1. A guide to understanding covert channel capacity analysis of a trusted system, National computer security center, November 1993, at www.fas.org/irp/nsa/rainbow/tg030.htm

2. A guide to understanding data remanence in automated information systems, NCSC–TG–025, www.cerberussystems.com/INFOSEC/stds/ncsctg25.htm

3. M. Abadi and R. Needham, Prudent engineering practice for cryptographic protocols, *IEEE Trans. on Software Engineering*, Vol. 22, No. 1, pp. 6-15, January 1996

4. E. Ackerman, Student skirts CD's piracy guard, SiliconValley.com, at www.siliconvalley.com/mld/siliconvalley/news/local/6960633.htm

5. ACLs versus Capabilities, www.erights.org/elib/capability/delegations.html

6. Aleph One, Smashing the stack for fun and profit, *Phrack* 49, at www.phrack.org/show.php?p=49&a=14

7. Anarchriz, CRC and how to reverse it, at its.mine.nu/html/re/essays/CRC.html

8. D. Anderson, T. Frivold, and A. Valdes, Next-generation intrusion detection expert system (NIDES): summary, at www.sdl.sri.com/papers/4/s/4sri/4sri.pdf

9. R. Anderson and E. Biham, Tiger: a fast new hash function, at www.cs.technion.ac.il/~biham/Reports/Tiger/tiger.ps

10. R. Anderson, Security in open versus closed source systems—the dance of Boltzmann, Coarse and Moore, at www.ftp.cl.cam.ac.uk/ftp/users/rja14/toulouse.pdf

11. R. Anderson, TCPA/Palladium frequently asked questions, at www.cl.cam.ac.uk/%7Erja14/tcpa-faq.html

12. W. A. Arbaugh, N. Shankar, and Y. C. J. Wan, Your 802.11 wireless network has no clothes, at www.cs.umd.edu/~waa/wireless.pdf

13. A real MD5 collision, *Educated Guesswork*, August 2004 archives, at www.rtfm.com/movabletype/archives/2004_08.html#001055

14. D. V. Bailey, Inside eBook security, *Dr. Dobb's Journal*, November 2001, at www.ddj.com/documents/s=1487/ddj0111d/0111d.htm

15. I. Balepin, Superworms and cryptovirology: a deadly combination, at wwwcsif.cs.ucdavis.edu/~balepin/new_pubs/worms-cryptovirology.pdf

16. M. Barrett and C. Thomborson, Using NGSCB to mitigate existing software threats, at www.cs.auckland.ac.nz/~cthombor/Pubs/cses.pdf

17. BBC News, Afghan girl found after 17 years, at news.bbc.co.uk/1/hi/world/south_asia/1870382.stm

18. Beale Screamer, Microsoft's digital rights management scheme—technical details, at web.elastic.org/~fche/mirrors/cryptome.org/beale-sci-crypt.htm

19. D. J. Bernstein, The IPv6 mess, at cr.yp.to/djbdns/ipv6mess.html

20. P. Biddle et. al., The darknet and the future of content distribution, at crypto.stanford.edu/DRM2002/darknet5.doc

21. L. Boettger, The Morris worm: how it affected computer security and lessons learned by it, at hackersnews.org/hackerhistory/morrisworm.html

22. N. Borisov, I. Goldberg, and D. Wagner, Intercepting mobile communications: the insecurity of 802.11, at www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

23. D. Brumley and D. Boneh, Remote timing attacks are practical, at crypto.stanford.edu/~dabo/papers/ssl-timing.pdf

24. P. Capitant, Software tamper-proofing deployed 2-year anniversary report, Macrovision Corporation, at www.cs.sjsu.edu/faculty/stamp/DRM/DRM%20papers/Software_Tamper-Proofing.ppt

25. J. Carr, Strategies & issues: thwarting insider attacks, *Network Magazine*, September 4, 2002, at www.networkmagazine.com/article/NMG20020826S0011

26. P. Červeň, *Crackproof Your Software: Protect Your Software Against Crackers*, No Starch Press, 2002

27. H. Chang and M. J. Atallah, Protecting software code by guards *Workshop on Security and Privacy in Digital Rights Management 2001*

