Bibliography

[AB04] Tom Anderson and David Brady. Principle of least astonishment. *Oregon Pattern Repository*, November 15 2004. http://c2.com/cgi/wiki?PrincipleOfLeastAstonishment.

[Acc05] Access Data. Forensic toolkit—overview, 2005. http://www.accessdata.com/Product04_Overview.htm?ProductNum=04.

[Adv87] Display ad 57, February 8 1987.

[Age05] US Environmental Protection Agency. Wastes: The hazardous waste manifest system, 2005. http://www.epa.gov/epaoswer/hazwaste/gener/manifest/.

[AHR05a] Ben Adida, Susan Hohenberger, and Ronald L. Rivest. Fighting Phishing Attacks: A Lightweight Trust Architecture for Detecting Spoofed Emails (to appear), 2005. Available at http://theory.lcs.mit.edu/~rivest/publications.html.

[AHR05b] Ben Adida, Susan Hohenberger, and Ronald L. Rivest. Separable Identity-Based Ring Signatures: Theoretical Foundations For Fighting Phishing Attacks (to appear), 2005. Available at http://theory.lcs.mit.edu/~rivest/publications.html.

[AIS77] Christopher Alexander, Sara Ishikawa, and Murray Silverstein. *A Pattern Language: towns, buildings, construction*. Oxford University Press, 1977. (with Max Jacobson, Ingrid Fiksdahl-King and Shlomo Angel).

[AKM+93] H. Alvestrand, S. Kille, R. Miles, M. Rose, and S. Thompson. RFC 1495: Mapping between X.400 and RFC-822 message bodies, August 1993. Obsoleted by RFC2156 [Kil98]. Obsoletes RFC987, RFC1026, RFC1138, RFC1148, RFC1327 [Kil86, Kil87, Kil89, Kil90, HK92]. Status: PROPOSED STANDARD.

[Ale79] Christopher Alexander. *The Timeless Way of Building*. Oxford University Press, 1979.

[Ale96] Christopher Alexander. Patterns in architecture [videorecording], October 8 1996. Recorded at OOPSLA 1996, San Jose, California.

[Alt00] Steven Alter. Same words, different meanings: are basic IS/IT concepts our self-imposed Tower of Babel? *Commun. AIS*, 3(3es):2, 2000.

[Alv97] Harald T. Alvestrand. X.400 frequenty asked questions, October 27 1997. `http://www.alvestrand.no/x400/faq-mhsnews.html`. Cited on March 22, 2005.

[Ame05] American Library Association Office for Information Technology Policy. Managing cookies to protect patron privacy, 2005. `http://www.ala.org/ala/washoff/oitp/emailtutorials/privacya/20.htm`. Accessed April 20, 2005.

[And98] M. Andrews. RFC 2308: Negative caching of DNS queries (DNS NCACHE), March 1998. Updates RFC1034, RFC1035 [Moc87b, Moc87c]. Status: PROPOSED STANDARD.

[App03] Appligent, Inc. *Redax User Guide, Version 3.5*. Appligent, 2003. `http://www.appligent.com`.

[App04a] Apple Computer. Apple human interface guidelines, December 2004. `http://developer.apple.com/documentation/UserExperience/Conceptual/OSXHIGuidelines/OSXHIGuidelines.pdf`.

[App04b] Apple Computer. Apple human interface guidelines, March 2004. `http://developer.apple.com/documentation/UserExperience/Conceptual/OSXHIGuidelines/OSXHIGuidelines.pdf`.

[App04c] Apple Computer. Apple human interface guidelines, October 2004. `http://developer.apple.com/documentation/UserExperience/Conceptual/OSXHIGuidelines/OSXHIGuidelines.pdf`.

[App04d] Apple Computer. Apple software design guidelines, May 2004. `http://developer.apple.com/documentation/MacOSX/Conceptual/AppleSWDesign/AppleSWDesign.pdf`.

[App04e] Apple Computer. Enabling secure storage with keychain services, June 2004. `http://developer.apple.com/documentation/Security/Conceptual/keychainServConcepts/keychainServConcepts.pdf`.

[App05] Apple. Apple – Mac OS X – security, 2005. `http://www.apple.com/macosx/features/security/`. Cited on April 15, 2005.

[Art02] Henrik Artman. Procurer usability requirements: negotiations in contract development. In *NordiCHI '02: Proceedings of the second Nordic conference on Human-computer interaction*, pages 61–70. ACM Press, 2002. ISBN 1-58113-616-1.

[AS99] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42:41–46, 1999.

