standards and Technology. This is a draft copy, included with permission.

patches.txt Klaus, Christopher William. ''Security Patches FAQ for Your System: The Patch List.'' A list of security patches for most any operating system, and how to obtain them.

pbaa.ps Neuman, B. Clifford. ''Proxy-Based Authorization and Accounting for Distributed Systems.'' A method to support both authorization and accounting in a distributed environment.

pnetext.ps Bellovin, S. M. ''Pseudo-Network Drivers and Virtual Networks.'' A method for creating pseudo-networks, much like the pseudo-terminals in use on many UNIX systems.

primer.ps Brand, Russell L. ''Coping with the Threat of Computer Security Incidents: A Primer from Prevention through Recovery.'' A basic text for the author's one-day seminar on the practical aspects of computer security in an unclassified networked environment.

tools.ps Polk, W. Timothy. ''Automated Tools for Testing Computer System Vulnerability.'' Discusses some of the automated tools for checking the security of a wide variety of systems.

vendors.txt Klaus, Christopher William. ''Vendor Security Contacts: Reporting Vulnerabilities and Obtaining New Patches.'' Contact names, numbers, and addresses for most major operating systems.

1.4.6. */papers/legal*

The ***/papers/legal*** directory contains documents related to computer security, the law, and ethics. The files in this directory are:

bbslibel.txt Kahn, John R. ''Defamation Liability of Computerized Bulletin Board Operators and Problems of Proof.'' A discussion of the libel and slander laws, and how they apply to bulletin board operators.

cfa.txt Complete text of the Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030.

copyrfaq.txt Carroll, Terry. ‘‘Frequently Asked Questions About Copyright.’’

cslaw.txt Morris, Gary S. ‘‘Computer Security and the Law.’’ A review of legal issues surrounding computer security, for the system administrator.

cubby.txt The complete text of the judge’s decision in the Cubby v. CompuServe libel case, in which CompuServe was found not to be responsible for material posted on one of their bulletin boards.

ecpa.txt Complete text of the Electronic Communications Privacy Act of 1986, United States Public Law 99-508.

elaw.ps Loundy, David J. ‘‘E-Law: Legal Issues Affecting Computer Information Systems and System Operator Liability.’’ First appeared in the Albany Law Journal of Science and Technology, Volume 3, Number 1.

ethics.ps Spafford, Eugene H. ‘‘Are Computer Hacker Break-ins Ethical?’’ Lists and refutes many of the reasons given to justify computer break-ins.

ferpa.txt The complete text of the U.S. Family Educational Right to Privacy Act (the Buckley Amendment), 20 U.S.C. 1232g.

frlaw.txt Information about the computer crime laws in France.

hansen.txt Hansen, Stephen E. ‘‘Legal Issues, A Site Manager’s Nightmare.’’ Examines the legal ramifications of computer security laws on system administrators.

libel.txt Godwin, Mike. ‘‘Internet Libel: Is the Provider Responsible?’’ An examination of the Cubby v. Compuserve case as it applies to Internet service providers.

mailpriv.txt Hernandez, Ruel T. ‘‘Computer Electronic Mail and Privacy.’’ A discussion of the Electronic Communications Privacy Act as it applies to electronic mail.

musings.ps Spafford, Eugene H. ‘‘Some Musings on Ethics and Computer Break-Ins.’’ A discussion of ethics and responsibility, particularly as they pertain to the Internet Worm of November, 1988.

privacy.ps Complete text of the Privacy Act of 1974 and Amendments, 5 U.S.C. 552a.

simson.ps Garfinkel, Simson. ‘‘An Introduction to Computer Security for Lawyers.’’ A number of articles serving to introduce lawyers to the concepts behind computer security.

sentence.txt King, Jack. ‘‘Revised Computer Crime Sentencing Guidelines.’’ A description of the new federal sentencing guidelines that address the Computer Fraud and Abuse Act.

statelaw.txt Computer crime laws, listed by state.

