BIBLIOGRAPHY

Important articles and papers in this field are often reprinted, and this section notes alternative sources for the article when known. However, each entry in this list is only as complete as it needs to be. When an entry contains a partial reference to another publication, look for that publication's entry here for the full citation. If the entry refers to a vendor or Web site, check the **Web and Vendor Resources** section for contact information.

Abrams, Marshall D., and Harold J. Podell, eds., *Tutorial: Computer and Network Security* (Los Angeles: IEEE Computer Society Press, 1986).

Alberts, Christopher, and Audrey Dorofee, "An Introduction to the OCTAVE Method," white paper (Pittsburgh, PA: Software Engineering Institute of Carnegie Mellon University, 30 January 2001). Posted on the CERT Web site.

Alexander, Christopher, Sara Ishikawa, and Murray Silverstein, with Max Jacobson, Ingrid Fiksdahl-King, and Shlomo Angel, *A Pattern Language: Towns, Buildings, Construction* (New York: Oxford University Press, 1977).

Allison, Jeremy, "Windows NT Password Dump Utility" software README file, March 1997. Posted on the Samba Web site.

Anastasia, George, "Scarfo Case Could Test Cyber-Spying Tactic," *Philadelphia Inquirer* (4 December 2000).

Anderson, Ross J., "Why Cryptosystems Fail," *Communications of the ACM* 37, no. 11 (November 1994). Reprinted in *Practical Cryptography for Data Internetworks,* edited by William Stallings.

———, *Security Engineering: A Guide to Building Dependable Distributed Systems* (New York: John Wiley & Sons, 2001).

———, and Markus Kuhn, "Tamper Resistance—A Cautionary Note," *Proceedings of the Second USENIX Workshop on Electronic Commerce* (Berkeley, CA: USENIX Association, 1996), pp. 1–11.

Anonymous [pseudonym], *Maximum Linux Security* (Indianapolis, IN: Sams Publishing, 2000).

———, *Maximum Security,* 2nd edition (Indianapolis, IN: Sams Publishing, 1998).

Apple, "Mac OS 9: File Security—Choosing a Good Password," Tech Info Library Article ID 60483 (Cupertino, CA: Apple, 20 October 1999). This is posted on the Apple Web site.

———, "Technical Note TN1176: Mac OS 9," (Cupertino, CA: Apple, 24 April 2000). This is posted on the Apple Web site.

———, "Mac OS 9.1 Specification Sheet," Item L12404A (Cupertino, CA: Apple, January 2001). This is posted on the Apple Web site.

———, "Mac OS X Specification Sheet," Item L13291A (Cupertino, CA: Apple, March 2001). This document is posted on the Apple Web site.

———, "56 Bits?????" by various authors, Apple Mailing List Archives, 26–27 October 1999.

Atkins, D., M. Graff, A. K. Lenstra, and P. C. Leyland, "The Magic Words Are Squeamish Ossifrage," in *Advances in Cryptology—ASIACRYPT '94 Proceedings* (Heidelberg: Springer-Verlag, 1995).

Atkinson, Randall, "IP Authentication Header," Internet RFC 1826, August 1995. Posted on the IETF Web site.

Beavan, Colin, *Fingerprints: The Origin of Crime Detection and the Murder Case That Launched Forensic Science* (New York: Hyperion, 2001).

Bell, C. Gordon, J. Craig Mudge, and John E. MacNamara, *Computer Engineering: A DEC View of Hardware Systems Design* (Maynard, MA: Digital Press, 1978).

Bellare, M., R. Canetti, and H. Krawczyk, "Keyed Hash Functions and Message Authentication," *Proceedings of Crypto'96, Lecture Notes in Computer Science* 1109, (Heidelberg: Springer-Verlag, 1996), pp. 1–15.

Bellovin, Steven, "Security Problems in the TCP/IP Protocol Suite," *Computer Communication Review* 19, no. 2, pp. 32–48 (April 1989).

———, and Michael Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," *Proceedings of the 1992 IEEE Symposium or Research in Security and Privacy* (Piscataway, NJ: IEEE Press, 1992).

———, and Michael Merritt, "Limitations of the Kerberos Authentication System," *Proceedings of Winter '91 USENIX* (Berkeley, CA: USENIX Association, 1991). An earlier version appeared in *Computer Communications Review*, October 1990.

Biham, E., and P. C. Kocher, "A Known Plaintext Attack on PKZIP Encryption," in *K. U. Leuven Workshop on Cryptographic Algorithms* (Heidelberg: Springer-Verlag, 1995).

Biryukov, Alex, Adi Shamir, and David Wagner, "Real Time Cryptanalysis of A5/1 on a PC," Fast Software Encryption Workshop 2000, New York, NY, April 2000. Posted on the Cryptome Web site.

Blaauw, Gerrit A., and Frederick P. Brooks, Jr., *Computer Architecture: Concepts and Evolution* (Reading, MA: Addison-Wesley, 1997).

Blair, Bruce G., *The Logic of Accidental Nuclear War* (Washington, DC: The Brookings Institution, 1993).

Blaze, Matt, "Protocol Failure in the Escrowed Encryption Standard," research report (New Jersey: AT&T Bell Laboratories, 20 May 1994).

Blaze, Matt, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Weiner, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security," white paper, January 1996. Posted on the Counterpane Web site.

Boebert, W. Earl, and Chuck Nove, "Technical Report for the Tessera Authentication Protocol Specification Program," CDRL B001, Contract MDA904-92-C-0284 (Roseville, MN: Secure Computing Corporation, 1994).

Bolt, Beranek, and Newman, Inc., "Interface Message Processor—Specifications for the Interconnection of a Host and IMP," BBN Report 1822 (Cambridge, MA: Bolt, Beranek, and Newman, May 1978).

Bosen, Bob, "When Passwords Are Not Enough," white paper (Roseville, MN: Secure Computing Corporation, 1996). Posted on the SafeWord Web site.

