Bibliography

A number of *RFC*s—*Requests for Comments*—are listed in the bibliography. They may be obtained by electronic mail or by anonymous FTP. For instructions, send mail to *rfc-info*@ISI.EDU with a message body of

```
help: ways_to_get_rfcs
```

For other documents, we have listed anonymous FTP repositories when we are aware of them. See Appendix A for instructions.

[Amoroso, 1994] E. Amoroso. *Fundamentals of Computer Security Technology*. Prentice-Hall, Englewood Cliffs, NJ, 1994. Cited on: *21, 81*.

[Anderson, 1993] Ross Anderson. Why cryptosystems fail. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 215–227, Fairfax, VA, November 1993. Cited on: *121*.

Describes how real-world failures of cryptographic protocols don't always match the classical academic models.

[Anklesaria *et al.*, 1993] Farhad Anklesaria, Mark McCahill, Paul Lindner, David Johnson, Daniel Torrey, and Bob Alberti. The Internet gopher protocol (A distributed document search and retrieval protocol). RFC 1436, March 1993. Cited on: *44*.

[ANSI, 1988] Information retrieval service definition and protocol specifications for library applications. Z39.50-1988, ANSI, 1988. Cited on: *107*.

This protocol is the basis for WAIS.

[Arkin *et al.*, 1992] Stanley S. Arkin, Barry A. Bohrer, John P. Donohue, Robert Kasanof, Donald L. Cuneo, Jeffrey M. Kaplan, Andrew J. Levander, and Sanford Sherizen. *Prevention and Prosecution of Computer and High Technology Crime*. Matthew Bender & Co., New York, 1992. Cited on: *202, 202*.

[Asimov, 1951] Isaac Asimov. *Foundation*. Doubleday & Company, New York, 1951. Cited on: *143*.

[Avolio and Ranum, 1994] Frederick Avolio and Marcus Ranum. A network perimeter with secure external access. In *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, San Diego, CA, February 3, 1994. Cited on: *31, 115, 122, 241*.

All the President's E-mail! A description of the firewall created for the Executive Office of the President, including mail support for *president*@WHITEHOUSE.GOV. Available from FTP.TIS.COM as `/pub/firewalls/isoc94.ps.Z`.

[Avolio and Vixie, 1994] Frederick M. Avolio and Paul Vixie. *Sendmail: Theory and Practice*. Digital Press, Burlington, MA, 1994. (To appear). Cited on: *30*.

[Balenson, 1993] David Balenson. Privacy enhancement for Internet electronic mail: Part III: Algorithms, modes, and identifiers. RFC 1423, February 1993. Cited on: *232*.

[BB, 1991] *The Bluebook: A Uniform System of Citation*. Harvard Law Review Association, 15th edition, 1991. Cited on: *198*.

[Bellovin, 1989] Steven M. Bellovin. Security problems in the TCP/IP protocol suite. *Computer Communications Review*, 19(2):32–48, April 1989. Cited on: *24, 24, 65, 67, 71, 141*.

Available by *ftp* from FTP.RESEARCH.ATT.COM in `/dist/internet_security/ipext.ps.Z`.

[Bellovin, 1990] Steven M. Bellovin. Pseudo-network drivers and virtual networks. In *USENIX Conference Proceedings*, pages 229–244, Washington, D.C., January 22-26, 1990. Cited on: *79*.

Available by anonymous *ftp* from FTP.RESEARCH.ATT.COM in `/dist/smb/pnet.ext.ps.Z`.

[Bellovin, 1993] Steven M. Bellovin. Packets found on an internet. *Computer Communications Review*, 23(3):26–31, July 1993. Cited on: *137, 137, 152, 193*.

Available by anonymous *ftp* from FTP.RESEARCH.ATT.COM in `/dist/smb/packets.ps`.

[Bellovin, 1994] Steven M. Bellovin. Firewall-friendly FTP. RFC 1579, February 1994. Cited on: *60*.

[Bellovin and Merritt, 1991] Steven M. Bellovin and Michael Merritt. Limitations of the Kerberos authentication system. In *USENIX Conference Proceedings*, pages 253–267, Dallas, TX, Winter 1991. Cited on: *223, 225, 236*.

Available by *ftp* from FTP.RESEARCH.ATT.COM in `/dist/internet_security/kerblimit.usenix.ps`.

[Bellovin and Merritt, 1992] Steven M. Bellovin and Michael Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *Proc. IEEE Computer Society Symposium on Research in Security and Privacy*, pages 72–84, Oakland, CA, May 1992. Cited on: *219, 226*.

Available by anonymous *ftp* from FTP.RESEARCH.ATT.COM in `/dist/smb/neke.ps`.

[Bellovin and Merritt, 1993] Steven M. Bellovin and Michael Merritt. Augmented encrypted key exchange. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 244–250, Fairfax, VA, November 1993. Cited on: *219*.

Available by anonymous *ftp* from FTP.RESEARCH.ATT.COM in `/dist/smb/aeke.ps`.

[Bellovin and Merritt, 1994] Steven M. Bellovin and Michael Merritt. An attack on the *Interlock Protocol* when used for authentication. *IEEE Transactions on Information Theory*, 40(1):273–275, January 1994. Cited on: *219*.

[Bender, 1992] David Bender. *Computer Law*, Volume 3. Matthew Bender & Co., New York, 1992. Cited on: *202*.

[Berners-Lee, 1993] Tim Berners-Lee. Uniform resource locators. Internet Draft, October 14, 1993. Work in progress. Cited on: *44*.

Available for *ftp* from the various `internet-drafts` directories around the Internet.

[Biham and Shamir, 1991] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991. Cited on: *216*.

[Biham and Shamir, 1993] Eli Biham and Adi Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, Berlin, 1993. Cited on: *216*.

[Bishop, 1990] Matt Bishop. A security analysis of the NTP protocol. In *Sixth Annual Computer Security Conference Proceedings*, pages 20–29, Tuscon, AZ, December 1990. Cited on: *33*.

Available for *ftp* from LOUIE.UDEL.EDU as `/pub/ntp/doc/bishop.ps.Z`.

[Bishop, 1992] Matt Bishop. Anatomy of a proactive password changer. In *Proceedings of the Third Usenix* UNIX *Security Symposium*, pages 171–184, Baltimore, MD, September 1992. Cited on: *12*.