28. Clipper chip, at en.wikipedia.org/wiki/Clipper_chip

29. F. B. Cohen, Experiments with computer viruses, 1984, at www.all.net/books/virus/part5.html

30. F. B. Cohen, Operating system protection through program evolution, at all.net/books/IP/evolve.html

31. C. S. Collberg and C. Thomborson, Watermarking, tamper-proofing and obfuscation—tools for software protection, *IEEE Transactions on Software Engineering*, vol. 28, no. 8, August 2002

32. S. A. Craver et. al., Reading between the lines: lessons learned from the SDMI challenge, *Proceedings of the 10th USENIX Security Symposium*, Washington, DC, August 13–17, 2001, at www.usenix.org/events/sec01/craver.pdf

33. RSA Conference 2002 Trip Report, at home.earthlink.net/~mstamp1/tripreports/RSA2002.html

34. RSA Conference 2004 Trip Report, at www.cs.sjsu.edu/faculty/stamp/papers/tripreports/RSA04.html

35. J. Daugman, How iris recognition works, at www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf

36. D. Davis, Defective sign & encrypt in S/MIME, PKCS#7, MOSS, PEM, PGP, and XML, at world.std.com/~dtd/sign_encrypt/sign_encrypt7.html

37. E. X. DeJesus, SAML brings security to XML, *XML Magazine*, at www.fawcette.com/xmlmag/2002_02/magazine/columns/collaboration/edejesus/

38. Defcon 11 Trip Report, at home.earthlink.net/~mstamp1/tripreports/defcon11.html

39. D. E. Denning, Descriptions of key escrow systems, at www.cosc.georgetown.edu/~denning/crypto/Appendix.html

40. J. F. Dhem et. al., A practical implementation of the timing attack, at www.cs.jhu.edu/~fabian/courses/CS600.624/Timing-full.pdf

41. W. Diffie and M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, vol. IT–22, no. 6, pp. 644–654, November 1976, at
www.cs.jhu.edu/~rubin/courses/ sp03/papers/diffie.hellman.pdf

42. I. Dubrawsky and L. Hayden, Wireless LANs and privacy, at
inet2002.org/CD-ROM/lu65rw2n/papers/t07-c.pdf

43. EFF DES cracker project, at www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/

44. P. Earley, Family of spies: The John Walker Jr. spy case, *The Crime Library*, at www.crimelibrary.com/spies/walker/

45. Easy solution to bypass latest CD-audio protection, at
www.cdfreaks.com/news/4068

46. C. Ellison and B. Schneier, Ten risks of PKI: what you're not being told about public key infrastructure, *Computer Security Journal*, vol. 16, no. 1, pp. 1–7, 2000, at www.schneier.com/paper-pki.html

47. G. Ellison, J. Hodges, and S. Landau, Risks presented by single sign-on architectures, October 18, 2002, at research.sun.com/liberty/RPSSOA/

48. P. England et. al., A trusted open platform, *IEEE Computer*, pp. 55–62, July 2003

49. A. C. Engst, Mac OS X trojan technique: beware of geeks bearing gifts, *TidBITS*, no. 726, April 2004, at db.tidbits.com/getbits.acgi?tbart=07636

50. Enigma machine, at en.wikipedia.org/wiki/Enigma_machine

51. D. B. Everett, Trusted computing platforms, at
www.netproject.com/presentations/TCPA/david_everett.pdf

52. S. Forrest, A. Somayaji, and D. H. Ackley, Building diverse computer systems, at www.cs.unm.edu/~forrest/publications/hotos-97.pdf

53. S. Forrest, S. A. Hofmeyr, and A. Somayaji, Computer immunology, *Communications of the ACM*, vol. 40, no. 10, pp. 88–96, October 1997