1.4.7. */papers/password*

The ***/papers/password*** directory contains documents related to passwords. The files in this directory are:

dodpwman.txt ‘‘Department of Defense Password Management Guideline.’’ Enumerates a number of good password management practices.

fips181.txt National Institute of Standards and Technology. ‘‘Standard for Automated Password Generator.’’ Federal Information Processing Standard No. 181.

klein.ps Klein, Daniel V. ‘‘Foiling the Cracker: A Survey of, and Improvements to, Password Security.’’ Demonstrates the ease with which most passwords can be guessed by a motivated attacker.

observe.ps Spafford, Eugene H. ‘‘Observing Reusable Password Choices.’’ A method for observing password choices made by users, and how to protect it from being compromised.

opus.ps Spafford, Eugene H. ‘‘OPUS: Preventing Weak Password Choices.’’ A system that uses Bloom filters to implement a constant-time dictionary lookup, regardless of dictionary size, to check a user’s password choice for ‘‘goodness.’’

passbib.ps Spafford, Eugene H. and Stephen A. Weeber. ‘‘User Authentication and Related Topics: An Annotated Bibliography.’’

pwstudy.ps Morris, Robert and Ken Thompson. ‘‘Password Security: A Case History.’’ A description of the original UNIX password algorithm, and the reasons for replacing it with the current one.

pwtenyrs.ps Feldmeier, David C. and Philip R. Karn. ‘‘UNIX Password Security – Ten Years Later.’’ A reexamination of the UNIX password algorithm after ten years of advances in software and hardware.

skey.ps Haller, Neil M. ‘‘The S/Key One-Time Password System.’’ A freely available implementation of one-time passwords.

1.4.8. */papers/protocol*

The ***/papers/protocol*** directory contains documents related to the design of secure network protocols, and to the security analysis of existing protocols. The files in this directory are:

afs.ps Honeyman, P., L. B. Huston, M. T. Stolarchuk. ‘‘Highjacking AFS.’’ A description of security weaknesses in the Andrew File System (AFS).

e2e.ps Estrin, Deborah and Gene Tsudik. ‘‘An End-to-End Argument for Network Layer, Inter-Domain Access Controls.’’ A method by which different administrative domains of an internetwork can interconnect without exposing their internal resources to unrestricted access.

ident.txt St. Johns, M. ‘‘Identification Protocol – RFC 1413.’’ A description of the Identification Protocol, a means to determine the identity of the user of a particular TCP connection.

ipext.ps Bellovin, S. M. ‘‘Security Problems in the TCP/IP Protocol Suite.’’ A description of several attacks on TCP/IP protocols including sequence number spoofing, routing attacks, source address spoofing, and authentication attacks.

nis.ps Hess, David K., David R. Safford, and Udo W. Pooch. ‘‘A Unix Network Protocol Security Study: Network Information Service.’’ A discussion of the security weaknesses in the Network Information Service (Yellow Pages) protocol from Sun Microsystems.

ntp.ps Bishop, Matt. ‘‘A Security Analysis of the NTP Protocol.’’ A security analysis of the Network Time Protocol (NTP).

oak93.ps Stubblebine, Stuart G. and Virgil D. Gligar. ‘‘Protocol Design for Integrity Protection.’’ A design method for message integrity protection.

pem.ps Bishop, Matt. ‘‘Privacy-Enhanced Electronic Mail.’’ A description of the Internet Privacy-Enhanced Mail protocols.

tcp.ps Morris, Robert T. ‘‘A Weakness in the 4.2BSD TCP/IP Software.’’ A description of a security weakness of the TCP/IP protocol suite as implemented in 4.2BSD UNIX.

time.ps Bishop, Matt. ‘‘Security Analyses of Network Time Services.’’ An analysis of the security requirements for a network time service.

transit.ps Estrin, Deborah and Gene Tsudik. ‘‘Secure Control of Transit Internetwork Traffic.’’ Methods for controlling traffic traversing a local network on its way from one remote network to another.

tsudik Tsudik, Gene. This subdirectory contains the PostScript files that make up ‘‘Access Control and Policy Enforcement in Internetworks.’’ Methods of controlling access policy between different administrative domains of an internetwork.