[Ass05] Association for India's Development Austin. Computer drive, February 2005. `http://studentorgs.utexas.edu/aidaustin/comp_drive.html`.

[ASZ96] D. Atkins, W. Stallings, and P. Zimmermann. RFC 1991: PGP message exchange formats, August 1996. Status: INFORMATIONAL.

[Bal93] D. Balenson. RFC 1423: Privacy enhancement for Internet electronic mail: Part III: Algorithms, modes, and identifiers, February 1993. Obsoletes RFC1115. Status: PROPOSED STANDARD.

[Bar91] John A. Barry. *Technobabble*. MIT Press, 1991.

[Bax05] Ilse Baxter. Response to your questions, April 15 2005.

[BBG00] Nicholas Bohm, Ian Brown, and Brian Gladman. Electronic commerce: Who carries the risk of fraud? *Journal of Information Law & Technology*, 2000. `http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/`.

[bBL02] Yung bin Benjamin Lee, August 2002. Personal Communication (via Gene Spafford).

[BC87] Kent Beck and Ward Cunningham. Using pattern languages for object-oriented programs. Technical Report CR-87-43, Apple Computer, Tektronix, September 1987.

[BDSG04] Dirk Balfanz, Glenn Durfee, D. K. Smetters, and R. E. Grinter. In search of usable security: five lessons from the field. *Security & Privacy Magazine*, 2:19–24, Sept–Oct 2004.

[BDSG05] Dirk Balfanz, Glenn Durfee, D. K. Smetters, and R. E. Grinter. Making the impossible easy: Usable PKI. In Lorrie Cranor and Simson Garfinkel, editors, *Security and Usability*. O'Reilly, 2005. To appear in August 2005.

[Ber02] Scott Berinato. Good stuff cheap: A new hardware market is developing to give CIOs what they want most: good stuff cheap. This is its story. *CIO*, pages 53–59, 15 October 2002.

[Ber05a] David Berlind. Thought to be redacted, classified military info exposed by cut n' paste. *ZDNet*, May 1 2005. `http://blogs.zdnet.com/BTL/?p=1329`.

[Ber05b] Jordy Berson. Creating usable security products for consumers. In Lorrie Cranor and Simson Garfinkel, editors, *Security and Usability*. O'Reilly, 2005. To appear in August 2005.

[BF01] Dan Boneh and Matthew Franklin. Identity based encryption from the Weil pairing. *Lecture Notes in Computer Science*, 2139:213+, 2001. `citeseer.ist.psu.edu/article/boneh01identitybased.html`.

[BHm04] Bob Blakley, Craig Heath, and members of The Open Group Security Forum. Security design patterns. Technical Report G031, The Open Group, April 2004. http://www.opengroup.org/publications/catalog/g031.htm.

[Bid96] C. Bradford Biddle. Misplaced priorities: The Utah Digital Signature Act and liability allocation in a public key infrastructure. *San Diego Law Review*, 33, 1996.

[Bis96] Matt Bishop. Unix security: Threats and solutions, March 1996. http://seclab.cs.ucdavis.edu/projects/vulnerabilities/scriv/1996-share86.pdf. Presentation to SHARE 86.0.

[BL03] Ann Bostrom and Ragnar E. Lofstedt. Communicating risk: Wireless and hardwired. *Risk Analysis*, 23(2):241–247, 2003.

[Bla93] Matt Blaze. A cryptographic file system for Unix. In *1st ACM Conference on Communications and Computing Security*, pages 9–16. ACM Press, November 1993.

[BNN04a] Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security proofs for identity-based identification and signature schemes, 2004. http://eprint.iacr.org/2004/252.pdf. Updated version of [BNN04b].

[BNN04b] Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security proofs for identity-based identification and signature schemes. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology — Eurocrypt 2004*, volume 3027 of Lecture notes in Computer Science, pages 268–286. 2004, 2004.

[Bor96] Lorraine Borman. SIGCHI: the early years. *SIGCHI Bull.*, 28(1):4–6, 1996. ISSN 0736-6906. http://doi.acm.org/10.1145/249170.249172.

[BP01] Steven Bauer and Nissanka B. Priyantha. Secure data deletion for Linux file systems. In *Proc. 10th Usenix Security Symposium*, pages 153–164. Usenix, San Antonio, Texas, 2001. http://www.usenix.org/events/sec01/full_papers/bauer/bauer_html/.

[Bra89a] R. Braden. STD 3: Requirements for Internet hosts — communication layers, October 1989. See also RFC1122, RFC1123 [Bra89b, Bra89c].

[Bra89b] R. T. Braden. RFC 1122: Requirements for Internet hosts — communication layers, October 1, 1989. See also STD0003 [Bra89a]. Status: STANDARD.