54. L. Fraim, SCOMP: A solution to the multilevel security problem, *IEEE Computer*, pp. 26–34, July 1983

55. GSM cloning, at www.isaac.cs.berkeley.edu/isaac/gsm.htm

56. W. W. Gibbs, Software's chronic crisis, Trends in Computing, *Scientific American*, p. 86, September 1994, at www.cis.gsu.edu/~mmoore/CIS3300/handouts/SciAmSept1994.html

57. R. Glenn and S. Kent, RFC 2410 — The NULL encryption algorithm and its use with IPsec, at www.faqs.org/rfcs/rfc2410.html

58. D. B. Glover, *Secret Ciphers of the 1876 Presidential Election*, Aegean Park Press, 1991

59. S. Goodwin, Internet gambling software flaw discovered by Reliable Software Technologies software security group, at www.cigital.com/news/index.php?pg=art&artid=20

60. E. Grevstad, CPU-based security: the NX bit, at hardware.earthweb.com/chips/article.php/3358421

61. B. Guignard, How secure is PDF?, at www-2.cs.cmu.edu/~dst/Adobe/Gallery/PDFsecurity.pdf

62. Hacker may be posing as Microsoft, *USA Today*, February 6, 2002, at www.usatoday.com/tech/techinvestor/2001-03-22-microsoft.htm

63. N. Hardy, The confused deputy (or why capabilities might have been invented), at www.skyhunter.com/marcs/capabilityIntro/confudep.html

64. History of GSM, at www.cellular.co.za/gsmhistory.htm

65. B. Horne et, al., Dynamic self-checking techniques for improved tamper resistance, *Workshop on Security and Privacy in Digital Rights Management 2001*

66. D. Isbell, M. Hardin, and J. Underwood, Mars climate team finds likely cause of loss, at www.iki.rssi.ru/jplmirror/mars/msp98/news/mco990930.html

67. A. Jain, L. Hong, and S. Pankanti, Biometric Identification, *Communications of the ACM*, vol. 43, no. 2, pp. 91–98, 2000

68. John the Ripper password cracker, at www.openwall.com/john/

69. M. E. Kabay, Salami fraud, *Network World Security Newsletter*, July 24, 2002, at www.nwfusion.com/newsletters/sec/2002/01467137.html

70. L. Kahney, OS X trojan horse is a nag, at www.wired.com/news/mac/0,2125,63000,00.html?tw=rss.TEK

71. Kerckhoffs' law, at en.wikipedia.org/wiki/Kerckhoffs'_law

72. P. C. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, at www.cryptography.com/resources/whitepapers/TimingAttacks.pdf

73. D. P. Kormann and A. D. Rubin, Risks of the Passport single signon protocol, at avirubin.com/passport.html

74. H. Krawczyk, M. Bellare and R. Canetti, RFC 2104 — HMAC: Keyed-hashing for message authentication, at www.faqs.org/rfcs/rfc2104.html

75. M. Kuhn, Security—biometric identification, at www.cl.cam.ac.uk/Teaching/2003/Security/guestslides/slides-biometric-4up.pdf

76. P. B. Ladkin, Osprey, cont'd, *The Risks Digest*, vol. 21, issue 41, 2001, at catless.ncl.ac.uk/Risks/21.41.html#subj7

77. B. W. Lampson, Computer security in the real world, *IEEE Computer*, pp. 37–46, June 2004

78. C. E. Landwehr et. al., A taxonomy of computer program security flaws, with examples, *ACM Computing Surveys*, vol. 26, no. 3, pp. 211–254, September 1994, at chacs.nrl.navy.mil/publications/ CHACS/1994/1994landwehr-acmcs.pdf

79. R. Lemos, Spat over MS 'flaw' gets heated, *ZD Net UK News*, at news.zdnet.co.uk/software/developer/0,39020387,2104559,00.htm

80. C. J. Lennard and T. Patterson, History of fingerprinting, at www.policensw.com/info/fingerprints/finger01.html

81. J. Lettice, Bad publicity, clashes trigger MS Palladium name change, *The Register*, at www.theregister.co.uk/content/4/29039.html