1.4.9. */papers/unix*

The ***/papers/unix*** directory contains documents related to the security of the UNIX operating system. The files in this directory are:

cops.ps Farmer, Daniel and Eugene H. Spafford. ‘‘The COPS Security Checker System.’’ A description of one of the most popular UNIX security scanners.

farmer.txt Farmer, Dan and Wietse Venema. ‘‘Improving the Security of Your Site by Breaking Into It.’’ Discussion of a number of commonly used attacks on UNIX systems, and how to check your systems for vulnerability to them.

nides This subdirectory contains papers describing the Next-Generation Intrusion Detection Expert System (NIDES) from SRI International. This system monitors the C2 audit trails generated by Sun workstations in real-time and alerts the administrator to anomalous user behavior. The papers in this subdirectory are:

- ***canada93.ps*** Lunt, Teresa F. ‘‘Detecting Intruders in Computer Systems.’’
- ***reqts94.ps*** Lunt, Teresa F. and Debra Anderson. ‘‘Software Requirements Specification: Next Generation Intrusion Detection Expert System.’’
- ***safegard.ps*** Anderson, Debra, Teresa F. Lunt, Harold Javitz, Ann Tamaru, Alfonso Valdes. ‘‘SAFEGUARD Final Report: Detecting Unusual Program Behavior Using the NIDES Statistical Component.’’

statrept.ps Javitz, Harold S. and Alfonso Valdes. ‘‘The NIDES Statistical Component: Description and Justification.’’

survey.ps Lunt, Teresa F. ‘‘Automated Audit Trail Analysis and Intrusion Detection: A Survey.’’

noroot.ps Simmons, Steve. ‘‘Life Without Root.’’ A method for authorizing users to perform certain system administration tasks without giving them the super-user password.

password.ps Belgers, Walter. ‘‘UNIX Password Security.’’ A discussion of the importance of well-chosen passwords, and how passwords are cracked.

ritchie.ps Ritchie, Dennis M. ‘‘On the Security of UNIX.’’ The original UNIX security paper.

sessext.ps Bellovin, S. M. ‘‘The ‘Session Tty’ Manager.’’ A method for controlling access to terminals by background processes after the user has logged out.

sri.ps Curry, David A. ‘‘Improving the Security of Your UNIX System.’’ A description of many of the security features of the average UNIX system, and how to use them.

tools.ps Morrison, Geoff. ‘‘UNIX Security Tools.’’ An excellent summary of most of the public domain UNIX security tools, and where to obtain them. Almost all of these tools are available on this CD-ROM.

tripwire.ps Kim, Gene H. and Eugene H. Spafford. ‘‘The Design and Implementation of Tripwire: A File System Integrity Checker.’’ Tripwire computes checksums of files on the system, and then scans later for any changes to those files.

twexper.ps Kim, Gene H. and Eugene H. Spafford. ‘‘Experiences With Tripwire: Using Integrity Checkers for Intrusion Detection.’’ A description of how the Tripwire integrity checker (see ***tripwire.ps***) has performed in the field.

unixsec.ps Bačić, Eugen Mate. ‘‘UNIX & Security.’’ Describes many of the security features of the UNIX operating system, as well as features that could be added to result in an evaluatable system at Class C2.

utnet.ps Spurgeon, Charles. ‘‘UTnet Guide to UNIX System Security.’’ A guide to UNIX security resources.

1.4.10. */papers/virus*

The ***/papers/virus*** directory contains documents related to computer viruses, worms, etc. The Internet Worm papers are in this directory. The files in this directory are:

alife.ps Spafford, Eugene H. ‘‘Computer Viruses as Artificial Life.’’ A consideration of computer viruses as artificial life – self-replicating organisms.

faq.txt Readers of *VIRUS-L* and *comp.virus*. ‘‘Frequently Asked Questions on VIRUS-L/comp.virus.’’

fedeli.txt Fedeli, Alan. ‘‘Organizing a Corporate Anti-Virus Effort.’’ A description of how IBM Corp. has learned to cope with computer viruses and related threats.

gao.txt United States Government Accounting Office. ‘‘Computer Security.’’ The G.A.O.’s report on the Internet Worm of November, 1988, and on the then-current state of Internet vulnerabilities and prosecution of computer virus cases.

iworm1.ps Spafford, Eugene H. ‘‘The Internet Worm Program: An Analysis.’’ A description of the algorithms used by the Internet Worm program of November 2, 1988.

iworm2.ps Spafford, Eugene H. ‘‘The Internet Worm Incident.’’ A description of the events involved in the Internet Worm of November 2, 1988.