Branstad, Dennis, "Encryption protection in computer data communications," *Proceedings of the 4th Data Communications Symposium* (New York: Association for Computing Machinery, 1975).

Bryant, Bill, "Designing an Authentication System: a Dialogue in Four Scenes," white paper from MIT Project Athena, 8 February 1988. Distributed on the FIRST CD-ROM.

Carlton, Steven, John Taylor, and John Wyszynski, "Alternate Authentication Mechanisms," *Proceedings of the 11th National Computer Security Conference* (Washington, DC: National Bureau of Standards, 1988).

Carrel, Dave, and Lol Grant, "TACACS+ Protocol Specification," Revision 1.78, January 1997. This has been distributed as an Internet Draft.

Carter, Ashton B., John D. Steinbruner, and Charles A. Zraket, eds., *Managing Nuclear Operations* (Washington, DC: The Brookings Institution, 1987).

Cavoukian, Ann, "Privacy and Biometrics: An Oxymoron or Time to Take a 2nd Look?" presented at Computers, Freedom and Privacy 98, Austin Texas. Posted on the Information Privacy Commissioner/Ontario Web site.

CERT, "Advisory CA-1990-03: Unisys U5000 /etc/passwd problem," issued 7 May 1990; last revised: 17 September 1997. Posted on the CERT Web Site.

———, "Advisory CA-1991-03: Unauthorized Password Change Requests Via Mail Messages," issued 4 April 1991; last revised: 18 September 1997. Posted on the CERT Web Site.

———, "Advisory CA-1992-14 Altered System Binaries Incident," issued 22 June 1992; last revised: 19 September 1997. Posted on the CERT Web Site.

———, "Advisory CA-1994-01: Ongoing Network Monitoring Attacks," issued 3 February 1994; last revised: 19 September 1997. Posted on the CERT Web Site.

———, "Advisory CA-1995-01: Spoofing Attacks and Hijacked Terminal Connections," issued 23 January 1995; last revised: 23 September 1997. Posted on the CERT Web Site.

———, "Advisory CA-1995-06: Security Administrator Tool for Analyzing Networks (SATAN)," issued 3 April 1995; last revised: 23 September 1997. Posted on the CERT Web Site.

———, "Advisory CA-1996-21: TCP SYN Flooding and IP Spoofing Attacks," issued 19 September 1996; last revised: 29 November 2000. Posted on the CERT Web Site.

———, "Advisory CA-1998-03: Vulnerability in ssh-agent," issued 22 January 1998; last revised: 2 March 1998. Posted on the CERT Web Site.

———, "Advisory CA-1999-04: Melissa Macro Virus," issued 27 March 1999; last revised: 31 March 1999. Posted on the CERT Web Site.

———, "Advisory CA-1999-17: Denial-of-Service Tools," issued 28 December 1999; last revised: 3 March 2000. Posted on the CERT Web Site.

———, "Advisory CA-2001-01: Interbase Server Contains Compiled-in Back Door Account," issued 10 January 2001; last revised: 11 January 2001. Posted on the CERT Web Site.

———, "Advisory CA-2001-09: Statistical Weaknesses in TCP/IP Initial Sequence Numbers," issued 1 May 2001. Posted on the CERT Web Site.

Cheswick, William R., and Steven M. Bellovin, *Firewalls and Internet Security: Repelling the Wily Hacker* (Reading, MA: Addison-Wesley, 1994).

Clolery, Paul, "How Biometrics Have Tamed Welfare Double Dipping," *ID World* 1, no 1 (March/April 1999).

Comer, Douglas E., *Internetworking with TCP/IP, Volume 1*, 2nd edition (Englewood Cliffs, NJ: Prentice Hall, 1991).

Cooper, Russ, "SAM Attacks v1.1," research paper, 22 July 1998. Posted on the NT Bugtraq Web site.

Corbató, F. J., "On Building Systems That Will Fail (A. M. Turing Award lecture)" *Communications of the ACM* 34, no. 9 (September 1991).

———, J. H. Saltzer, and C. T. Clingen, "Multics—The First Seven Years," *AFIPS Conference Proceedings* 40 (1972). Reprinted in the Multics Program Manual, Part I, from MIT Project MAC.

Counterpane Systems, "Password Safe," help file, 1999. Posted on the Counterpane Web site.

Crowell, William, "Testimony to the House International Relations Committee by William P. Crowell, Deputy Director, National Security Agency (NSA)," Office of Official Reporters, Office of the Clerk, U. S. House of Representatives, July 21, 1997. A redacted transcript of this closed hearing appears on the Cryptome Web site.

CSI/FBI, "Computer Crime and Security Survey," (San Francisco: Computer Security Institute, 2001).

CSS, "DeCSS in Words," *2600* 17, no. 3 (fall 2000).

Curtin, C. Matthew, "Snake Oil Warning Signs: Encryption Software to Avoid (Snake Oil FAQ)," white paper, 10 April 1998. Posted on Matt Curtin's personal Web page.

Custer, Helen, *Inside Windows NT*, 1st edition (Redmond, WA: Microsoft Press, 1993).

Datakey, "Datakey multi-purpose smart cards deployed by the FDIC for Secure online communications and building access," press release (Minneapolis, MN: Datakey, 26 October 2000). Posted on the Datakey Web site.

———, "Datakey smart card used by President Clinton to sign e-signature law," press release (Minneapolis, MN: Datakey, 26 October 2000). Posted on the Datakey Web site.

———, "Technical Specifications: Datakey's Cryptographic Smart Card and Smart Key," sales materials (Minneapolis, MN: Datakey, May 2000).

Davis, Ann, "The Body as Password," *Wired* 5, no. 7, (July 1997).

Delio, Michelle, "Palm Virus Hits, But Don't Worry," *Wired News* (22 September 2000). Posted on the Wired News Web site.

Denning, Dorothy E., and Giovanni Maria Sacco, "Timestamps in Key Distribution Protocols," *Communications of the ACM* 24, no. 8 (August 1981).