[Blaze, 1993] Matt Blaze. A cryptographic file system for UNIX. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 9–16, Fairfax, VA, November 1993. Cited on: *107*.

Available from FTP.RESEARCH.ATT.COM as `/dist/mab/cfs.ps`.

[Blaze, 1994] Matt Blaze. Key management in an encrypting file system. In *Proc. Summer Usenix Conference*, pages 27–35, Boston, MA, June 1994. Cited on: *14*.

> Adding a smart card-based key escrow system to CFS [Blaze, 1993]. Available from RESEARCH.ATT.COM as `/dist/mab/cfskey.ps`.

[Borenstein and Freed, 1993] Nathaniel Borenstein and Ned Freed. MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for specifying and describing the format of internet message bodies. RFC 1521, September 1993. Cited on: *31*.

[Borman, 1993a] David Borman, editor. Telnet authentication: Kerberos version 4. RFC 1411, January 1993. Cited on: *231*.

[Borman, 1993b] David Borman, editor. Telnet authentication option. RFC 1416, February 1993. Cited on: *31, 231*.

[Braden, 1989a] Robert Braden, editor. Requirements for Internet hosts—application and support. RFC 1123, October 1989. Cited on: *29, 30*.

[Braden, 1989b] Robert Braden, editor. Requirements for Internet hosts—communication layers requirements for internet hosts communication layers. RFC 1122, October 1989. Cited on: *26*.

[Brickell *et al.*, 1993] Ernest F. Brickell, Dorothy E. Denning, Stephen T. Kent, David P. Maher, and Walter Tuchman. SKIPJACK review: The SKIPJACK algorithm, July 28, 1993. Interim Report. Cited on: *214*.

> The final report will discuss the security of the entire key escrow system, and not just the underlying cryptographic algorithm. It isn't clear when that report will be finished.

[Bryant, 1988] B. Bryant. Designing an authentication system: A dialogue in four scenes, February 8, 1988. Draft. Cited on: *8, 39, 223*.

> A light-hearted derivation of the requirements Kerberos was designed to meet.

[Callaghan and Lyon, 1989] Brent Callaghan and Tom Lyon. The automounter. In *USENIX Conference Proceedings*, pages 43–51, San Diego, CA, Winter 1989. Cited on: *107*.

[Campbell and Wiener, 1993] K. W. Campbell and M. J. Wiener. Proof that DES is not a group. In *Advances in Cryptology: Proceedings of CRYPTO '92*, pages 518–526, Santa Barbara, CA, 1993. Springer-Verlag. Cited on: *217*.

[Carson, 1993] Mark E. Carson. *Sendmail* without the superuser. In *Proceedings of the Fourth Usenix* UNIX *Security Symposium*, pages 139–144, Santa Clara, CA, October 1993. Cited on: *31*.

> A good example of retrofitting an existing program to use the principle of "least privilege."

[Case *et al.*, 1990] Jeffrey Case, Mark Fedor, Martin Schoffstall, and James Davin. Simple network management protocol (SNMP). RFC 1157, May 1990. Cited on: *138*, *231*.

[Chapman, 1992] D. Brent Chapman. Network (in)security through IP packet filtering. In *Proceedings of the Third Usenix* UNIX *Security Symposium*, pages 63–76, Baltimore, MD, September 1992. Cited on: *55*, *65*, *66*.

Shows how hard it is to set up secure rules for a packet filter. Available for *ftp* from FTP.GREATCIRCLE.COM as `/pub/firewalls/pkt_filtering.ps.Z`.

[Cheswick, 1992] William R. Cheswick. An evening with Berferd, in which a cracker is lured, endured, and studied. In *Proc. Winter USENIX Conference*, San Francisco, CA, January 1992. Cited on: *167*.

Available by *ftp* from FTP.RESEARCH.ATT.COM in `/dist/internet_security/berferd.ps`.

[Comer, 1991] Douglas E. Comer. *Internetworking with TCP/IP: Principles, Protocols, and Architecture*, Volume I. Prentice-Hall, Englewood Cliffs, NJ, second edition, 1991. Cited on: *19*.

A well-known description of the TCP/IP protocol suite.

[Comer and Stevens, 1994] Douglas E. Comer and David L. Stevens. *Internetworking with TCP/IP: Design, Implementation, and Internals*, Volume II. Prentice-Hall, Englewood Cliffs, NJ, second edition, 1994. Cited on: *19*.

How to implement TCP/IP.

[Cook and Crocker, 1993a] Jeff Cook and Stephen D. Crocker. Truffles—A secure service for widespread file sharing. TIS Report 484, Trusted Information Systems, Glenwood, MD, February 1993. Cited on: *81*.

[Cook and Crocker, 1993b] Jeff Cook and Stephen D. Crocker. Truffles—Secure file sharing with minimal system administrator intervention. TIS Report 485, Trusted Information Systems, Glenwood, MD, April 1993. Cited on: *81*.

[Cook *et al.*, 1993] Jeff Cook, Stephen D. Crocker, Thomas Page, Jr., Gerald Popek, and Peter Reiher. Truffles—A secure service for widespread file sharing. In *Workshop on Network and Distributed System Security*, San Diego, CA, February 1993. Cited on: *81*.

[Costales, 1993] Bryan Costales, with Eric Allman and Neil Rickert. *sendmail*. O'Reilly and Associates, Sebastopol, CA, 1993. Cited on: *30*, *30*.

[Crocker, 1982] David Crocker. Standard for the format of ARPA Internet text messages. RFC 822, 13 August 1982. Cited on: *30*.

[Curry, 1992] David A. Curry. UNIX *System Security: A Guide for Users and System Administrators*. Addison-Wesley, Reading, MA, 1992. Cited on: *xiii*.

[Davies and Price, 1989] Donald W. Davies and Wyn L. Price. *Security for Computer Networks*. John Wiley & Sons, second edition, 1989. Cited on: *122, 211*.

A guide to deploying cryptographic technology.

[Deering, 1989] Steve Deering. Host extensions for IP multicasting. RFC 1112, August 1989. Cited on: *46*.

[Denning, 1982] Dorothy E. Denning. *Cryptography and Data Security*. Addison-Wesley, Reading, MA, 1982. Cited on: *211*.

[Denning, 1993] Dorothy E. Denning. To tap or not to tap. *Communications of the ACM*, 36(3):26–33, March 1993. Cited on: *220*.