mallogic.ps Bishop, Matt. ‘‘An Overview of Computer Viruses in a Research Environment.’’ An examination of computer viruses as malicious logic in a research and development environment and current techniques in controlling the threats of viruses and other malicious logic programs.

mgtguide.ps Wack, John P. and Lisa J. Carnahan. ‘‘Computer Viruses and Related Threats: A Management Guide.’’ Guidelines for preventing, deterring, containing, and recovering from attacks of viruses and related threats. A report from the U.S. National Institute of Standards and Technology.

mit.ps Eichin, Mark W. and Jon A. Rochlis. ‘‘With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988.’’ A detailed description of the events of the Internet Worm of November 2, 1988 from one of the teams of people who combatted it.

selguide.ps Polk, W. T. and L. E. Bassham. ‘‘A Guide to the Selection of Anti-Virus Tools and Techniques.’’ Criteria for judging the functionality, practicality, and convenience of anti-virus tools. A report from the U.S. National Institute of Standards and Technology.

tour.ps Seeley, Donn. ‘‘A Tour of the Worm.’’ A tour of the Internet Worm of November 2, 1988.

1.5. */passdict*

The ***/passdict*** directory contains a collection of password cracking dictionaries in various languages. The directory is subdivided by language, with dictionaries from different sources in different files.

1.6. */policies*

The ***/policies*** directory contains a collection of policies on vaious topics, maintained as part of the Computers and Academic Freedom archives of the Electronic Freedom Foundation.

NOTE: The files in this directory are stored in a single ‘‘tar’’ archive, because the archive creators used extremely long file names that are not easily reduced to the 8-character limit required by ISO-9660. This ‘‘tar’’ archive will have to be extracted on a UNIX system; MS-DOS will not handle the file names well at all.

1.7. */software*

The ***/software*** directory contains public domain (or freely available) software tools that are related to computer security or incident response. Some of these programs are directed at computer security, others have primary purposes doing other things, but can be useful in the security field as well. Where possible, source code is provided. In cases where binaries only are provided, use them at your own risk. Within the ***/software*** directory, the following subdirectories are available:

dos	Software for PCs running MS-DOS.
mac	Software for the Macintosh.
unix	Software for various flavors of the UNIX operating system.

1.7.1. */software/dos*

The ***/software/dos*** directory contains software for PCs running MS-DOS. The subdirectories of this directory are:

network	Programs for controlling access to a system via the network.
security	Programs for controlling PC security.
virus	Anti-virus utilities.

1.7.1.1. */software/dos/network*

The ***/software/dos/network*** directory contains programs for controlling access to a system via the network. The files in this subdirectory are:

kbridge.zip	The `KarlBridge` package by Doug Karl. A program that runs on a PC with two Ethernet boards, turning the PC into a sophisticated, high-level, packet-filtering bridge. It can filter packets based on any specified protocol, including IP, XNS, DECNET, LAT, IPX, AppleTalk, etc. Version 2.0.

1.7.1.2. */software/dos/security*

The ***/software/dos/security*** directory contains programs for controlling PC security. The files in this directory are a mirror of the SimTel ***/msdos/security*** archive from `oak.oakland.edu`. See the file ***00_index.txt*** for a description of the files in this directory.

1.7.1.3. */software/dos/virus*

The ***/software/dos/virus*** directory contains anti-virus utilities. The files in this directory are a mirror of the SimTel ***/msdos/virus*** archive from `oak.oakland.edu`. See the file ***00_index.txt*** for a description of the files in this directory.

1.7.2. */software/mac*

The ***/software/mac*** directory contains software for the Macintosh. The subdirectories of this directory are:

virus	Anti-virus utilities.

1.7.2.1. */software/mac/virus*

The ***/software/mac/virus*** directory contains anti-virus utilities. The files in this directory are:

disinf.sea The Disinfectant virus scanner, preventer, and remover. Version 3.5.

gatekeep.hqx The Gatekeeper virus preventer. Version 1.3.

sample.sea The public source code for the reusable human interface modules from Disinfectant. Version 2.4.

virusdet.hqx The Virus Detective virus scanner. Version 5.05.