82. S. Levy, The open secret, *Wired*, issue 7.04, April 1999, at `www.wired.com/wired/archive/7.04/crypto_pr.html`

83. A. Main, Application security: building in security during the development stage, at `www.cloakware.com/downloads/news/`

84. J. McLean, A comment on the "basic security theorem" of Bell and LaPadula, *Information Processing Letters*, vol. 20, no. 2, February 1985, at `chacs.nrl.navy.mil/publications/ CHACS/Before1990/1985mclean-ipl.pdf`

85. T. McNichol, Totally random: how two math geeks with a lava lamp and a webcam are about to unleash chaos on the Internet, *Wired*, Issue 11.08, August 2003, at `www.wired.com/wired/archive/11.08/random.html`

86. R. Merkle, Secure communications over insecure channels, *Communications of the ACM*, April 1978, pp. 294–299 (submitted in 1975), at `www.itas.fzk.de/mahp/weber/merkle.htm`

87. M. S. Miller, K.-P. Yee, and J. Shapiro, Capability myths demolished, at `zesty.ca/capmyths/`

88. D. Moore et. al., The spread of the Sapphire/Slammer worm, at `www.cs.berkeley.edu/~nweaver/sapphire/`

89. A. Muchnick, Microsoft nearing completion of Death Star, at `bbspot.com/News/2002/05/deathstar.html`

90. P. S. Pagliusi, A contemporary foreword on GSM security, in G. Davida, Y. Frankel, and O. Rees, editors, *Infrastructure Security: International Conference—InfraSec 2002*, Bristol, UK, October 1–3, 2002, Lecture Notes in Computer Science 2437, pp. 129–144, Springer–Verlag, 2002

91. J. C. Panettieri, Who let the worms out? — the Morris worm, *eWeek*, March 12, 2001, at `www.eweek.com/article2/0,1759,1245602,00.asp`

92. D. B. Parker, Automated crime, at `infosecuritymag.techtarget.com/articles/1999/autocrime.shtml`

93. D. B. Parker, Automated security, at `infosecuritymag.techtarget.com/articles/1999/autocrime2.shtml`

94. Passwords revealed by sweet deal, *BBC News*, April 20, 2004, at news.bbc.co.uk/2/hi/technology/3639679.stm

95. M. Pietrek, Peering inside the PE: a tour of the Win32 portable executable file format, at msdn.microsoft.com/library/default.asp

96. A. Pressman, Wipe 'em out, then sue for back pay, at www.internetwright.com/drp/RiskAssess.htm

97. Purple Cipher, at en.wikipedia.org/wiki/PURPLE

98. C. Ren, M. Weber, and G. McGraw, Microsoft compiler flaw technical note, at www.cigital.com/news/index.php?pg=art&artid=70

99. Robert Morris, at www.rotten.com/library/bio/hackers/robert-morris/

100. M. J. Rose, Stephen King's 'Plant' uprooted, *Wired*, November 28, 2000, at www.wired.com/news/culture/0,1284,40356,00.html

101. P. Sayer, 'The Plant' withers for Stephen King, *InfoWorld*, November 29, 2000, at www.infoworld.com/articles/hn/xml/00/11/29/001129hnplant.html

102. B. Schneier, Attack trees, *Dr. Dobb's Journal*, December 1999, at www.schneier.com/paper-attacktrees-ddj-ft.html

103. B. Schneier, Biometrics: truths and fictions, at www.schneier.com/crypto-gram-9808.html

104. B. Schneier, Risks of relying on cryptography, Inside Risks 112, *Communications of the ACM*, vol. 42, no. 10, October 1999, at www.schneier.com/essay-021.html

105. A. Shamir and N. van Someren, Playing hide and seek with stored keys, at www.ncipher.com/resources/downloads/files/white_papers/keyhide2.pdf

106. C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, vol. 28–4, pp. 656–715, 1949, at www.cs.ucla.edu/~jkong/research/security/shannon1949.pdf

107. R. Slade, Brain, at www.cknow.com/vtutor/vtsladebrain.htm

108. M. Stamp and A. Hushyar, Multilevel security models, to appear as a chapter of *The Handbook of Information Security*