[Bra89c] R. T. Braden. RFC 1123: Requirements for Internet hosts — application and support, October 1, 1989. See also STD0003 [Bra89a]. Updates RFC0822 [Cro82a]. Updated by RFC2181 [EB97]. Status: STANDARD.

[Bre00] Eric A. Brewer. Towards robust distributed systems (abstract). In *PODC '00: Proceedings of the nineteenth annual ACM symposium on Principles of distributed computing*, page 7. ACM Press, 2000. ISBN 1-58113-183-6.

[BS99] Ian Brown and C. R. Snow. A proxy approach to e-mail security. *Softw. Pract. Exper.*, 29(12):1049–1060, 1999. ISSN 0038-0644.

[BS03] Sacha Brostoff and M. Angela Sasse. Ten strikes and you're out: Increasing the number of login attempts can improve password usability. In *Workshop on Human-Computer Interaction and Security Systems, part of CHI2003*. ACM Press, April 2003. `citeseer.ist.psu.edu/618589.html`.

[BSD93] unlink, 1993. 4th Berkeley Distribution.

[Bud02] Len Budney. Mailcrypt, September 2002. `http://mailcrypt.sourceforge.net/`.

[Bus05] Business Environmental Resource Center. Hazardous waste generator fact sheet, 2005. `http://sacberc.org/HazWaste.html`.

[Bye03] Simon Byers. Scalable exploitation of, and responses to information leakage through hidden data in published documents, April 3 2003.

[CAG02] Lorrie Faith Cranor, Manjula Arjula, and Praveen Guduru. Use of a P3P user agent by early adopters. In *WPES '02: Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*, pages 1–10. ACM Press, 2002. ISBN 1-58113-633-1.

[CAM+04] Lorrie Cranor, Mark Ackerman, Fabian Monrose, Andrew Patrick, and Norman Sadeh. DIMACS workshop on usable privacy and security software, July 2004. `http://dimacs.rutgers.edu/Workshops/Tools/`.

[CAN03] CAN-SPAM act of 2003, November 2003. `http://www.spamlaws.com/federal/108s877.html`.

[Car96] Remy Card. Announce 0.4, October 7 1996. `http://www.ibiblio.org/pub/historic-linux/ftp-archives/tsx-11.mit.edu/Oct-07-1996/packages/ext2fs/old/announce.0.4`.

[Car02] Remy Card. CHATTR(1), 2002.

[Car04] Caron Carlson. CAN-SPAM leaves lid wide open. *eWeek*, May 20 2004. `http://www.eweek.com/article2/0,1759,1596134,00.asp`.

[CDE+05] Lorrie Cranor, Brooks Dobbs, Serge Egelman, Giles Hogben, Jack Humphrey, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph Reagle, Matthias Schunter, David A. Stampley, and Rigo Wenning. The platform for privacy preferences 1.1 (P3P1.1) specification, January 4 2005. `http://www.w3.org/TR/2005/WD-P3P11-20050104/Overview.html`.

[CDFT98] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer. RFC 2440: OpenPGP message format, November 1998. Status: PROPOSED STANDARD.

[CER99] CERT Coordination Center. CERT advisory ca-1999-04 melissa macro virus. Technical report, CERT Coordination Center, Pittsburgh, PA, 27. March 1999. http://www.cert.org/advisories/CA-1999-04.html.

[CER00] CERT Coordination Center. CERT advisory ca-2000-04 love letter worm. Technical report, CERT Coordination Center, Pittsburgh, PA, 4. May 2000. http://www.cert.org/advisories/CA-2000-04.html.

[CER01] CERT Coordination Center. CERT advisory ca-2001-26 Nimda Worm. Technical report, CERT Coordination Center, Pittsburgh, PA, 18. September 2001. http://www.cert.org/advisories/CA-2001-26.html.

[CFIJ99] Giovannissell Di Crescenzo, Niels Ferguson, Russell Impagliazzo, and Markus Jakobsson. How to forget a secret. In *STACS 99*, pages 500–509. Springer Verlag, 1999. http://www.macfergus.com/pub/forget.html. Lecture Notes in Computer Science 1563.

[CG05] Lorrie Cranor and Simson Garfinkel. *Security and Usability*. O'Reilly, 2005.

[Chr95] Da Chronic. AOHell v3.0 rage against the machine, 1995.

[CK05] Michael Crawford and Paul Kallender. Trend micro bug down to over-quick testing. *Techworld*, April 26 2005. http://www.techworld.com/security/news/index.cfm?NewsID=3559.