1.7.3. */software/unix*

The ***/software/unix*** directory contains software for various flavors of the UNIX operating system. The subdirectories of this directory are:

authent Programs for performing user and program authentication.

digsig Programs for computing digital signatures (cryptographic checksums).

firewall Programs for constructing network firewalls.

netmon Programs for monitoring network security.

network Programs for controlling access to a system via the network.

password Programs pertaining to password security.

sysmon Programs for monitoring system security.

tools Programs that are not specifically designed for computer security uses, but are nevertheless useful to the security practitioner.

1.7.3.1. */software/unix/authent*

The ***/software/unix/authent*** directory contains software for performing user and program authentication. The files in this directory are:

kerberos This subdirectory contains the sources and documentation for the Kerberos package from the Massachusetts Institute of Technology. There are two subdirectories of this directory:

- ***v4*** Version 4 Patchlevel 10. This is the final release of Version 4; all future development efforts will be based on Version 5. Release date: 9 December 1992.

- ***v5*** Version 5 Beta 4. This is the current release of Version 5; all current development efforts are based on this version. Release date: 15 June 1994.

libident.tar The `libident` library by Peter Eriksson. A library of functions to interface with an RFC1413 identification server. Version 0.14.

pidentd.tar The `pident` daemon by Peter Eriksson. Implements the RFC1413 identification server, that can be used to query a remote host for the identification of the user making a TCP connection request. Version 2.2.

skey.tar The S/Key one-time password system from Bellcore. Implements one-time passwords for UNIX systems. Includes one-time password generator programs for PCs and Macs.

1.7.3.2. */software/unix/digsig*

The ***/software/unix/digsig*** directory contains programs for computing digital signatures (cryptographic checksums). The files in this directory are:

md2.txt The source code and specification for the MD-2 message digest function.

md4.txt The source code and specification for the MD-4 message digest function.

md5.txt The source code and specification for the MD-5 message digest function.

snefru.tar The source code and documentation for the Snefru message digest function (Xerox Secure Hash Function). Version 2.5a.

1.7.3.3. */software/unix/firewall*

The ***/software/unix/firewall*** directory contains software for constructing network firewalls. The files in this directory are:

gau.tar The Gateway Access Utilities package from Sterling Software. Supports access to the Internet through a network firewall without requiring that users have accounts on the firewall host itself. These are modifed TELNET and FTP programs that work in a ‘‘proxy’’ fashion through the firewall. Version of 22 March 1993.

socks.tar The `socks` package, by David and Michelle Koblas. An Internet ‘‘socket server’’ consisting of a set of client library routines and a daemon that interact through a simple protocol to provide convenient and secure network connectivity through a firewall host. Version 3.

sckscstc.tar The CSTC release of the `socks` package (see ***socks.tar***). This version includes full source for the SOCKS server and SOCKS-ified client programs for `finger`, `ftp`, `telnet`, and `whois`. Version 4.1.

tcpr.tar The `tcpr` package by Paul Ziemba. A set of Perl scripts that enable the use of FTP and TELNET across a firewall. It consists of an `inetd`-like server, a relay program, and a client that talks to the server. Version 1.1.5.

tisfwtk This subdirectory contains the Trusted Information Systems (TIS) Firewall Toolkit, a fairly complete set of programs and instructions for constructing network firewalls. The contents of this directory are:

- ***alpha.tar*** The latest ‘‘prerelease’’ version of the toolkit, for those who wish to experiment with or modify the version that is currently under development. It is considered a stable release but may not contain up-to-date documentation or porting fixes. There are a number of portability fixes in this version that are not present in Version 1.2.
- ***fwtkdoc.tar*** The toolkit documentation. Version 1.2.
- ***fwtksrc.tar*** The toolkit source code. Version 1.2.

udprelay.tar The `udprelay` package by Tom Fitzgerald. A daemon process that runs on a firewall host and forwards UDP packets into and out of the firewalled network, as directed by a configuration file. Version 0.2.

xforward.tar The `xforward` package by Win Treese. Used for relaying X Window System connections across network firewalls. Version 1.0.