Denning, Dorothy E., "Digital Signatures with RSA and Other Public-Key Cryptosystems," *Communications of the ACM* 27, no. 4 (April 1984).

———, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1998).

———, and Dennis K. Branstad, "A Taxonomy of Key Recovery Encryption Systems," in *Internet Besieged*, edited by Denning and Denning. An earlier version was published as "A Taxonomy of Key Escrow Encryption," *Communications of the ACM* 39, no. 3 (March 1996).

———, and Peter J. Denning, eds., *Internet Besieged: Countering Cyberspace Scofflaws* (Reading, MA: Addison-Wesley, 1998).

———, and Peter MacDoran, "Location-Based Authentication: Grounding Cyberspace for Better Security" *Computer Fraud and Security* (February 1996). Reprinted in *Internet Besieged*, edited by Denning and Denning.

Denning, Peter, ed., *Computers Under Attack: Intruders, Worms, and Viruses* (Reading, MA: Addison-Wesley, 1990).

Diffie, Whitfield, "The First Ten Years of Public Key Cryptography," *Proceedings of the IEEE* 76, no. 5 (May 1988). Also appears in *Contemporary Cryptology*, edited by Gustavus Simmons.

———, and Martin Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," *IEEE Computer* 10 (1977).

Dorobek, Christopher J., "Agencies Expect E-Sign Law to Spur E-Gov," *Government Computer News* 19, no. 19 (10 July 2000).

Economist, "Biometrics, The Measure of Man," *The Economist* (9 September 2000).

Eddie the Wire, *The Complete Guide to Lock Picking* (Port Townsend, WA: Loompanics Unlimited, 1981).

Electronic Frontier Foundation, *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design* (Sebastopol, CA: O'Reilly & Associates, 1998).

Evans, Arthur, Jr., William Kantrowitz, and Edwin Weiss, "A User Authentication Scheme Not Requiring Secrecy in the Computer," *Communications of the ACM* 17, no. 8 (August 1974).

FBI (Federal Bureau of Investigation), "Financial Fraud and Failure Report" (Washington, DC: FBI, 1998). Posted on the FBI Web site.

Feghhi, Jalal, and Jalil Feghhi, *Secure Networking with Windows 2000 and Trust Services* (Boston: Addison-Wesley, 2001).

Feldmeier, David C., and Philip R. Karn, "UNIX Password Security—Ten Years Later," *Advances in Cryptology—Proceedings of Crypto '89* (Heidelberg: Springer-Verlag, 1990).

Feynman, Richard P., *"Surely You're Joking, Mr. Feynman!"* (New York: W. W. Norton, 1985).

Finseth, Craig, "An Access Control Protocol, Sometimes Called TACACS," Internet RFC 1492, July 1993. Posted on the IETF Web site.

FIRST (Forum of Incident Response and Security Teams), "Security Tools and Techniques Resource Library," CD-ROM, (Washington, DC: National Institute of Science and Technology, October 1994). Posted on the FIRST CD-ROM Web site.

Freier, Alan O., Philip Karlton, and Paul C. Kocher, "The SSL Protocol Version 3.0," 18 November 1996. Posted on the Netscape Web site.

Gamma, Erich, Richard Helm, Ralph Johnson, and John Vlissides, *Design Patterns: Elements of Reusable Object-Oriented Software* (Reading, MA: Addison-Wesley, 1995).

Ganesan, Ravi, and Chris Davies, "A New Attack on Random Pronounceable Password Generators," *Proceedings of the 17th National Computer Security Conference* (1994).

Gardner, Martin, "A New Kind of Cipher That Will Take Millions of Years to Break," *Scientific American* 237, no. 8 (August 1977).

Garfinkel, Simson, *PGP: Pretty Good Privacy* (Sebastopol, CA: O'Reilly & Associates, 1995).

Greenlee, M. Blake, "Requirements for Key Management Protocols in the Wholesale Financial Industry," in Abrams and Podell, *Tutorial: Computer and Network Security*.

Gutman, Peter, "How to Recover Private Keys from Microsoft Internet Explorer, Internet Information Server, Outlook Express, and Many Others - or - Where Do Your Encryption Keys Want to Go Today?" Research paper, posted to the Cryptography mailing list, 21 January 1999.

Hadfield, Lee, Dave Hatter, and Dave Bixler, *Windows NT Server 4 Security Handbook* (Indianapolis, IN: Que Corporation, 1997).

Hafner, Katie, and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier* (New York: Simon and Schuster, 1991).

Haller, Neil, "The S/Key One Time Password System," in *Proceedings of the Symposium on Network and Distributed Systems Security*, Internet Society, February 1994.

Heberlein, Todd, and Matt Bishop, "Attack Class: Address Spoofing" *Proceedings of the 19th National Computer Security Conference*, National Institute of Standards and Technology, October 1996. Reprinted in *Internet Besieged*, edited by Denning and Denning.

Hellman, Martin, "The Mathematics of Public-Key Cryptography," *Scientific American* (August 1979). Also appears in *Practical Cryptography*, edited by William Stallings.

Himowitz, Michael, "Keep Your Secrets Safe with Voice-Activated Software," *Fortune* (1 March 1999).

Hofmann-Wellenhof, B., H. Lichtenegger, and J. Collins, *Global Positioning System: Theory and Practice*, 4th edition (Heidelberg: Springer-Verlag, 1997).

Holzmann, Gerard J., and Björn Pehrson, *The Early History of Data Networks* (Los Alamitos, CA: IEEE Computer Society Press, 1995).

Houdini, Harry, *A Magician Among the Spirits* (New York: Harper & Brothers, 1924). Reprinted in New York by Arno Press, 1972.

Housley, Russ, Warwick Ford, Tim Polk, and Dave Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile," Internet RFC 2459, January 1999.

ITU-T (formerly CCITT), "Information Technology—Open Systems Interconnection—The Directory: Authentication Framework," Recommendation X.509 ISO/IEC 9594-8.

Jablon, David, "Strong Password-Only Authenticated Key Exchange" *ACM Computer Communications Review* (October 1996). Posted on the IEEE P1363a study group Web site and on the Integrity Sciences Web site.