109. M. Stamp and D. Holankar, Secure streaming media and digital rights management, *Proceedings of the 2004 Hawaii International Conference on Computer Science*, January 2004, at home.earthlink.net/~mstamp1/papers/hawaii.pdf

110. M. Stamp and E. J. Sebes, Enterprise digital rights management: Ready for primetime?, *Business Communications Review*, pp. 52–55, March 2004, at www.bcr.com/bcrmag/2004/03/p52.asp

111. M. Stamp and S. Thaker, Software watermarking via assembly code transformations, *Proceedings of ICCSA 2004*, June 2004, at www.cs.sjsu.edu/faculty/stamp/papers/iccsaSmita.doc

112. M. Stamp, Digital rights management: For better or for worse?, *ExtremeTech*, May 20, 2003, at www.extremetech.com/article2/0,3973,1051610,00.asp

113. M. Stamp, Digital rights management: the technology behind the hype, *Journal of Electronic Commerce Research*, vol. 4, no. 3, 2003, at www.csulb.edu/web/journals/jecr/issues/20033/paper3.pdf

114. M. Stamp, Risks of digital rights management, Inside Risks 147, *Communications of the ACM*, vol. 45, no. 9, p. 120, September 2002, at www.csl.sri.com/users/neumann/insiderisks.html#147

115. M. Stamp, Risks of monoculture, Inside Risks 165, *Communications of the ACM*, vol. 47, no. 3, p. 120, March 2004, at www.csl.sri.com/users/neumann/insiderisks04.html#165

116. S. Staniford, V. Paxson, and N. Weaver, How to own the Internet in your spare time, at www.cs.berkeley.edu/~nweaver/cdc.web/

117. P. Ször and P. Ferrie, Hunting for metamorphic, Symantec Corporation White Paper, http://www.peterszor.com/metamorp.pdf

118. D. Terdiman, Vegas gung-ho on gambling tech, *Wired*, September 19, 2003, at www.wired.com/news/print/0,1294,60499,00.html

119. C. Thomborson and M. Barrett, NGSCB: a new tool for securing applications, at www.cs.auckland.ac.nz/~cthombor/Pubs/barrettNZISF120804.pdf

120. K. Thompson, Reflections on trusting trust, *Communication of the ACM*, vol. 27, no. 8, pp. 761–763, August 1984, at `www.acm.org/classics/sep95/`

121. US v. ElcomSoft & Sklyarov FAQ, at `www.eff.org/IP/DMCA/US_v_Elcomsoft/us_v_elcomsoft_faq.html`

122. R. Vamosi, Windows XP SP2 more secure? Not so fast, at `reviews.zdnet.co.uk/software/os/0,39024180,39163696,00.htm`

123. VENONA, at `www.nsa.gov/venona/index.cfm`

124. L. von Ahn, M. Blum, and J. Langford, Telling humans and computers apart automatically, *Communications of the ACM*, vol. 47, no. 2, pp. 57–60, February 2004, at `www.cs.cmu.edu/~biglou/captcha_cacm.pdf`

125. L. von Ahn et. al., The CAPTCHA project, at `www.captcha.net/`

126. R. N. Williams, A painless guide to CRC error detection algorithms, at `www.ross.net/crc/crcpaper.html`

127. W. Wong, Revealing your secrets through the fourth dimension, to appear in *ACM Crossroads*, available at `www.cs.sjsu.edu/faculty/stamp/students/wing.html`

128. M. Zalewski, Strange attractors and TCP/IP sequence number analysis—one year later, at `lcamtuf.coredump.cx/newtcp/`

129. L. Zeltser, Reverse engineering malware, at `www.zeltser.com/sans/gcih-practical/`

130. L. Zeltser, SANS malware FAQ: reverse engineering srvcp.exe, at `http://www.sans.org/resources/malwarefaq/srvcp.php`

131. Zimmermann Telegram, at `en.wikipedia.org/wiki/Zimmerman_telegram`

132. M. Zorz, Basic security with passwords, at `www.net-security.org/article.php?id=117`