[Cla92] David Clark. A cloudy crystal ball—visions of the future (alternative title: Apocalypse now). In *Proceedings of the Twenty-Fourth Internet Engineering Task Force*. The Internet Society, July 13–17 1992. http://ietf.org/proceedings/prior29/IETF24.pdf.

[Cla03] David Clark. Personal communication, 2003.

[CLR90] Thomas H. Cormen, Charles E. Leiserson, and Ronald L. Rivest. *Introduction to Algorithms*. The MIT Press, 1990.

[CLRS01] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, Second Edition*. The MIT Press, 2001.

[CNN05] CNN. U.S. soldiers cleared in Italian agent's death. *CNN.com*, April 30 2005. http://www.cnn.com/2005/US/04/30/italian.shooting/.

[Co.03] Hitachi Software Engineering Co. Selinux policy editor, 2003. http://www.selinux.hitachi-sk.co.jp/en/tool/selpe/selpe-top.html.

[Coa92] Peter Coad. Object-oriented patterns. *Commun. ACM*, 35(9):152–159, 1992. ISSN 0001-0782.

[Coc05] Alistair Cockburn. The risk management catalog, 2005. http://members.aol.com/acockburn/riskcata/risktoc.htm. unpublished; cited on March 25, 2005.

[Col04] Andrew Colley. Latest phishing scam most "devious" ever. *ZDNet Australia*, March 3 2004. http://www.zdnet.com.au/news/security/0,2000061744,39116416,00.htm.

[Com03] Comcast. How do I setup and clear the history (visted sites) in Internet Explorer? Technical Report 17601, Comcast, 2003. http://faq.comcast.net/faq/answer.jsp?name=17601.

[Com04a] Federal Trade Comission. Disposal of consumer report information and records, November 18 2004. http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf. Final Rule.

[Com04b] Federal Trade Comission. FTC issues final regulation on consumer information and records disposal, November 18 2004. http://www.ftc.gov/opa/2004/11/factadisposal.htm. Press Release.

[Com04c] Apple Computer. Hardware—iSight, 2004. http://www.apple.com/isight/. Cited September 18, 2004.

[Com05a] Apple Computer. About Safari international domain name support, March 21 2005. http://docs.info.apple.com/article.html?artnum=301116.

[Com05b] Apple Computer. Filevault: Safe, secure and speedy, 2005. http://www.apple.com/macosx/features/filevault/.

[Coo99] Alan Cooper. *The Inmates Are Running The Asylum*. Sams, Indianapolis, Indiana, 1999.

[Cor96] Microsoft Corporation. The microsoft internet security framework: Technology for secure communication, access control, and commerce, 1996. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/msdn_misf.asp.

[Cor04a] Microsoft Corporation. How to minimize metadata in Microsoft Word documents, August 2004. http://support.microsoft.com/kb/223790/. Microsoft Knowledge Base #223790.

[Cor04b] Microsoft Corporation. How to minimize metadata in word 2000 documents, September 2004. http://support.microsoft.com/kb/237361/. Microsoft Knowledge Base #237361.

[Cor04c] Microsoft Corporation. The Remove Hidden Data tool for Office 2003 and Office XP, August 2004. http://support.microsoft.com/kb/834427. Microsoft Knowledge Base #834427.

[Cor05a] Microsoft Corporation. How to minimize metadata in Microsoft PowerPoint presentations, 2005. http://support.microsoft.com/kb/314797. Microsoft Knowledge Base #314797.

[Cor05b] Microsoft Corporation. How to minimize metadata in word 2002, January 2005. http://support.microsoft.com/kb/290945/. Microsoft Knowledge Base #290945.

[Cor05c] Microsoft Corporation. How to minimize metadata in word 2003, 2005. http://support.microsoft.com/kb/825576/. Microsoft Knowledge Base #825576.

[Cor05d] Microsoft Corporation. Microsoft powertoys for windows XP, 2005. http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx.

[Cov05] Lynne Coventry. Usable biometrics. In Lorrie Cranor and Simson Garfinkel, editors, *Security and Usability*. O'Reilly, 2005. To appear in August 2005.

[CPG+04] Jim Chow, Ben Pfaff, Tal Garfinkel, Kevin Christopher, , and Mendel Rosenblum. Understanding data lifetime via whole system simulation. In *Proceedings of the 13th USENIX Security Symposium*, pages 321–336. Usenix, 2004. http://www.usenix.org/events/sec04/tech/chow.html.