Jacobs, John F., *The SAGE Air Defense System: A Personal History* (Bedford, MA: MITRE Corporation, 1986).

Jain, Anil, Ruud Bolle, and Sharath Pankanti, eds., *Biometrics: Personal Identification in Networked Society* (Boston: Kluwer Academic Publishers, 1999).

Jermyn, Ian, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Avi Rubin, "The Design and Analysis of Graphical Passwords," draft submitted to 8th USENIX Security Symposium, dated 8 March 1999.

Joncheray, Laurent, "Simple Active Attack Against TCP," Proceedings of the 5th *Unix Security Symposium* (Berkeley, CA: USENIX Association, 1995).

Kaplan, Ray, "Diary of a Security Incident." Usenet posting to alt.security, 22 May 1992.

Kaufman, Charlie, Radia Perlman, and Mike Speciner, *Network Security: PRIVATE Communication in a PUBLIC World* (Englewood Cliffs, NJ: Prentice Hall, 1995).

Kent, Stephen, "Privacy Enhancement for Internet Electronic Mail: Part II—Certificate-Based Key Management," Internet RFC 1422, February 1993. Posted on the IETF Web site.

———, and Randall Atkinson, "IP Authentication Header," Internet RFC 2402, November 1998. Posted on the IETF Web site.

———, and Randall Atkinson, "Security Architecture for the Internet Protocol," Internet RFC 2401, November 1998. Posted on the IETF Web site.

Kilburn, T., D. J. Howarth, R. B. Payne, and F. H. Sumner, "The Manchester University Atlas Operating System, Part 1: Internal Organization," *Comp. J.* 4 (October 1961), pp. 222–225.

Kim, Gene H., and Eugene H. Spafford, "The design and implementation of Tripwire: A file system integrity checker," *Proceedings of the 1994 ACM Conference on Communications and Computer Security* (New York: ACM Press, 1994).

Kingpin, "Attacks and Countermeasures for USB Hardware Token Devices," research paper, file date: 17 October 2000. Posted on the @stake Web site.

———, "Palm OS Password Lockout Bypass," @stake Security Advisory, 3 March 2001. Posted on the @stake Web site.

———, "SafeWord e.iD Palm Authenticator PIN Extraction," @stake Security Advisory, 14 December 2000. Posted on the @stake Web site.

———, "Wardialing Brief," white paper, file date: 1 August 2000. Posted on the @stake Web site.

Klein, Daniel V., "A Survey of, and Improvements to, Password Security," *Unix Security Workshop II* (Berkeley, CA: USENIX Association, 1990).

Knuth, Donald E., *Seminumerical Algorithms: The Art of Computer Programming, Volume 2* (Reading, MA: Addison-Wesley, 1969).

Kocher, Paul, Joshua Jaffe, and Benjamin Jun, "Differential Power Analysis," *Proceedings of Crypto '99*. Posted on the Cryptography Research, Inc., Web site.

Kohl, John, and Clifford Neuman, "The Kerberos Network Authentication Service (V5)," Internet RFC 1510, September 1993. Posted on the IETF Web site.

Konheim, Alan G., *Cryptography: A Primer* (New York: John Wiley, 1981).

Kornfelder, Leon, "Towards a Practical Public-Key Cryptosystem," B.S. thesis, Massachusetts Institute of Technology, May 1978.

Krawczyk, H., M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," Internet RFC 2104, February 1997. Posted on the IETF Web site.

Kuhn, Marcus G., "Probability Theory for Pickpockets—ec-PIN Guessing," COAST working paper (West Lafayette, IN: Purdue University, 1997). Posted on the COAST Web site.

Kwon, Taekyoung, and J. Song, "Authentication and Key Agreement via Memorable Password," Cryptology ePrint Archive Report 2000/026, 20 August 2000. Posted on the IACR Eprint Web site.

L0pht, "L0phtCrack 2.5 FAQ," Web page, 16 March 2001. Posted on the Security Software Technologies Web site.

La Macchia, B. A., and A. M. Odlyzko, "Computation of Discrete Logarithms in Prime Fields," *Designs, Codes, and Cryptography* 1, pp. 47–62 (1991).

Lamport, Leslie, "Password Authentication with Insecure Communication," *Communications of the ACM* 24, no. 11 (November 1981).

Lampson, Butler, Martín Abadi, Michael Burrows, and Edward Wobber, "Authentication in Distributed Systems: Theory and Practice," *ACM Transactions on Computer Systems* 10, no. 4 (November 1992). Also appears in *Practical Cryptography*, edited by William Stallings. A preliminary version appeared in the *Proceedings of the 13th ACM Symposium on Operating System Principles*.

Landau, Susan, "Standing the Test of Time: The Data Encryption Standard," *Notices of the AMS* 47, no. 3 (March 2000).

Levy, Matthys, and Mario Salvadori, *Why Buildings Fall Down* (New York: W. W. Norton & Co., 1992).

Levy, Steven, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age* (New York: Viking, 2001).

———, *Hackers: Heroes of the Computer Revolution* (New York: Dell Publishing, 1984).

Lions, J., "A Commentary on the Unix Operating System," Department of Computer Science, University of New South Wales, 1977.

———, "Unix Operating System Source Code Level Six," Department of Computer Science, University of New South Wales, 1977.

Littman, Jonathan, *The Fugitive Game: Online with Kevin Mitnick* (Boston: Little, Brown & Co., 1996).

Lloyd, Seth, "Ultimate Physical Limits to Computation," *Nature* 406 (August 2000).

Loeb, Vernon, "Energy Chief Touts Security Upgrades at Nuclear Labs," *Washington Post* (January 26, 2000), p. A13.

Lomas, T. M. A., L. Gong, J. I. Saltzer, and R. M. Needham, "Reducing Risks from Poorly Chosen Keys," *Proceedings of the Twelfth ACM Symposium on Operating Systems Principles* (December 1989), pp. 14–18.