A defense of the U.S. government's key escrow initiative.

[Denning and Sacco, 1981] Dorothy E. Denning and Giovanni M. Sacco. Timestamps in key distribution protocols. *Communications of the ACM*, 24(8):533–536, August 1981. Cited on: *123, 223*.

Some weaknesses in [Needham and Schroeder, 1978].

[Diffie, 1988] Whitfield Diffie. The first ten years of public key cryptography. *Proceedings of the IEEE*, 76(5):560–577, May 1988. Cited on: *121*.

An exceedingly useful retrospective.

[Diffie and Hellman, 1976] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-11:644–654, November 1976. Cited on: *34, 218, 219, 225*.

The original paper on public-key cryptography. A classic.

[Diffie and Hellman, 1977] Whitfield Diffie and Martin E. Hellman. Exhaustive cryptanalysis of the NBS data encryption standard. *Computer*, 10(6):74–84, June 1977. Cited on: *216*.

The original warning about DES's key length being too short.

[DoD, 1985a] DoD trusted computer system evaluation criteria. DoD 5200.28-STD, DoD Computer Security Center, 1985. Cited on: *8, 162*.

The famous "Orange Book." Available for *ftp* from FTP.CERT.ORG as `/pub/info/orange-book.Z`.

[DoD, 1985b] Technical rationale behind CSC-STD-003-83: Computer security requirements. DoD CSC-STD-004-85, DoD Computer Security Center, 1985. Cited on: *8*.

A lesser known companion to the Orange Book [DoD, 1985a]. It describes how to select a security assurance level based on the data on the system and the risks to which it is exposed.

[Eichin and Rochlis, 1989] M. W. Eichin and J. A. Rochlis. With microscope and tweezers: An analysis of the Internet virus of november 1988. In *Proc. IEEE Symposium on Research in Security and Privacy*, pages 326–345, Oakland, CA, May 1989. Cited on: *30, 161, 198*.

Available by *ftp* from ATHENA-DIST.MIT.EDU in `/pub/virus/mit.PS`.

[Emtage and Deutsch, 1992] Alan Emtage and Peter Deutsch. *archie* — An electronic directory service for the internet. In *Proc. Winter Usenix Conference*, pages 93–110, San Francisco, January 1992. Cited on: *184*.

[Farmer and Spafford, 1990] Dan Farmer and Eugene H. Spafford. The COPS security checker system. In *USENIX Conference Proceedings*, pages 165–170, Anaheim, CA, Summer 1990. Cited on: *154, 244*.

A package to audit systems for vulnerabilities. This paper is available for anonymous *ftp* from FTP.CS.PURDUE.EDU as `/pub/spaf/security/COPS.PS.Z`.

[Farmer and Venema, 1993] Dan Farmer and Wietse Venema. Improving the security of your site by breaking into it. Available from FTP.WIN.TUE.NL, file `/pub/security/admin-guide-to-cracking.101.Z`, 1993. Cited on: *33, 149*.

[Farrow, 1991] Rik Farrow. UNIX *System Security: How to Protect Your Data and Prevent Intruders*. Addison-Wesley, Reading, MA, 1991. Cited on: *xiii*.

[Feldmeier and Karn, 1990] David C. Feldmeier and Philip R. Karn. UNIX password security—ten years later. In *Advances in Cryptology: Proceedings of CRYPTO '89*, pages 44–63. Springer-Verlag, 1990. Cited on: *12*.

[Flink and Weiss, 1988] Charles W. Flink II and Jonathan D. Weiss. System V/MLS labeling and mandatory policy alternatives. *AT&T Technical Journal*, 67(3):53–64, May/June 1988. Cited on: *22*.

[Flink and Weiss, 1989] Charles W. Flink II and Jonathan D. Weiss. System V/MLS labeling and mandatory policy alternatives. In *USENIX Conference Proceedings*, pages 413–427, San Diego, CA, Winter 1989. Cited on: *22*.

[Galvin *et al.*, 1992] James Galvin, Keith McCloghrie, and James Davin. SNMP security protocols. RFC 1352, July 1992. Cited on: *231*.

[Ganesan, 1994] Ravi Ganesan. BAfirewall: A modern design. In *Proceedings of the Internet Society Symposium on Network an d Distributed System Security*, San Diego, CA, February 3, 1994. Cited on: *78*.

A firewall that uses Kerberos to authenticate requests.

[Garfinkel and Spafford, 1991] Simson Garfinkel and Gene Spafford. *Practical Unix Security*. O'Reilly, Sebastopol, CA, 1991. Cited on: *xiii*.

[Garon and Outerbridge, 1991] Gilles Garon and Richard Outerbridge. DES Watch: An examination of the sufficiency of the data encryption standard for financial institution information security in the 1990's. *Cryptologia*, XV(3):177–193, July 1991. Cited on: *217*.

Gives the economics—and the economic impact—of cracking DES.

[Gavron, 1993] Ehud Gavron. A security problem and proposed correction with widely deployed DNS software. RFC 1535, October 1993. Cited on: *28*.

[Gemignani, 1989] Michael C. Gemignani. *A Legal Guide to EDP Management*. Quorum Books, New York, 1989. Cited on: *198, 208*.

[Gifford, 1982] David K. Gifford. Cryptographic sealing for information secrecy and authentication. *Communications of the ACM*, 25(4):274–286, 1982. Cited on: *14*.

[Gong *et al.*, 1993] Li Gong, Mark A. Lomas, Roger M. Needham, and Jerome H. Saltzer. Protecting poorly chosen secrets from guessing attacks. *IEEE Journal on Selected Areas in Communications*, 11(5):648–656, June 1993. Cited on: *159*, *164*.

[Grampp and Morris, 1984] Fred T. Grampp and Robert H. Morris. UNIX operating system security. *AT&T Bell Laboratories Technical Journal*, 63(8, Part 2):1649–1672, October 1984. Cited on: *xi*, *12, 130, 159, 183*.

[Haber and Stornetta, 1991a] S. Haber and W. S. Stornetta. How to time-stamp a digital document. In *Advances in Cryptology: Proceedings of CRYPTO '90*, pages 437–455. Springer-Verlag, 1991. Cited on: *201, 222*.