[CPM+98] Crispan Cowan, Calton Pu, Dave Maier, Jonathan Walpole, Peat Bakke, Steve Beattie, Aaron Grier, Perry Wagle, Qian Zhang, and Heather Hinton. StackGuard: Automatic adaptive detection and prevention of buffer-overflow attacks. In *Proc. 7th USENIX Security Conference*, pages 63–78. Usenix, San Antonio, Texas, jan 1998. citeseer.nj.nec.com/cowan98stackguard.html.

[CPVH77] D. Crocker, K. T. Pogran, J. Vittal, and D. A. Henderson. RFC 724: Proposed official standard for the format of ARPA network messages, May 12, 1977. Obsoleted by RFC0733 [CVPH77]. Status: UNKNOWN. Not online.

[CRA03] Four grand challenges in trustworthy computing, November 2003. http://www.cra.org/Activities/grand.challenges/security/home.html.

[Cre81] R. J. Creasy. The origin of the VM/370 time-sharing system. *IBM Journal of Research and Development*, 25, September 1981.

[CRG97] Lorrie Faith Cranor, Paul Resnick, and Danielle Gallo. Technology inventory: A catalog of tools that support parents's ability to choose online content appropriate for their children, December 1997. http://www.research.att.com/projects/tech4kids/actions.html. Prepared for the Internet Online Summit: Focus on Children, December 1997; Revised for America Links Up, September 1998.

[Cro82a] D. Crocker. RFC 822: Standard for the format of ARPA Internet text messages, August 13, 1982. See also STD0011 [Cro82b]. Obsoletes RFC0733 [CVPH77]. Updated by RFC1123, RFC1138, RFC1148, RFC1327, RFC2156 [Bra89c, Kil89, Kil90, HK92, Kil98]. Status: STANDARD.

[Cro82b] David H. Crocker. STD 11: Standard for the format of ARPA Internet text messages, August 13, 1982. See also RFC0822 [Cro82a]. Obsoleted by RFC2822 [Res01]. Obsoletes RFC0733 [CVPH77].

[CSI03] CSI. *2003 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute, 2003. `http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf`.

[CSI04] CSI. *2004 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute, 2004. `http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf`.

[CVPH77] D. Crocker, J. Vittal, K. T. Pogran, and D. A. Henderson. RFC 733: Standard for the format of ARPA network text messages, November 21, 1977. Obsoleted by RFC0822 [Cro82a]. Obsoletes RFC0724 [CPVH77]. Status: UNKNOWN.

[CW87] D. D. Clark and D. R. Wilson. A comparison of commercial and military computer security models. In *1987 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, April 1987.

[Dav96] Don Davis. Compliance defects in public key cryptography. In *6th USENIX Security Symposium*, pages 171–178. Usenix, July 22–27 1996.

[dCZ00] Leandro Nunes de Castro and Fernando José Von Zuben. Artificial immune systems: Part II—a survey of applications. Technical Report DCA-RT 02/00, Department of Computer Engineering and Industrial Automation, School of Electrical and Computer Engineering, State University of Campinas, SP, Brazil, February 2000. `citeseer.ist.psu.edu/nunesdecastro00artificial.html`.

[Del04a] Mark Delany. Domain-based email authentication using public-keys advertised in the DNS (domainkeys), August 2004. INTERNET DRAFT.

[Del04b] What are the top 5 things you can do to improve your system performance?, September 14 2004. `http://support.dell.com/support/topics/global.aspx/support/kb/en/document?dn=1089806&l=en&s=gen`.

[DG02] Dipankar Dasgupta and Fabio González. An immunity-based technique to characterize intrusions in computer networks. *IEEE Trans. Evol. Comput.*, 6(3):1081–1088, June 2002. `citeseer.ist.psu.edu/dasgupta02immunitybased.html`.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976. `citeseer.ist.psu.edu/diffie76new.html`.

[DHR+98] S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, and L. Repka. RFC 2311: S/MIME version 2 message specification, March 1998. Status: INFORMATIONAL.

[DiS02] Jennifer DiSabatino. Enron bankruptcy case highlights e-mail's lasting trail. *Computerworld*, January 21 2002. http://www.computerworld.com/industrytopics/financial/story/0,10801,67583,00.html.

[DoD85] DoD CSC. *Department of Defense Password Management Guideline*. US DoD, April 12 1985. http://www.fas.org/irp/nsa/rainbow/std002.htm. CSC-STD-002-85.

[DoD95] Cleaning and sanitization matrix, 1995. www.dss.mil/isec/nispom_0195.htm. Chapter 8.

[Don05] Steve Doner. Personal communication, February 2005.