Marks, Leo, *Between Silk and Cyanide: A Codemaker's War 1941–1945* (New York: The Free Press, 1998).

Maxwell, Scott, *Linux Core Kernel Commentary* (Scottsdale, AZ: The Coriolis Group, 1999).

McCarthy, Michael J., "Thinking Out Loud," *Wall Street Journal* 105, no. 47 (March 7, 2000).

McDonald, Daniel L., Randall J. Atkinson, and Craig Metz, "One Time Passwords in Everything (OPIE): Experiences with Building and Using Stronger Authentication," *Proceedings of the 5th Unix Security Symposium* (Berkeley CA: USENIX Association, 1995).

McLellan, Vin, "SecurID White Paper—A Comment," posted to best-of-security mailing list, 10 September 1996.

McNamara, John E., *Technical Aspects of Data Communication* (Maynard, MA: Digital Press, 1978).

Meinel, Carolyn P., *The Happy Hacker*, 2nd edition (Show Low, AZ: American Eagle Publications, 1998).

Metcalfe, Bob, "The Stockings Were Hung by the Chimney with Care," Internet RFC 602, December 1973. Posted on the IETF Web site.

Microsoft, "Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard," Microsoft Security Bulletin MS01-017, 22 March 2001. Posted on the Microsoft Web site.

———, "How to Enable Strong Password Functionality in Windows NT," Knowledge Base Article Q161990, revised 18 December 2000. Posted on the Microsoft Web site.

———, "Integrity Checking on Secure Channels with Domain Controllers," Knowledge Base Article Q183859, revised 10 April 1999. Posted on the Microsoft Web site.

———, "Secure Networking Using Windows 2000 Distributed Security Services." Microsoft TechNet article network/distsec.asp, 19 January 2000. Posted on the Microsoft Web site.

———, "Smart Card Logon," Windows 2000 white paper, 1999. Posted on the Microsoft Web site.

———, "Windows NT System Key Permits Strong Encryption of the SAM." Microsoft TechNet article Q143475, 17 February 2001. Posted on the Microsoft Web site.

———, "Windows 2000 Kerberos Authentication," Windows 2000 white paper, 1999. Posted on the Microsoft Web site.

———, "Update Available to Revoke Fraudulent Microsoft Certificates Issued by VeriSign," Microsoft TechNet article Q293811, 29 March 2001. Posted on the Microsoft Web site.

———, "User Authentication with Windows NT," Knowledge Base Article Q102716, revised 5 October 2000. Posted on the Microsoft Web site.

Miller, George A. "The Magical Number Seven—Plus or Minus Two: Some Limits on Our Capacity for Processing Information," *Psychological Science* 63 (1956), pp. 81–97.

Miller, Mike, "Pgpcrack README," software documentation.

MIT Project MAC, "Multiplexed Information and Computing Service: Programmers' Manual—Part I: Introduction to Multics," Revision 14 (Cambridge, MA: Massachusetts Institute of Technology, 30 September 1973).

———, "Project MAC Progress Report III: July 1965 to July 1966," Report MAC-PR-3 (Cambridge, MA: Massachusetts Institute of Technology, 1966).

Moore, Gordon E., *Electronics* 38, no. 11, (1965), pp. 114–117.

Morris, Robert, and Ken Thompson, "Password Security: A Case History," *Communications of the ACM* 22, no. 8 (November 1979).

Morris, Robert T., "A Weakness in the 4.2BSD Unix TCP/IP Software," Computing Science Technical Report No. 117 (Murray Hill, NJ: AT&T Bell Laboratories, 1985).

Moynihan, Daniel Patrick, *Secrecy: The American Experience* (New London, CT: Yale University Press, 1998).

Mudge and Kingpin, "Initial Cryptanalysis of the RSA SecurID Algorithm" research paper, January 2001. Posted on the @stake Web site.

Murray, Eric, "SSL Server Security Survey" research paper, 21 July 2000. Posted on Eric Murray's personal Web site.

Myer, T. H., and I. E. Sutherland, "On the Design of Display Processors," *Communications of the ACM* 11, no. 6 (June 1968).

Myers, M., R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol—OCSP," Internet RFC 2560, June 1999.

NBS (National Bureau of Standards), "Computer Security Guidelines for Implementing the Privacy Act of 1974," FIPS Publication 41 (Washington, DC: NBS, 30 May 1975). The standard was withdrawn on 18 November 1998.

———, "Guideline for Automatic Data Processing Risk Analysis," FIPS Publication 65 (Washington, DC: NBS, 1 August 1979). The standard was withdrawn on 25 August 1995.

NCSC (National Computer Security Center), "Department of Defense Password Management Guideline," CSC-STD-002-85 (Fort Meade, MD: National Computer Security Center, 12 April 1985).

———, "A Guide to Understanding Audit in Trusted Systems," NCSC-TG-001 Version 2 (Fort Meade, MD: NCSC, 1 June 1988).

———, "A Guide to Understanding Data Remanence in Automated Information Systems," NCSC-TG-025, Version 2 (Fort Meade, MD: NCSC, September 1991).

———, "Department of Defense Trusted Computer System Evaluation Criteria," DOD 5200.28-STD (Fort Meade, MD: NCSC, 26 December 1985).

NIST (National Institute for Standards and Technology), "Advanced Encryption Standard (AES)," Draft FIPS (Washington, DC: NIST, 2001). Posted on the NIST Web site.

———, "Automated Password Generator," FIPS Publication 181 (Washington, DC: NIST, 5 October 1993). Posted on the NIST Web site.

———, "Data Encryption Standard (DES)," FIPS Publication 46-3 (Washington, DC: NIST, 25 October 1999). Posted on the NIST Web site.

———, "DES Modes of Operation," FIPS Publication 81 (Washington, DC: NIST, 2 December 1980). Posted on the NIST Web site.

———, "Digital Signature Standard," FIPS Publication 186-2 (Washington, DC: NIST, 27 January 2000). Posted on the NIST Web site.