1.7.3.4. */software/unix/netmon*

The ***/software/unix/netmon*** directory contains programs for monitoring network security. The files in this directory are:

netman This subdirectory contains the NETMAN package of network monitoring and visualization tools from Curtin University. The `etherman` program is an X Window System tool that displays a representation of real-time Ethernet communications. The `interman` program focuses on IP connectivity within a single segment. The `packetman` tool is a retrospective Ethernet packet analyzer. Within the subdirectory are binaries for a number of different platforms. Source code is available for $500.00 for universities and $1,000.00 for companies and other groups. Version 1.1.

nocol.tar The NOCOL (Network Operations Center On-Line) package from JVNC-Net. Can monitor various network variables such as ICMP or RPC reachability, name servers, ethernet load, port reachability, host performance, SNMP traps, modem line usage, AppleTalk and Novell routes and services, BGP peers, etc. The software is extensible and new monitors can be added easily. Version 4.0beta (the beta release is very near formal release, and is recommended over the previous version).

tcpwho.tar The `tcpwho` program by Scott Chasin. Displays a list of all TCP connections and the corresponding user name and process identifier associated with each connection. Version 1.0.

1.7.3.5. */software/unix/network*

The ***/software/unix/network*** directory contains programs for controlling access to a system via the network. The files in this subdirectory are:

ipacl.tar The `ipacl` package from Siemens. Forces all TCP and UDP packets to pass through an access control list facility. The configuration file allows packets to be accepted, rejected, conditionally accepted, and conditionally rejected based on characteristics such as source address, destination address, source port number, and destination port number. Should be portable to any system that uses System V STREAMS for its network code. Version of 13 January 1993.

ldaemon.tar The `logdaemon` package by Wietse Venema. Provides modified versions of `rshd`, `rlogind`, `ftpd`, `rexecd`, `login`, and `telnetd` that log significantly more information than the standard vendor versions, enabling better auditing of problems via the logfiles. Also includes support for the S/Key one-time password package. Version 4.2.

portmap.tar The `portmap` program by Wietse Venema. A replacement for the standard Sun `portmap` program (portable to a number of vendors' systems) that attempts to close all known holes in `portmap`. This includes prevention of NIS password file theft, prevention of unauthorized `ypset` commands, and prevention of NFS file handle theft. Version 3.

rpcbind.tar The `rpcbind` program by Wietse Venema. A replacement for the Sun `rpcbind` program that offers access control and copious logging. Allows host access control based on network addresses. Preliminary version.

screend.tar The `screend` package by Jeff Mogul. Provides a daemon and kernel modifications to allow all packets to be filtered based on source address, destination address, or any other byte or set of bytes in the packet. Should work on most systems that use Berkeley-style networking in the kernel, but requires kernel modifications (i.e., kernel source code). Version of 21 January 1993.

seclib.tar The `securelib` package by William LeFebvre. Provides a replacement shared library for SunOS 4.1.*x* systems that offers new versions of the `accept`, `recvfrom`, and `recvmsg` networking system calls. These calls are compatible with the originals, except that they check the address of the machine initiating the connection to make sure it is allowed to connect, based on the contents of a configuration file. The advantage of this approach is that it can be installed without recompiling any software. Version 3.

tcpwrap.tar The `tcp_wrapper` package by Wietse Venema. Formerly called `log_tcp`. Allows monitoring and control over who connects to a host's TFTP, EXEC, FTP, RSH, TELNET, RLOGIN, FINGER, and SYSTAT ports. Also includes a library so that other programs can be controlled and monitored in the same fashion. Version 6.3.

xinetd.tar The `xinetd` program by Panagiotis Tsirigotis. A replacement for the `inetd` program that can be configured to perform access control based on host address or time of day, and to log significantly more information than most vendor versions. Version 2.0.6.

1.7.3.6. */software/unix/password*

The ***/software/unix/password*** directory contains programs pertaining to password security. The files in this subdirectory are:

anlpassw.tar The `anlpasswd` program (formerly `perl-passwd2`) from Argonne National Library. A proactive password checker that refuses to let users choose ‘‘bad’’ passwords. Version 2.2.

crack.tar The `crack` program by Alec Muffett. A password-cracking program with a configuration language, allowing the user to program the types of guesses used. Version 4.1.

cracklib.tar The `cracklib` distribution, by Alec Muffett. A library of functions that can be called from `passwd`-like programs to try to prevent users from choosing passwords that `crack` would be able to guess. Version 2.5.

npasswd.tar The `npasswd` program by Clyde Hoover. A plug-compatible replacement for `passwd` that refuses to accept ‘‘bad’’ passwords. Includes support for System V Release 3 password aging and Sun's Network Information Service (NIS) (Yellow Pages). Version 1.2.4.