[DVGD96] C. Davis, P. Vixie, T. Goodwin, and I. Dickinson. RFC 1876: A means for expressing location information in the domain name system, January 1996. Updates RFC1034, RFC1035 [Moc87b, Moc87c]. Status: EXPERIMENTAL.

[Eas97] D. Eastlake. RFC 2137: Secure domain name system dynamic update, April 1997. Updates RFC1035 [Moc87c]. Status: PROPOSED STANDARD.

[EB96] R. Elz and R. Bush. RFC 1982: Serial number arithmetic, August 1996. Updates RFC1034, RFC1035 [Moc87b, Moc87c]. Status: PROPOSED STANDARD.

[EB97] R. Elz and R. Bush. RFC 2181: Clarifications to the DNS specification, July 1997. Updates RFC1034, RFC1035, RFC1123 [Moc87b, Moc87c, Bra89c]. Status: PROPOSED STANDARD.

[Edm03] Ron Edmonds. Justice department hid parts of report criticizing diversity effort. *Associated Press*, October 31 2003. http://www.usatoday.com/news/washington/2003-10-31-doj-report_x.htm.

[EFL+99] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen. RFC 2693: SPKI certificate theory. IETF RFC Publication, September 1999.

[EHN03] A systematic review of the reserach on consumer understanding of nutrition labeling, June 2003. http://www.ehnheart.org/files/consumer\%20nutrition-143058A.pdf.

[Elk96] M. Elkins. RFC 2015: MIME security with pretty good privacy (PGP), October 1996. Status: PROPOSED STANDARD.

[Ell99] C. Ellison. RFC 2692: SPKI requirements. IETF RFC Publication, September 1999.

[Ell02] Carl Ellison. Improvements on conventional PKI wisdom. In *1st Annual PKI Research Workshop—Proceedings*, pages 165–175. National Institutes of Standards and Technology, 2002. http://www.cs.dartmouth.edu/~pki02/Ellison/.

[EMUM90] C. F. Everhart, L. A. Mamakos, R. Ullmann, and P. V. Mockapetris. RFC 1183: New DNS RR definitions, October 1, 1990. Updates RFC1034, RFC1035 [Moc87b, Moc87c]. Status: EXPERIMENTAL.

[Eng67] D. C. Engelbart. X-y position indicator for a display system, June 1967. US Patent 3,541,541.

[EPC05] EPCglobal. Guidelines on epc for consumer products, 2005. `http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html`.

[ErK97] D. Eastlake, 3rd, and C. Kaufman. RFC 2065: Domain name system security extensions, January 1997. Updates RFC1034, RFC1035 [Moc87b, Moc87c]. Status: PROPOSED STANDARD.

[ES00] Carl Ellison and Bruce Schneier. Ten risks of PKI: What you're not being told about public key infrastructure. *Computer Security Journal*, XVI(1), 2000.

[Far96] Dan Farmer. Personal communication, December 21 1996.

[FB99] Armando Fox and Eric A. Brewer. Harvest, yield and scalable tolerant systems. In *Workshop on Hot Topics in Operating Systems*, pages 174–178. IEEE Computer Society Press, March 28–30 1999. `citeseer.ist.psu.edu/fox99harvest.html`.

[FC99] Andrew Flaig and Gloria Chang. Managing fraud and integrity risk... best practices offer key, Spring 1999. `http://www.hotel-online.com/Trends/Andersen/1999_FraudRisk.html`.

[Fed97] Federal Trade Comission. Ftc says internet scam re-routes 'surfers' to international telephone lines: High-tech scheme cost consumers hundreds of thousands in illegally-billed computer time, February 19 1997. `http://www.cslib.org/attygenl/press/1997/comp/audiotex.htm`.

[FK96] A. O. Freier and P. Karltrons. The SSL protocol, 1996. `http://wp.netscape.com/eng/ssl3/ssl-toc.html`.

[FM97] David H. Freedman and Charles C. Mann. *At Large: The Strange Case of the World's Biggest Internet Invasion*. Simon & Schuster, 1997.

[FM04] Leah Findlater and Joanna McGrenere. A comparison of static, adaptive, and adaptable menus. In *CHI '04: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 89–96. ACM Press, New York, NY, USA, 2004. ISBN 1-58113-702-8.

[For05] Stephanie Forrest. Computer immune systems—papers, 2005. `http://www.cs.unm.edu/~immsec/papers.htm`.

[FS03] Niels Ferguson and Bruce Schneier. *Practical Cryptography*. Wiley Publishing, 2003.

[FSA97] Stephanie Forrest, Anil Somayaji, and David. H. Ackley. Building diverse computer systems. In *Workshop on Hot Topics in Operating Systems*, pages 67–72. Usenix, 1997. citeseer.ist.psu.edu/forrest97building.html.