———, "Entity Authentication Using Public Key Cryptography," FIPS Publication 196 (Washington, DC: NIST, 18 February 1997). Posted on the NIST Web site.

———, "Escrowed Encryption Standard," FIPS Publication 185 (Washington, DC: NIST, 9 February 1994). Posted on the NIST Web site.

———, "Secure Hash Standard," FIPS Publication 180-1 (Washington, DC: NIST, April 1995). Posted on the NIST Web site.

National Research Council, *Cryptography's Role In Securing the Information Society: CRISIS* (Washington, DC: National Academy Press, 1996).

Nechvatal, James, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback, "Report on the Development of the Advanced Encryption Standard (AES)" (Washington, DC: NIST, 2 October 2000).

Needham, Roger M., and Michael D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," *Communications of the ACM* 21, no. 12 (December 1978).

Negin, Michael, Thomas Chmielewski, Jr., Marcos Salganicoff, Theodore A. Camus, Ulf M. Cahn von Seelen, Péter L. Venetianer, Guanghua. G. Zhang, "An Iris Biometric System for Public and Personal Use," *IEEE Computer* 33, no. 2 (February 2000).

Neuman, B. Clifford, and S. Stubblebine, "A Note on the Use of Timestamps as Nonces," *Operating Systems Review* (April 1993).

Neuman, B. Clifford, and Theodore Ts'o, "Kerberos: An Authentication Service for Computer Networks," *IEEE Communications Magazine* 32, no. 9 (September 1994). Also appears in *Practical Cryptography for Data Internetworks*, edited by Stallings.

Neuman, Michael, "Monitoring and Controlling Suspicious Activity in Realtime With IP-Watcher," *Proceedings of the 11th Annual Computer Security Applications Conference*, December 1995.

Neumann, Peter, *Computer Related Risks* (Reading, MA: Addison-Wesley, 1996).

Nickel, Larry, "Why Use Magnetic Stripe Cards?" Web page file "why-use.htm," 1998. Posted on the Mercury Security Web site.

Norman, Donald, *The Design of Everyday Things* (New York: Doubleday Currency, 1988).

Noyce, R. N., "Microelectronics," *Scientific American* 237, no. 3 (September 1977), pp. 62–69.

O'Gorman, Lawrence, "Practical Systems for Personal Fingerprint Identification," *IEEE Computer* 33, no. 2 (February 2000).

Oppliger, Rolf, *Authentication Systems for Secure Networks* (Boston: Artech House, 1996).

Pankanti, Sharath, Ruud M. Bolle, and Anil Jain, "Biometrics: The Future of Identification," *IEEE Computer* 33, no. 4 (February 2000).

Parker, Donn, *Crime by Computer: Startling New Kinds of Million-Dollar Fraud, Theft, Larceny, & Embezzlement* (New York: Charles Scribner's Sons, 1976).

———, *Fighting Computer Crime: A New Framework for Protecting Information* (New York: John Wiley & Sons, 1998).

PC Dynamics, "ActivCard Synchronous Authentication," Report ALL/TU.90.001/En, (San Francisco: PC Dynamics, 1997). Posted on the PC Dynamics Web site.

Peltier, Tom, *Information Security Risk Analysis* (Boca Raton, FL: Auerbach, 2001).

Pentland, Alex (Sandy), and Tanzeem Choudhury, "Face Recognition for Smart Environments" *IEEE Computer* 33, no. 2 (February 2000).

Perlman, Radia, and Charlie Kaufman, "Secure Password-Based Protocol for Downloading a Public Key," *Proceedings of the 1999 Network and Distributed System Security Symposium* (Reston, VA: Internet Society, 1999).

Perlman, Radia, *Interconnections: Bridges, Routers, Switches, and Internetworking Protocols*, 2nd edition (Reading, MA: Addison-Wesley, 2000).

PixIL, "Read This! User Manual," Version 2.62, 2 October 1999. Posted on the PixIL Web site.

Postel, Jonathan, "Internet Protocol—DARPA Internet Program Protocol Specification," Internet RFC 791, 1 September, 1981. Posted on the IETF Web site.

———, "Transmission Control Protocol—DARPA Internet Program Protocol Specification," Internet RFC 793, 1 September, 1981. Posted on the IETF Web site.

Power, Richard, "CSI Special Report on DDOS: Part 1. Diary of a Debacle," *Computer Security Alert* 205 (April 2000).

———, *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace* (Indianapolis, IN: Que, 2000).

Rabin, M. O., "Digital Signatures and Public-Key Functions as Intractable as Factorization," MIT Laboratory for Computer Science, Report MIT/LCS/TR-212, January 1979.

———, "Probabilistic Algorithm for Testing Primality," *Journal of Number Theory* 12, no. 1 (February 1980).

Raleigh, T. M., and R. W. Underwood, "CRACK: A Distributed Password Advisor," *Proceedings of the USENIX UNIX Security Workshop* (Berkeley, CA: USENIX Association, 1988).

Ramsbottom, Alan, "FAQ: NT Cryptographic Password Attacks and Defenses," 17 July 1997. Posted on the NT Bugtraq Web site.

Ratha, Nalini K., and Ruud Bolle, "Smartcard Based Authentication," Chapter 18 of Jain, Bolle, and Pankanti, eds., *Biometrics: Personal Identification in Networked Society*.

Reeds, J. A., and B. J. Weinberger, "File Security and the Unix Crypt Command," *AT&T Technical Journal* 63, no. 8 (October 1984).

Rescorla, Eric, *SSL and TLS: Designing and Building Secure Systems* (Boston: Addison-Wesley, 2001).

Rigney, C., S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," Internet RFC 2865, June 2000.

Ritchie, D. M., "The Unix Time-Sharing System: A Retrospective," *Bell System Technical Journal* 57, no. 6, part 2 (July–August 1978).

Rivest, Ron, "Can We Eliminate Certificate Revocation Lists?" *Proceedings of Financial Cryptography 1998*.