obvious.tar The `obvious-pw` function by John Nagle. This function depends upon a subtle property of English. Less than one-third of the possible ‘‘triples,’’ sequences of three letters, are used in English words. This property makes it possible to distinguish random letter strings from strings that look like English words. The idea is to reject passwords that ‘‘look like’’ English words. Version of 10 November 1988.

pwplus.tar The `passwd+` program by Matt Bishop. A proactive password checker that is driven by a configuration file to determine what types of passwords are and are not allowed. The configuration file allows the use of regular expressions, the comparison of passwords against the contents of files (e.g., dictionaries), and the calling of external programs to examine the password. Version of 1 December 1993.

shadow.tar The `shadow` program by John F. Haugh, II. A replacement for `login` and `passwd` that can enable any system to use shadow password files. Includes support for shadow password files, shadow group files, DBM password files, double length passwords, and password aging. Version 3.1.4.

1.7.3.7. */software/unix/sysmon*

The ***/software/unix/sysmon*** directory contains programs for monitoring system security. The files in this directory are:

binaudit.tar The RIACS Intelligent Auditing and Categorizing System, from the Research Institute for Advanced Computer Science. A file system auditing program that compares current contents against previously-generated listings, and reports differences. Version 3.1.3.

cops.tar The Computer Oracle and Password System (COPS) package from Purdue University. Examines a system for a number of known weaknesses and alerts the system administrator to them; in some cases it can automatically correct these problems. Version 1.04.

cpm.tar The cpm program from Carnegie Mellon University. Checks a system for any network interfaces in promiscuous mode; this may indicate that an attacker has broken in and started a packet snooping program. Version 1.0.

ifstatus.tar The `ifstatus` program by Dave Curry. Checks a system for any network interfaces in promiscuous mode; this may indicate that an attacker has broken in and started a packet snooping program. Designed to be run out of `cron`.

iss.tar The `iss` program by Christopher Klaus. A multi-level security scanner that checks a UNIX system for a number of known security holes such as problems with `sendmail`, improperly configured NFS file sharing, etc. Version 1.21.

secure.tar The programs and scripts from the appendix of *UNIX System Security* by Patrick Wood and Steven Kochan. Version of 25 February 1989.

swatch.tar The `Swatch` package by Stephen Hansen and Todd Atkins. A system for monitoring events on a large number of systems. Modifies certain programs to enhance their logging capabilities, and software to then monitor the system logs for ‘‘important’’ messages. Version 2.1.

tamu This subdirectory contains the various TAMU security tools from Texas A&M University. The contents of this directory are:

check.txt A shell script for checking the integrity of the distribution.

drawbrid.tar The `drawbridge` bridging filter. It uses a PC with two ethernet cards to perform the filtering. Version 1.1.

netlog.tar The `netlog` programs. These constitute a TCP and UDP traffic logging system, usable for locating suspicious network traffic. Version 1.2.

spar.tar The `spar` program, for showing process accounting records. Much more flexible and powerful than the standard UNIX utilities such as `lastcomm`. Version 1.2.

sra.tar The `sra` program, which provides secure RPC authentication for FTP and TELNET. Version 1.3.

tiger.tar The `tiger` package of system monitoring scripts. Similar to COPS in what they do, but significantly more up to date, and easier to configure and use. Version 2.2.3.

tigersig.tar The digital signature databases for several operating system distributions, for use by the `tiger` file integrity scanning scripts. Version of 23 December 1993.

tripwire.tar The Tripwire package from Purdue University. Scans file systems and computes digital signatures for the files therein, then can be used later to check those files for any changes. Version 1.1.

watcher.tar The `Watcher` package by Kenneth Ingham. A configurable and extensible system monitoring tool that issues a number of user-specified commands, parses the output, checks for items of significance, and reports them to the system administrator. Version of 15 July 1991.