[Haber and Stornetta, 1991b] S. Haber and W. S. Stornetta. How to time-stamp a digital document. *Journal of Cryptology*, 3(2):99–112, 1991. Cited on: *201, 222*.

[Hafner and Markoff, 1991] Katie Hafner and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Simon & Schuster, New York, 1991. Cited on: *11, 114, 235*.

Background and personal information on three famous hacking episodes.

[Haller, 1994] Neil M. Haller. The S/Key one-time password system. In *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, San Diego, CA, February 3, 1994. Cited on: *122*.

An implementation of the scheme described in [Lamport, 1981].

[Hansen and Atkins, 1992] Stephen E. Hansen and E. Todd Atkins. Centralized system monitoring with *swatch*. In UNIX *Security III Symposium*, pages 105–117, Baltimore, MD, September 14–17, 1992. USENIX. Cited on: *139*.

[Harrenstien, 1977] Ken Harrenstien. NAME/FINGER protocol. RFC 742, December 30, 1977. Cited on: *33*.

[Harrenstien and White, 1982] Ken Harrenstien and Vic White. NICNAME/WHOIS. RFC 812, March 1, 1982. Cited on: *33*.

[Hedrick, 1988] Chuck Hedrick. Routing information protocol. RFC 1058, June 1988. Cited on: *27*.

[Hernandez, 1988] Ruel Torres Hernandez. ECPA and online computer privacy. *Federal Communications Law Journal*, 41(1):17–41, November 1988. Cited on: *205*.

[Hobbs, 1853] Alfred Charles Hobbs. *Rudimentary Treatise on the Construction of Locks*. Edited by Charles Tomlinson. J. Weale, London, 1853. Cited on: *143*.

[Holbrook and Reynolds, 1991] J. Paul Holbrook and Joyce Reynolds, editors. Site security handbook. RFC 1244, July 1991. Cited on: *4*.

[Honeyman *et al.*, 1992] P. Honeyman, L. B. Huston, and M. T. Stolarchuk. Hijacking afs. In *USENIX Conference Proceedings*, pages 175–182, San Francisco, CA, Winter 1992. Cited on: *39*.

A description of some security holes—now fixed—in AFS.

[Housley, 1993] Russell Housley. Security label framework for the Internet. RFC 1457, May 1993. Cited on: *21*.

[Howard, 1988] John H. Howard. On overview of the Andrew File System. In *USENIX Conference Proceedings*, pages 23–26, Dallas, TX, Winter 1988. Cited on: *38*.

[Ioannidis and Blaze, 1993] John Ioannidis and Matt Blaze. The architecture and implementation of network-layer security under unix. In *Proceedings of the Fourth Usenix* UNIX *Security Symposium*, pages 29–39, October 1993. Cited on: *229*.

Available from FTP.RESEARCH.ATT.COM as `/dist/mab/swipeusenix.ps`.

[ISO, 1987a] ISO. *Information Processing Systems – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)*, 1987. International Standard 8824. Cited on: *35*.

[ISO, 1987b] ISO. *Information Processing Systems – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*, 1987. International Standard 8825. Cited on: *35*.

[ISO, 1991] ISO. *Information Technology — Telecommunications and Information Exchange Between Systems — Transport Layer Security Protocol*, October 1991. Draft International Standard DIS 10736. Cited on: *227*.

[ISO, 1992] ISO. *Information Technology — Telecommunications and Information Exchange Between Systems — Network Layer Security Protocol*, November 1992. Draft International Standard DIS 11577. Cited on: *227*.

[Kahn, 1967] David Kahn. *The Code-Breakers*. Macmillan, New York, 1967. Cited on: *211*.

> The definitive work on the history of cryptography, and an introduction to classical cryptography. A must-read. But it does not discuss modern cryptographic techniques.

[Kahn, 1989] John R. Kahn. Defamation liability of computerized bulletin board operators and problems of proof. Available from LCS.MIT.EDU, file `/telecom-archives/sysop.libel.liability`, February 1989. CHTLJ Comment, Computer Law Seminar, Upper Division Writing. Cited on: *208*.

[Kaliski, 1992] Burt Kaliski. The MD2 message-digest algorithm. RFC 1319, April 1992. Cited on: *222, 247*.

[Kaliski, 1993] Burt Kaliski. Privacy enhancement for Internet electronic mail: Part IV: Key certification and related services. RFC 1424, February 1993. Cited on: *232*.

[Kantor and Lapsley, 1986] Brian Kantor and Phil Lapsley. Network news transfer protocol. RFC 977, February 1986. Cited on: *45*.

[Kaufman, 1993] Charles Kaufman. DASS distributed authentication security service. RFC 1507, September 1993. Cited on: *234*.

[Kazar, 1988] Michael Leon Kazar. Synchronization and caching issues in the andrew file system. In *USENIX Conference Proceedings*, pages 27–36, Dallas, TX, Winter 1988. Cited on: *38*.

[Keeton *et al.*, 1984] W. Page Keeton, Dan B. Dobbs, Robert E. Keeton, and David G. Owen. *Prosser and Keeton on Torts*. West Publishing Company, St. Paul, MN, fifth edition, 1984. Cited on: *206, 208*.

[Kent, 1991] Stephen Kent. Security options for the Internet protocol. RFC 1108, November 1991. Cited on: *21*.

[Kent, 1993] Stephen Kent. Privacy enhancement for Internet electronic mail: Part II: Certificate-based key management. RFC 1422, February 1993. Cited on: *232*.

[Kim and Spafford, 1993] Gene Kim and Eugene H. Spafford. The design and implementation of Tripwire: A file system integrity checker. Technical Report CSD-TR-93-071, Purdue University, 1993. Cited on: *111, 244*.

> A package to audit systems for vulnerabilities and evidence of hacking attacks. This paper is available for anonymous *ftp* from FTP.CS.PURDUE.EDU as `/pub/spaf/security/Tripwire.PS.Z`.

[Kim and Spafford, 1994a] Gene Kim and Eugene H. Spafford. Experiences with Tripwire: The evaluation and writing of a security tool, 1994. (In preparation). Cited on: *111, 244*.

[Kim and Spafford, 1994b] Gene Kim and Eugene H. Spafford. Experiences with Tripwire: Using integrity checkers for intrusion detection, 1994. (In preparation). Cited on: *111, 244*.