———, "MD5 Digest Algorithm," Internet RFC 1321, April 1992. Posted on the IETF Web site.

———, A. Shamir, and L. Adelman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM* 21, no. 2 (February 1978).

Rochlis, Jon, and Mark Eichin, "With Microscope and Tweezers: The Worm from MIT's Perspective," *Communications of the ACM* 32, no. 6 (June 1989), pp. 689–698. Also in *Computers Under Attack*, edited by Denning.

Roper, C. A., and Bill Phillips, *The Complete Book of Locks and Locksmithing*, 3rd edition (Blue Ridge Summit, PA: Tab Books, 1991).

Rothke, Ben, "Fingerprint Biometric Devices: How They Work and How to Choose Them," *Computer Security Journal* 14, no. 4 (fall 1998).

RSA Security, "DES-II Challenges Solved," *Cryptobytes* (summer 1998). Posted on the RSA Security Web site.

———, "RSA Crypto Challenge Sets New Security Benchmark," press release, 26 August 1999. Posted on the RSA Security Web site.

———, "Strong Enterprise User Authentication: RSA ACE/Server" (Bedford, MA: RSA Security, 1999). Posted on the RSA Security Web site.

Salus, Peter H., *A Quarter Century of Unix* (Reading, MA: Addison-Wesley, 1994).

Schneier, Bruce, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (New York: John Wiley & Sons, 1996).

———, "Why Cryptography Is Harder Than It Looks," white paper (Minneapolis, MN: Counterpane, 1997). Posted on the Counterpane Web site.

———, and Adam Shostack, "Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards," *Proceedings of the USENIX Workshop on Smart Card Technology* (Berkeley, CA: USENIX Association, 1999), pp. 175–185. Posted on the Counterpane Web site.

———, and Mudge, "Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)," *Proceedings of the 5th ACM Conference on Communications and Computer Security* (New York: ACM Press, 1998).

———, Mudge, and David Wagner, "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)," *CQRE '99* (Heidelberg: Springer-Verlag, 1999), pp. 192–203.

Senderek, Ralf, "Key-Experiments—How PGP Deals with Manipulated Keys," Web page security/key-experiments.html, August 2000. Posted on Ralf Senderek's personal Web site.

Shoch, John, and Jon Hupp, "The 'Worm' Programs—Early Experiences with a Distributed Computation." *Communications of the ACM* 25, no. 3 (March 1982), pp. 172-180. Also in *Computers Under Attack*, edited by Denning. An earlier version, dated September 1980, was distributed as Internet Working Group (INWG) Note 242 and presented at the *ACM SIGOPS/SIGPLAN Workshop on Fundamental Issues in Distributed Computing* in December 1980.

Schultz, E. Eugene, and Thomas Longstaff, "Internet Sniffer Attacks," *Proceedings of the 18th National Information Systems Security Conference*, National Institute of Standards and Technology, October 1995, pp. 534–542. Also in *Internet Besieged*, edited by Denning and Denning.

Schultz, Eugene, "Windows NT Password Security" *Computer Security Journal* 15, no. 2 (spring 1999).

Schwartau, Winn, *Information Warfare: Chaos on the Electronic Superhighway*, 2nd edition (New York: Thunder's Mouth Press, 1996).

Secure Computing, "SafeWord DES Gold Supervisor Guide" (Roseville, MN: Secure Computing Corporation, 1996). Posted on the Secure Computing Web site.

———, "SafeWord Plus Virtual Smart Card Server Solution," white paper (San Jose, CA: Secure Computing Corporation, July 2000). Posted on the Secure Computing Web site.

Shamir, Adi, and Nicko van Somerin, "Playing Hide and Seek with Stored Keys," research paper, 22 September 1998.

Shimomura, Tsutomu, with John Markoff, *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—By the Man Who Did It* (New York: Hyperion, 1996).

Shneiderman, Ben, *Designing the User Interface: Strategies for Effective Human–Computer Interaction,* 3rd edition (Reading, MA: Addison-Wesley, 1998).

Sicherman, Al, "By Any Other Name, He Probably Could Log On Somewhere," *Minneapolis Star Tribune* (23 November 1998), p. E4.

Silverman, Robert, "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths," Bulletin 13, RSA Laboratories, April 2000. Posted on the RSA Security Web site.

Simmons, Gustavus J., ed., *Contemporary Cryptology: The Science of Information Integrity* (New York: IEEE Press, 1992).

Simons, John, "Phone Hex," *Wall Street Journal* (1 October 1999).

Smith, Richard, "Deciphering the Advanced Encryption Standard," *Network Magazine* 16, no. 3 (March 2001), pp. 96–101.

———, "Authentication: Patterns Of Trust" *Information Security* 3 (August 2000).

———, "Historical Overview of Computer Architecture," *Annals of the History of Computing* 10, no. 4 (1989).

———, *Internet Cryptography* (Reading, MA: Addison-Wesley, 1997).

———, "Mandatory Protection for Internet Server Software," *Proceedings of the 12th Annual Computer Security Applications Conference*, December 1996, San Diego, CA.

Snider, L. Britt, and Daniel S. Seikaly, "Report of Investigation: Improper Handling of Classified Information by John M. Deutsch," Report 1998-0028-IG, (Washington, DC: Central Intelligence Agency, 18 February 2000). Posted on the Federation of American Scientists Web site.

Spafford, Eugene H., "Crisis and Aftermath" *Communications of the ACM* 32, no. 6 (June 1989), pp. 678–687. Also in *Computers Under Attack*, edited by Denning.

———, "Observing Reusable Password Choices" Purdue Technical Report CSD-TR-92-049, (West Lafayette, IN: Purdue University, 1992). Also appeared in *Proceedings of the 3rd USENIX Security Symposium* (Berkeley, CA: USENIX Association, 1992). Posted on the COAST Web site.

———, "OPUS: Preventing Weak Password Choices," Purdue Technical Report CSD-TR-92-028, (West Lafayette, IN: Purdue University, 1991). A version of this paper also appeared in *Proceedings of the 14th National Computer Security Conference* (Washington, DC: NIST, 1991). Posted on the COAST Web site.