1.7.3.8. */software/unix/tools*

The ***/software/unix/tools*** directory contains programs that are not specifically designed for computer security uses, but are nevertheless useful to the security practitioner. The files in this directory are:

dig.tar The `dig` utility by Steve Hotz and Paul Mockapetris. This is a command-line tool for querying Domain Name System servers. It is much easier to use than `nslookup`, and is well-suited for use within shell scripts. Version 2.0.

fremont.tar The `fremont` utility from the University of Colorado. A research prototype for discovering key network characteristics such as hosts, gateways, and topology. Stores this information in a database, and can then notify the administrator of anomalies detected. Version 1.02.

gated.tar The `gated` program from Cornell University. A network routing daemon that understands the BGP, EGP, RIP, RIP II, OSPF, and HELLO protocols. The primary advantage to `gated` is that it is much more configurable than the `routed` program that comes with most UNIX systems; this can be useful when constructing firewalls or otherwise trying to limit the advertisement or acceptance of routing information. Version 3.0.3.

host.tar The `host` program by Eric Wassenaar. A program for obtaining information from the Domain Name System. Much more flexible than `nslookup`, and well-suited for use in shell scripts. Version of 23 June 1994.

lsof.tar The `lsof` program by Vic Abell. A descendant of `ofiles` and `fstat`, `lsof` is used to list all open files (and network connections, pipes, streams, etc.) on a system. Can find out which processes have a given file open, which files a specific process has open, and so forth. Useful for tracing network connections to the processes using them, as well. Version 3.02.

nfswatch.tar The `nfswatch` program by Dave Curry and Jeff Mogul. Monitors the local network for NFS packets, and decodes them by client and server name, procedure name, and so forth. Can be used to determine how much traffic each client is sending to a server, what users are accessing the server, and several other modes. Version 4.1.

rdist.tar The `rdist` program from the University of Southern California. This is a replacement for the `rdist` software distribution utility that originated in Berkeley UNIX and is now shipped with most vendors' releases. In addition to a number of wonderful new features and improvements, this version has had all known `rdist` security holes fixed. This version does not need to run set-user-id ‘‘root,’’ unlike the standard version. Version 6.1.0.

sendmail The `sendmail` program by Eric Allman. This subdirectory contains the `sendmail` source code, the documentation, and the sample configuration files. This version is a successor to the version described in the *sendmail* book from O'Reilly and Associates, and is much newer than the versions shipped by most UNIX vendors. In addition to a number of improvements and bug fixes, this version has all known `sendmail` security holes fixed. It is likely that this version of `sendmail` is more secure than the versions shipped by any UNIX vendor. Version 8.6.9.

tcpdump.tar The `tcpdump` program by Van Jacobson. This program is similar to Sun's `etherfind`, but somewhat more powerful and slightly easier to use. It captures packets from an Ethernet in promiscuous mode, and displays their contents. Numerous options exist to filter the output down to only those packets of interest. This version runs on a number of different UNIX platforms. Version 3.0.

tracert.tar The `traceroute` program by Van Jacobson. A utility to trace the route IP packets from the current system take in getting to some destination system. Version of 28 February 1989.

wuftpd.tar The `ftpd` program from Washington University. This version is designed for use by large FTP sites, and provides a number of features not found in vendor versions, including increased security. This is the `ftpd` used by most major FTP sites, including *wuarchive.wustl.edu*, *ftp.uu.net*, and *oak.oakland.edu*. **NOTE**: Releases of `wu-ftpd` prior to version 2.4 have a serious security hole in them, and should be replaced as soon as possible with the latest version. Version 2.4.

1.8. */teaminfo*

The ***/teaminfo*** directory contains information about and provided by the FIRST member teams. Includes advisories, articles, etc. The subdirectories of this directory are:

assist The United States Department of Defense Automated Systems Security Incident Response Team (ASSIST).

cert The DARPA Computer Emergency Response Team/Coordination Center (CERT/CC).

cert_it The Italian Computer Emergency Response Team at the University of Milan. (CERT-IT).

cert_nl The Netherlands (SURFnet) Computer Emergency Response Team (CERT-NL).

ciac The United States Department of Energy Computer Incident Advisory Capability. (CIAC).

ddnscc The United States Defense Information Systems Agency (DISA) Defense Data Network Security Coordination Center. (DDN SCC).

dfn_cert The German Research Network Computer Emergency Response Team. (DFN-CERT).

first The Forum of Incident Response and Security Teams (FIRST).

nasirc The NASA Automated Systems Incident Response Capability (NASIRC).

nist The United States National Institute of Standards and Technology Computer Security Resource Center (NIST CSRC).