[Klein, 1990] Daniel V. Klein. "Foiling the cracker": A survey of, and improvements to, password security. In *Proceedings of the USENIX* UNIX *Security Workshop*, pages 5–14, Portland, OR, August 1990. Cited on: *11, 12, 14, 159*.

Describes the author's experiments cracking password files from many different machines.

[Koblas and Koblas, 1992] David Koblas and Michelle R. Koblas. Socks. In UNIX *Security III Symposium*, pages 77–83, Baltimore, MD, September 14-17, 1992. USENIX. Cited on: *77, 126, 240*.

A description of the most common circuit-level gateway package.

[Kohl and Neuman, 1993] John Kohl and Cliff Neuman. The Kerberos network authentication service (V5). RFC 1510, September 1993. Cited on: *8, 39, 223*.

[Korn and Krell, 1989] David G. Korn and Eduardo Krell. The 3-d file system. In *USENIX Conference Proceedings*, pages 147–156, Baltimore, MD, Summer 1989. Cited on: *77*.

[Lai, 1992] X. Lai. *On the Design and Security of Block Ciphers*, Volume 1 of *ETH Series in Information Processing*. Hartung-Gorre Verlag, Konstanz, Germany, 1992. Cited on: *214*.

[LaMacchia and Odlyzko, 1991] Brian A. LaMacchia and Andrew M. Odlyzko. Computation of discrete logarithms in prime fields. *Designs, Codes, and Cryptography*, 1:46–62, 1991. Cited on: *34, 164*.

Describes how the authors cryptanalyzed Secure RPC.

[Lamport, 1981] Leslie Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, November 1981. Cited on: *121, 241, 264*.

The basis for the Bellcore S/Key system.

[LeFebvre, 1992] William LeFebvre. Restricting network access to system daemons under SunOS. In UNIX *Security III Symposium*, pages 93–103, Baltimore, MD, September 14-17, 1992. USENIX. Cited on: *77, 240*.

Using shared libraries to provide access control for standing servers.

[Leong and Tham, 1991] Philip Leong and Chris Tham. UNIX password encryption considered insecure. In *Proc. Winter USENIX Conference*, Dallas, TX, 1991. Cited on: *12, 159*.

How to build a hardware password-cracker.

[Libes, 1991] Don Libes. *expect*: Scripts for controlling interactive processes. *Computing Systems*, 4(2):99–126, Spring 1991. Cited on: *149*.

[Linn, 1993a] John Linn. Generic security service application program interface. RFC 1508, September 1993. Cited on: *233*.

[Linn, 1993b] John Linn. Privacy enhancement for Internet electronic mail: Part I: Message encryption and authentication procedures. RFC 1421, February 1993. Cited on: *232*.

[Lloyd and Simpson, 1992] Brian Lloyd and William Simpson. PPP authentication protocols. RFC 1334, October 1992. Cited on: *235*.

[Lomas *et al.*, 1989] T. Mark A. Lomas, Li Gong, Jerome H. Saltzer, and Roger M. Needham. Reducing risks from poorly chosen keys. In *Proceedings of the Twelfth ACM Symposium on Operating Systems Principles*, pages 14–18. SIGOPS, December 1989. Cited on: *226*.

[Lottor, 1987] Mark Lottor. Domain administrators operations guide. RFC 1033, November 1987. Cited on: *27*.

[Lottor, 1988] Mark Lottor. TCP port service multiplexer (TCPMUX). RFC 1078, November 1988. Cited on: *64, 193*.

[MacAvoy, 1983] R. A. MacAvoy. *Tea with the Black Dragon*. Bantam Books, New York, 1983. Cited on: *160*.

A science fiction story of a rather different flavor.

[Machiavelli, 1950] Niccolò Machiavelli. *The Prince and The Discourses*. Random House, New York, modern library edition, 1950. Cited on: *239*.

A classic work on political philosophy—and it isn't all "Machiavellian."

[Malkin, 1993] Gary Malkin. RIP version 2—carrying additional information. RFC 1388, January 1993. Cited on: *27*.

[Markoff, 1989] John Markoff. Computer invasion: 'back door' ajar. In *New York Times*, Volume CXXXVIII, page B10, November 7, 1989. Cited on: *30*.

[Markoff, 1991] John Markoff. Move on unscrambling of messages is assailed. In *New York Times*, Volume CXL, page A16, April 17, 1991. Cited on: *220*.

[Markoff, 1993a] John Markoff. Communications plan to balance government access with privacy. In *New York Times*, Volume CXLII, page A1, April 16, 1993. Cited on: *214*.

[Markoff, 1993b] John Markoff. Keeping things safe and orderly in the neighborhood of cyberspace. In *New York Times*, Volume CXLIII, page E7, October 24, 1993. Cited on: *15*.

[Maryland Hacker, 1993] A Maryland Hacker. Telco UNIX trap. *2600*, pages 30–31, Autumn 1993. (letter to the editor). Cited on: *128*.

A correct—but incomplete—discussion on the limitations of `chroot` environments.

[Merkle, 1990a] Ralph C. Merkle. A fast software one-way hash function. *Journal of Cryptology*, 3(1):43–58, 1990. Cited on: *111, 111, 222*.

[Merkle, 1990b] Ralph C. Merkle. One way hash functions and DES. In *Advances in Cryptology: Proceedings of CRYPTO '89*, pages 428–446. Springer-Verlag, 1990. Cited on: *222*.

[Merkle and Hellman, 1981] Ralph C. Merkle and Martin Hellman. On the security of multiple encryption. *Communications of the ACM*, 24(7):465–467, July 1981. Cited on: *217*.

[Miller *et al.*, 1987] S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer. Kerberos authentication and authorization system. In *Project Athena Technical Plan*. MIT, December 1987. Section E.2.1. Cited on: *8, 39, 223*.

[Mills, 1992] David Mills. Network time protocol (version 3) specification, implementation and analysis. RFC 1305, March 1992. Cited on: *32*.

[Mitchell and Walker, 1988] Chris Mitchell and Michael Walker. Solutions to the multidestination secure electronic mail problem. *Computers & Security*, 7(5):483–488, 1988. Cited on: *222*.

[Mockapetris, 1987a] Paul Mockapetris. Domain names—concepts and facilities. RFC 1034, November 1987. Cited on: *27*.