[FTC05] Donate your used computer today, February 2005. http://www.firsttimecomputers.org/.

[GAI04] GAIN Publishing. Precision time — home, 2004. http://www.precision-time.com/. Cited December 1, 2004.

[Gar91] Simson Garfinkel. Designing a write-once file system. *Dr. Dobb's Journal*, 16: 78–88, January 1991.

[Gar94] Simson Garfinkel. *PGP: Pretty Good Privacy*. O'Reilly & Associates, 1994.

[Gar95] Simson Garfinkel. Illegal program troubles America Online. *The Boston Globe*, April 1995. http://simson.net/clips/1995/95.Globe.AOHell.pdf.

[Gar96a] Simson L. Garfinkel. The web masters are watching. *Internet Underground*, 1996.

[Gar96b] Peter Garza. Affidavit in support of complaint, 1996. http://www.simson.net/ref/1996/ardita.pdf. Prepared in connection with the criminal prosecution of Julio Cesar Ardita.

[Gar00] Simson L. Garfinkel. *Database Nation*. O'Reilly & Associates, 2000.

[Gar02] Simson L. Garfinkel. Adopting fair information practices to low cost RFID systems, 2002. Paper presented at Privacy in Ubicomp'2002 workshop, Gotenborg, Sweden, September 29th, 2002.

[Gar03a] Simson L. Garfinkel. Email-based identification and authentication: An alternative to PKI? *Security & Privacy Magazine*, 1:20–26, Nov. - Dec. 2003.

[Gar03b] Simson L. Garfinkel. Enabling email confidentiality through the use of opportunistic encryption. In *The 2003 National Conference on Digital Government Research*. National Science Foundation, 2003. http://www.digitalgovernment.org/dgrc/dgo2003/cdrom/PAPERS/citsprivacy/garfinkel.pdf.

[Gar04a] Simson Garfinkel. The pure software act of 2006. *TechnologyReview.com*, April 7 2004. http://simson.net/clips/2004/2004.TR.04.PureSoftware.pdf.

[Gar04b] Simson L. Garfinkel. Interview with owner of disk #21, October 21 2004.

[Gar04c] David Garrett. Outlook & its rivals. *Processor*, October 1 2004.

[Gar05] Simson L. Garfinkel. *Design Principles and Pattersn for Computer Systems that are Simultaneously Secure and Usable*. PhD thesis, MIT, Cambridge, MA, April 26 2005.

[Geh02] Christian Gehrmann. Bluetooth™ security white paper. Technical report, Bluetooth SIG Security Expert Group, may 2002. https://www.bluetooth.org/foundry/sitecontent/document/security_whitepaper_v1. Version 1.01.

[Gei04] Matthew Geiger. Computer-forensic privacy tools: A forensic evaluation, 2004. Final project in CMU 95-818: Privacy Policy, Law, and Technology.

[Ger04] Jack M. Germain. Dell spyware decision spurs new trend. *E Commerce Times*, November 2004. http://www.ecommercetimes.com/story/37668.html.

[GGL03] Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung. The Google file system. In *SOSP '03: Proceedings of the nineteenth ACM symposium on Operating systems principles*, pages 29–43. ACM Press, 2003. ISBN 1-58113-757-5.

[GHJV95] Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides. *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley Professional, 1995.

[Gil04] Alorie Gilbert. California lawmaker introduces RFID bill. *CNet News.com*, February 24 2004. http://news.zdnet.com/2100-3513_22-5164457.html.

[GJSJ91] David K Gifford, Pierre Jouvelot, Mark A. Sheldon, and James O'Toole Jr. Semantic file systems. In *Proceedings of the 13th ACM Symposium on Operating Systems Principles*. ACM Press, ACM Press, 1991.

[GK03] Nathaniel S. Good and Aaron Krekelberg. Usability and privacy: a study of Kazaa P2P file-sharing. In *Proceedings of the conference on Human factors in computing systems*, pages 137–144. ACM Press, 2003. ISBN 1-58113-630-7.

[GL85] Simson L. Garfinkel and J. Spencer Love. A file system for write-once media, October 1985.

[GLNS93] Li Gong, T. 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.

[GNM+05] Simson L. Garfinkel, Erik Nordlander, Robert C. Miller, David margrave, and Jeffrey I. Schiller. How to make secure email easier to use. In *CHI 2005*. ACM Press, 2005.