Stallings, William, *Practical Cryptography for Data Internetworks* (Los Alamitos, CA: IEEE Computer Society Press, 1996).

Standage, Tom, *The Victorian Internet* (New York: Berkley Books, 1998).

Steiner, Jennifer G., Clifford Neuman, and Jeffrey I. Schiller, "Kerberos: An Authentication Service for Open Network Systems," *Proceedings of the 1988 USENIX Winter Conference* (Berkeley, CA: USENIX Association, 1988).

Stevens, W. Richard, *TCP/IP Illustrated, Volume 1* (Reading, MA: Addison-Wesley, 1994).

Stinson, Douglas, *Cryptography Theory and Practice* (Boca Raton, FL: CRC Press, 1995).

Stoll, Clifford, *The Cuckoo's Egg* (Garden City, NY: Doubleday, 1989).

Sumner, F. H., G. Haley, and E. C. Y. Chen, "The Central Control Unit of the 'Atlas' Computer," *Proceedings of the IFIP Congress* (1962), pp. 657–662.

Sutton, Stephen, *Windows NT Security Guide* (Reading, MA: Addison-Wesley, 1997).

———, "Windows NT Security Guidelines: A Study for NSA Research" (Urbana, IL: Trusted Systems Services, 1998).

Tardo, J., and K. Alagappan, "SPX: Global Authentication Using Public Key Certificates," *Proceedings of the IEEE Symposium on Security and Privacy* (Los Alamitos, CA: IEEE Computer Society Press, 1991).

Tenner, Edward, *Why Things Bite Back* (New York: Alfred A. Knopf, 1996).

Tomko, George, "Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?" from the *9th Privacy Commissioners'/Data Protection Authorities Workshop*, 15 September 1998. Posted on the Information Privacy Commissioner/Ontario Web site.

Ts'o, Theodore, Clifford Neuman, George Kohl, Tom Yu, and Kenneth Raeburn, "The Kerberos Network Authentication Service (V5)," 7 March 2001. This has been distributed as an Internet Draft.

Tung, Brian, *Kerberos: A Network Authentication System* (Reading, MA: Addison-Wesley, 1999).

———, Clifford Neuman, Matthew Hur, Ari Medvinsky, Sasha Medvinsky, John Wray, and Jonathan Trostle, "Public Key Cryptography for Initial Authentication in Kerberos," 15 July 2000. This has been distributed as an Internet Draft.

Uehling, Mark, "Cracking the Uncrackable Code," *Popular Science* (September 1994). Also appears in *Practical Cryptography*, edited by William Stallings.

van Eck, Wim, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" (Leidschendam, The Netherlands: PTT Dr. Neher Laboratories, 16 April 1985).

Van Vleck, Tom, "The IBM 7094 and CTSS," Web page thvv/7094.html, 18 December 1997. Posted on the Multicians Web site.

———, "Multics: Security," Web page security.html, 15 February 1995. Posted on the Multicians Web site.

Wagner, David, and Bruce Schneier, "Analysis of the SSL 3.0 Protocol," *Proceedings of the Second USENIX Workshop on Electronic Commerce* (Berkeley, CA: USENIX Association, 1996) pp. 29–40.

———, Bruce Schneier, and John Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm," (Minneapolis, MN: Counterpane Labs, 20 March 1997). Posted on the Counterpane Labs Web site.

Wayner, Peter, *Disappearing Cryptography* (San Francisco: Morgan Kaufmann, 1996).

Weinstein, Lauren (lauren@UCLA-SECURITY), "60 Minutes Parody," text file, circa 1980. Probably first distributed via the "Human-Nets" e-mail distribution list.

Weizenbaum, Joseph, *Computer Power and Human Reason: From Judgement to Calculation* (San Francisco: W. H. Freeman and Co., 1976).

Whitten, Alma, and J. D. Tygar, "Usability of Security: A Case Study," Report CMU-CS-98-155, (Pittsburgh, Pennsylvania: Carnegie Mellon University Computer Science Department, 18 December 1998).

———, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," *Proceedings of the 8th USENIX Security Symposium* (Berkeley, CA: USENIX Association, 1999).

Wiener, Michael J., "Efficient DES Key Search." Technical Report TR-244, School of Computer Science (Canada: Carlton University, May 1994). Also appears in *Practical Cryptography*, edited by Stallings.

Wilkes, Maurice, *Timesharing Computer Systems* (London: Macdonald, 1968).

Willis, David, and Mike Lee, "Six Biometric Devices Point the Finger at Security," *Network Computing* (1 June 1998).

Woodward, John D., "Biometrics: Identifying Law and Policy Concerns," in *Biometrics: Personal Identification in Networked Society*, edited by Jain, Bolle, and Pankanti. The article is based on the paper "Biometrics: Privacy's Friend or Foe?" *Proceedings of the IEEE* (September 1997).

X9 Financial Services Committee, "Financial Institution Key Management (Wholesale)," Standard X9.17, (Washington, DC: American Bankers Association, 1985). Posted on the X9 Online Web site.

———, "Managing Risk and Mitigation Planning: Withdrawal of ANSI X9.9," Report X9/TG-24-1999 (Washington, DC: American Bankers Association, 1999). Posted on the X9 Online Web site.

———, "PIN Security Compliance Guideline," Report X9/TG-3 (Washington, DC: American Bankers Association, 1997). Posted on the X9 Online Web site.

Yan, Jianxin, Alan Blackwell, Ross Anderson, and Alasdair Grant, "Memorability and Security of Passwords—Some Empirical Results," research paper (Cambridge, UK: Cambridge University Computer Laboratory, 2001).

Yeager, Wayne B., *Techniques of Safecracking* (Port Townsend, WA: Loompanics Unlimited, 1990).

Zipes, Jack, ed., *The Arabian Nights: The Marvels and Wonders of the Thousand and One Nights* (New York: Signet Classic, 1991).