[Mockapetris, 1987b] Paul Mockapetris. Domain names—implementation and specification. RFC 1035, November 1987. Cited on: *27*.

[Mogul, 1989] Jeffrey C. Mogul. Simple and flexible datagram access controls for UNIX-based gateways. In *USENIX Conference Proceedings*, pages 203–221, Baltimore, MD, Summer 1989. Cited on: *57, 74, 242*.

A description of one of the first packet filters. The original paper is available as Research Report 89/4; send mail to *wrl-techreports*@WRL.PA.DEC.COM with "`Subject: help`" for ordering information. Also see [Mogul, 1991].

[Mogul, 1991] Jeffrey C. Mogul. Using *screend* to implement IP/TCP security policies. Network Note NN-16, Digital Equipment Corp. Network Systems Laboratory, July 1991. To find out how to order a copy, send email to nsl-techreports@nsl.pa.dec.com with "`Subject: help`". Cited on: *74, 269*.

A longer version of [Mogul, 1989], with some worked examples.

[Moore, 1988] J. H. Moore. Protocol failures in cryptosystems. *Procedings of the IEEE*, 76(5):594–602, May 1988. Cited on: *211*.

[Morris and Thompson, 1979] Robert H. Morris and Ken Thompson. UNIX password security. *Communications of the ACM*, 22(11):594, November 1979. Cited on: *11, 12, 159, 225*.

Gives the rationale for the design of the current UNIX password hashing algorithm.

[Morris, 1985] Robert T. Morris. A weakness in the 4.2BSD UNIX TCP/IP software. Computing Science Technical Report 117, AT&T Bell Laboratories, Murray Hill, NJ, February 1985. Cited on: *24, 141*.

The original paper describing sequence number attacks. Available for *ftp* from NETLIB.ATT.COM as `/netlib/research/cstr/117.Z`.

[Moy, 1991] John Moy. OSPF version 2. RFC 1247, July 1991. Cited on: *27*.

[Muffett, 1992] Alec D. E. Muffett. A sensible password checker for UNIX, 1992. Cited on: *12, 149*.

Available with the *Crack* package.

[Nat, 1979] National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration, U.S. Department of Justice. *Computer Crime: Criminal Justice Resource Manual*, 1979. Cited on: *201*.

[NBS, 1977] NBS. Data encryption standard, January 1977. Federal Information Processing Standards Publication 46. Cited on: *34, 212*.

The original DES standard. It's a bit hard to get, and most recent books on cryptography explain DES much more clearly. See, for example, [Schneier, 1994].

[NBS, 1980] NBS. DES modes of operation, December 1980. Federal Information Processing Standards Publication 81. Cited on: *212*.

The four officially approved ways in which DES can be used. Clearer explanations are available in most recent books on cryptography.

[Nechvatal, 1992] James Nechvatal. Public key cryptography. In Gustavus J. Simmons, editor, *Contemporary Cryptology: The Science of Information Integrity*, pages 177–288. IEEE Press, Piscataway, NJ, 1992. Cited on: *222*.

[Needham and Schroeder, 1978] R. M. Needham and M. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, December 1978. Cited on: *123, 223, 262*.

The first description of a cryptographic authentication protocol. Also see [Denning and Sacco, 1981] and [Needham and Schroeder, 1987].

[Needham and Schroeder, 1987] R. M. Needham and M. Schroeder. Authentication revisited. *Operating Systems Review*, 21(1):7, January 1987. Cited on: *123, 223, 270*.

[NIST, 1993] NIST. Secure hash standard (SHS), May 1993. Federal Information Processing Standards Publication 180. Cited on: *222*.

The algorithm is also described in [Schneier, 1994]. The original version has been recalled by NSA; a new version incorporates a one-line fix.

[NIST, 1994a] NIST. Digital signature standard (DSS), May 1994. Federal Information Processing Standards Publication 186. Cited on: *220*.

The algorithm is also described in [Schneier, 1994].

[NIST, 1994b] NIST. Escrowed encryption standard, February 1994. Federal Information Processing Standards Publication 185. Cited on: *214*.

The actual encryption algorithm is classified, and is not described in this publication.

[Niven, 1968] Larry Niven. Flatlander. In *Neutron Star*, pages 129–171. Ballantine Books, New York, NY, 1968. Cited on: *6*.

[Nycum, 1983] Susan H. Nycum. Legal exposures for computer abuse. In Daniel T. Brooks and Susan H. Nycum, editors, *Computer Crime: • Prevention • Detection • Prosecution •*, pages 19–31. Law & Business, New York, NY, 1983. Cited on: *207*.

[Pendry, 1989] Jan-Simon Pendry. `Amd` — An automounter, 1989. Department of Computing, Imperial College, London. Cited on: *107*, *192*.

Packaged with the *amd* automounter.

[Pike *et al.*, 1990] Rob Pike, David L. Presotto, Ken Thompson, and Howard Trickey. Plan 9 from Bell Labs. In *Proceedings of the Summer 1990 UKUUG Conference*, pages 1–9, London, July 1990. UKUUG. Cited on: *98*.

Documentation on Plan 9 can be found on FTP.RESEARCH.ATT.COM in `/dist/plan9doc` and `/dist/plan9man`.

[Piscitello and Chapin, 1994] David M. Piscitello and A. Lyman Chapin. *Open Systems Networking: TCP/IP and OSI*. Addison-Wesley, Reading, MA, 1994. Cited on: *26*.

[Plummer, 1982] David Plummer. Ethernet address resolution protocol: Or converting network protocol addresses to 48-bit ethernet address for transmission on ethernet hardware. RFC 826, November 1982. Cited on: *22*.

[Postel, 1980] Jon Postel. User datagram protocol. RFC 768, 28 August 1980. Cited on: *25*.

[Postel, 1981a] Jon Postel. Internet control message protocol. RFC 792, September 1981. Cited on: *25*.

[Postel, 1981b] Jon Postel. Internet protocol. RFC 791, September 1981. Cited on: *19*.

[Postel, 1981c] Jon Postel. Transmission control protocol. RFC 793, September 1981. Cited on: *22*.

[Postel, 1982] Jon Postel. Simple mail transfer protocol. RFC 821, August 1982. Cited on: *29*.

[Postel and Reynolds, 1985] Jon Postel and Joyce Reynolds. File transfer protocol. RFC 959, October 1985. Cited on: *39*.

[Presotto, 1985] David L. Presotto. *Upas*—a simpler approach to network mail. In *USENIX Conference Proceedings*, pages 533–538, Portland, OR, Summer 1985. Cited on: *30*.

[Presotto and Ritchie, 1985] David L. Presotto and Dennis M. Ritchie. Interprocess communication in the eighth edition unix system. In *USENIX Conference Proceedings*, pages 309–316, Portland, OR, Summer 1985. Cited on: *125*.

[Rago, 1990] Stephen Rago. A look at the Ninth Edition Network File System. In A. G. Hume and M. D. McIlroy, editors, UNIX *Research System: Papers*, Volume II, pages 513–522. AT&T Bell Laboratories, Murray Hill, NJ, tenth edition, 1990. Cited on: *81*, *108*.

[Ranum, 1992] Marcus J. Ranum. A network firewall. In *Proc. World Conference on System Administration and Security*, Washington, D.C., July 1992. Cited on: *75*.

A description of Digital's firewall.

[Reiher *et al.*, 1993] Peter Reiher, Jeff Cook, Thomas Page, Jr., Gerald Popek, and Stephen D. Crocker. Truffles—Secure file sharing with minimal system administrator intervention. In *World Conference On System Administration, Networking, and Security*, Arlington, VA, 1993. Cited on: *81*.

[Rekhter *et al.*, 1994] Yakov Rekhter, Robert G. Moskowitz, Daniel Karrenberg, and Geert Jan de Groot. Address allocation for private internets. RFC 1597, March 1994. Cited on: *73*.

[Riordan, 1992] Mark Riordan. RIPEM user's guide, December 1992. Cited on: *233*.

Available with the RIPEM package, but not export-restricted.

[Rivest, 1992] Ronald Rivest. The MD5 message-digest algorithm. RFC 1321, April 1992. Cited on: *222*, *247*.

[Rivest and Shamir, 1984] Ronald L. Rivest and Adi Shamir. How to expose an eavesdropper. *Communications of the ACM*, 27(4):393–395, 1984. Cited on: *219*.

[Rivest *et al.*, 1978] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method of obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978. Cited on: *218*.

The original RSA paper.

[Rochlis and Eichin, 1989] J. A. Rochlis and M. W. Eichin. With microscope and tweezers: The worm from MIT's perspective. *Communications of the ACM*, 32(6):689–703, June 1989. Cited on: *30*, *161*, *198*.

There are several other stories on the Worm in this issue of CACM.

[Rose, 1991] Lance Rose. Cyberspace and the legal matrix: Laws or confusion. Available from FTP.EFF.ORG, file `/pub/EFF/legal-issues/cyberspace-legal-matrix`, February 1991. Cited on: *205*.

[Rosenberry *et al.*, 1992] Ward Rosenberry, David Kenney, and Gerry Fisher. *Understanding DCE*. O'Reilly and Associates, Sebastopol, CA, 1992. Cited on: *35*.

[Safford *et al.*, 1993a] David R. Safford, David K. Hess, and Douglas Lee Schales. Secure RPC authentication (SRA) for TELNET and FTP. In *Proceedings of the Fourth Usenix* UNIX *Security Symposium*, pages 63–67, Santa Clara, CA, October 1993. Cited on: *31, 35*.

[Safford *et al.*, 1993b] David R. Safford, Douglas Lee Schales, and David K. Hess. The TAMU security package: An ongoing response to Internet intruders in an academic environment. In *Proceedings of the Fourth Usenix* UNIX *Security Symposium*, pages 91–118, Santa Clara, CA, October 1993. Cited on: *32, 74, 137, 168, 190, 244*.

A detailed look at a hacker's activities in a university environment—and what they did to stop them. The paper is available for *ftp* as part of the TAMU security package.

[Samuelson, 1989] Pamela Samuelson. Can hackers be sued for damages caused by computer viruses? *Communications of the ACM*, 32(6), June 1989. Cited on: *197*.

[Scheifler and Gettys, 1992] Robert W. Scheifler and James Gettys. *X Window System*. Digital Press, Burlington, MA, third edition, 1992. Cited on: *47*.

[Schneier, 1994] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, New York, 1994. Cited on: *211, 270, 270, 271*.

A comprehensive collection of cryptographic algorithms, protocols, etc. Source code is included for many of the most important algorithms.

[Shamir, 1979] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979. Cited on: *14*.

[Shannon, 1948] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3,4):379–423,623–656, July, October 1948. Cited on: *12*.

[Shannon, 1949] Claude E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28:656–715, October 1949. Cited on: *12*.

[Shannon, 1951] Claude E. Shannon. Prediction and entropy in printed English. *Bell System Technical Journal*, 30(1):50–64, 1951. Cited on: *12*.

One of the classic papers in information theory.

[Sieber, 1986] Ulrich Sieber. *The International Handbook on Computer Crime: Computer-related Economic Crime and the Infringements of Privacy*. John Wiley & Sons, New York, 1986. Cited on: *197, 202*.

[Simpson, 1992] William Simpson. The point-to-point protocol (PPP) for the transmission of multi-protocol datagrams over point-to-point links. RFC 1331, May 1992. Cited on: *80*.

[Smith, 1953] E. E. “Doc” Smith. *Second Stage Lensman*. Pyramid Communications, New York, 1953. Cited on: *82*.

[SP3, 1988] SDNS secure data networking system security protocol 3 (SP3). Technical Report Revision 1.3, SDNS Protocol and Signalling Working Group, SP3 Sub-Group, July 12 1988. Cited on: *227*.

[SP4, 1988] SDNS secure data networking system security protocol 4 (SP4). Technical Report Revision 1.2, SDNS Protocol and Signalling Working Group, SP4 Sub-Group, July 12 1988. Cited on: *227*.

[Spafford, 1989a] Eugene H. Spafford. An analysis of the Internet worm. In C. Ghezzi and J. A. McDermid, editors, *Proc. European Software Engineering Conference*, number 387 in Lecture Notes in Computer Science, pages 446–468, Warwick, England, September 1989. Springer-Verlag. Cited on: *30, 161, 198*.

> The timeline and effects of the Worm.. This paper is available for anonymous *ftp* from FTP.CS.PURDUE.EDU as `/pub/spaf/security/IWorm2.PS.Z`.

[Spafford, 1989b] Eugene H. Spafford. The Internet worm program: An analysis. *Computer Communication Review*, 19(1):17–57, January 1989. Cited on: *30, 161, 198*.

> A detailed description of how the Worm worked. This paper is available for anonymous *ftp* from FTP.CS.PURDUE.EDU as `/pub/spaf/security/IWorm.PS.Z`.

[Spafford, 1992a] Eugene H. Spafford. Observations on reusable password choices. In *Proceedings of the Third Usenix* UNIX *Security Symposium*, pages 299–312, Baltimore, MD, September 1992. Cited on: *159*.

> Analysis of user password selections based on actual recorded choices. The discussion of how the recorded passwords were protected from hackers is especially interesting. This paper is available for anonymous *ftp* from FTP.CS.PURDUE.EDU as `/pub/spaf/security/observe.PS.Z`.

[Spafford, 1992b] Eugene H. Spafford. OPUS: Preventing weak password choices. *Computers & Security*, 11(3):273–278, 1992. Cited on: *12*.

> Discusses how to use Bloom filters to check passwords against dictionaries without consuming large amounts of space. This paper is available for anonymous *ftp* from FTP.CS.PURDUE.EDU as `/pub/spaf/security/opus.PS.Z`.

[St. Johns, 1985] Michael St. Johns. Authentication server. RFC 931, January 1985. Cited on: *141*.

[St. Johns, 1993] Michael St. Johns. Identification protocol. RFC 1413, February 1993. Cited on: *138, 141*.

[Stahl, 1987] Mary Stahl. Domain administrators guide. RFC 1032, November 1987. Cited on: *27*.

[Steiner *et al.*, 1988] Jennifer Steiner, B. Clifford Neuman, and Jeffrey I. Schiller. Kerberos: An authentication service for open network systems. In *Proc. Winter USENIX Conference*, pages 191–202, Dallas, TX, 1988. Cited on: *8, 39, 223*.

The original Kerberos paper. Available as part of the Kerberos distribution.

[Sterling, 1992] Bruce Sterling. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Bantam Books, New York, 1992. Cited on: *xiii*.

A description of how law enforcement agents went overboard, though often in response to real threats.

[Stevens, 1990] W. Richard Stevens. UNIX *Network Programming*. Prentice-Hall, Englewood Cliffs, NJ, 1990. Cited on: *25*.

[Stevens, 1994] W. Richard Stevens. *TCP/IP Illustrated*, Volume 1. Addison-Wesley, Reading, MA, 1994. Cited on: *19*.

Uses *tcpdump* to show *how* the protocols work.

[Stoll, 1988] Cliff Stoll. Stalking the wily hacker. *Communications of the ACM*, 31(5):484, May 1988. Cited on: *128, 142, 173, 208*.

[Stoll, 1989] Cliff Stoll. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Doubleday, New York, 1989. Cited on: *128, 142, 173, 208*.

A good read, and the basis for an episode of Nova.

[Sun Microsystems, 1987] Sun Microsystems. XDR: External data representation standard. RFC 1014, June 1987. Cited on: *35*.

[Sun Microsystems, 1988] Sun Microsystems. RPC: Remote procedure call protocol specification: Version 2. RFC 1057, June 1988. Cited on: *34, 64*.

[Sun Microsystems, 1989] Sun Microsystems. NFS: Network file system protocol specification. RFC 1094, March 1989. Cited on: *37*.

[Sun Microsystems, 1990] Sun Microsystems. *Network Interfaces Programmer's Guide*. Mountain View, CA, March 1990. SunOS 4.1. Cited on: *34, 37, 64*.

[Tolkien, 1965] J. R. R. Tolkien. *Lord of the Rings*. Ballantine Books, New York, 1965. Cited on: *11, 119, 237*.

[Treese and Wolman, 1993] Win Treese and Alec Wolman. X through the firewall, and other application relays. In *USENIX Conference Proceedings*, pages 87–99, Cincinnati, OH, June 1993. Cited on: *106, 241*.

[Tsudik, 1992] Gene Tsudik. Message authentication with one-way hash functions. In *Proceedings of IEEE Infocom '92*, Florence, Italy, May 1992. Cited on: *221*.

[Venema, 1992] Wietse Venema. TCP WRAPPER: Network monitoring, access control and booby traps. In *Proceedings of the Third Usenix* UNIX *Security Symposium*, pages 85–92, Baltimore, MD, September 1992. Cited on: *92*.

> A very important paper. Available for *ftp* from FTP.WIN.TUE.NL as `/pub/security/tcp_wrapper.ps.Z`.

[Violino, 1993] Bob Violino. Cover story: Hackers. *Information Week*, (430):48–56, June 21, 1993. Cited on: *154*.

> A discussion of the wisdom and prevalence of hiring hackers as security experts.

[Voydock and Kent, 1983] V. L. Voydock and S. T. Kent. Security mechanisms in high-level network protocols. *ACM Computing Surveys*, 15(2):135–171, June 1983. Cited on: *215*.

[Waitzman, 1990] David Waitzman. Standard for the transmission of IP datagrams on avian carriers. RFC 1149, April 1, 1990. Cited on: *80*.

[Wiener, 1994] Michael J. Wiener. Efficient DES key search. Technical Report TR-244, School of Computer Science, Carleton University, Ottawa, Canada, May 1994. Presented at the Rump Session of Crypto '93. Cited on: *217*.

[Winternitz, 1984] Robert S. Winternitz. Producing a one-way hash function from DES. In *Advances in Cryptology: Proceedings of CRYPTO '83*, pages 203–207. Plenum Press, 1984. Cited on: *222*.

[Wood *et al.*, 1993] David C. M. Wood, Sean S. Coleman, and Michael F. Schwartz. Fremont: A system for discovering network characteristics and problems. In *USENIX Technical Conference Proceedings*, pages 335–347, San Diego, CA, Winter 1993. Cited on: *147*.

[Woodward and Bernstein, 1974] Carl Woodward and Robert Bernstein. *All the President's Men*. Simon and Schuster, New York, 1974. Cited on: *165*.

[Wray, 1993] John Wray. Generic security service API : C-bindings. RFC 1509, September 1993. Cited on: *233*.

[Zimmerman, 1992] Philip Zimmerman. PGP user's guide, September 1992. Cited on: *233*.

> Available with the PGP package.