[Gol91] James K. Goldston. *A Guide to Understanding Data Remanence in Automated Information Systems*. National Computer Security Center, 1991. http://www.fas.org/irp/nsa/rainbow/tg025-2.htm. NCSC-TG-025, Library No. 5-236,082.

[Goo04] Google. Choose your Google toolbar configuration, 2004. http://toolbar.google.com/prdlg.html. Cited December 1, 2004.

[Gra04] Jerry Grasso. Earthlink and webroot release second spyaudit report, June 16 2004.

[Gru89] Jonathan Grudin. The case against user interface consistency. *Commun. ACM*, 32(10):1164–1173, 1989. ISSN 0001-0782.

[GS91] Simson Garfinkel and Gene Spafford. *Practical UNIX Security*. O'Reilly & Associates, 1991.

[GS02a] Simson Garfinkel and Abhi Shelat. Remembrance of data passed. *IEEE Security and Privacy Magazine*, January 2002.

[GS02b] Simson Garfinkel and Gene Spafford. *Web Security, Privacy & Commerce*. O'Reilly & Associates, 2002.

[GSN+05] Simson L. Garfinkel, Jeffrey I. Schiller, Erik Nordlander, David Margrave, and Robert C. Miller. Views, reactions, and impact of digitally-signed mail in e-commerce. In *Financial Cryptography and Data Security 2005*. Springer Verlag, 2005. To Appear.

[Gut96] Peter Gutmann. Secure deletion of data from magnetic and solid-state memory. In *Sixth USENIX Security Symposium Proceedings*. Usenix, San Jose, California, July 22-25 1996. `http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html`. Online paper has been updated since presentation in 1996.

[Gut00] Peter Gutmann. X.509 style guide, October 2000. `http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt`.

[Gut01] Peter Gutmann. Pki technology survey and blueprint, 2001. `http://www.cs.auckland.ac.nz/~pgut001/pubs/pkitech.pdf`.

[Gut02a] Peter Gutmann. Lessons learned in implementing and deploying crypto software. In *Proc of the 11th Usenix Security Symposium*. Usenix, San Francisco, California, 2002.

[Gut02b] Peter Gutmann. PKI: It's not dead, just resting, August 2002. `http://www.cs.auckland.ac.nz/~pgut001/pubs/notdead.pdf`. Extended article with many more citations on the author's home page.

[Gut02c] Peter Gutmann. PKI: It's not dead, just resting. *Computer*, 35:41–49, August 2002.

[Gut03] Peter Gutmann. Plug-and-play PKI: A PKI your mother can use. In *12th USENIX Security Symposium*, pages 45–58. Usenix, August 4–8 2003. `http://www.usenix.org/events/sec03/tech/gutmann.html`.

[Gut04a] Peter Gutmann. Everything you never wanted to know about pki but were forced to find out, 2004. `http://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf`. Slides of Gutmann's PKI Tutorial.

[Gut04b] Peter Gutmann. Why isn't the Internet secure yet, dammit. In *AusCERT Asia Pacific Information Technology Security Conference 2004; Computer Security: Are we there yet?* AusCERT, May 2004. http://www.cs.auckland.ac.nz/~pgut001/pubs/dammit.pdf.

[GVU99] GVU. GVU's tenth WWW user survey results, 1999. http://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/.

[Hal03] Richard Hale. Personal communication, 2003.

[Har05] Jason Harris. Keyring stats, March 20 2005. http://keyserver.kjsl.com/~jharris/ka/2005-03-20/keyring_stats.

[Has02] Judi Hasson. VA toughens security after PC disposal blunders. *Federal Computer Week*, August 26 2002.

[HB05] Phillip Hallam-Baker. Re: [hcisec] outlook bug: altered digitally signed messages not reported, April 1 2005. Message-ID a123a5d6050401105218cffc7a@mail.gmail.com sent to the HCI-SEC mailing list.

[Hil05] Hillside.net. Hillside history, 2005. http://hillside.net/history.html.

[HK92] S. Hardcastle-Kille. RFC 1327: Mapping between X.400(1988) /ISO 10021 and RFC 822, May 1992. Obsoleted by RFC1495, RFC2156 [AKM+93, Kil98]. Obsoletes RFC987, RFC1026, RFC1138, RFC1148 [Kil86, Kil87, Kil89, Kil90]. Updates RFC0822, RFC0822 [Cro82a, Cro82a]. Status: PROPOSED STANDARD.

[Hod05] Carolyn Hodge. Personal communication, April 19 2005.

[Hof99] P. Hoffman. RFC 2634: Enhanced security services for s/mime, June 1999.

[Hop04] Clearing your Internet surfing history, 2004. http://www.hopeforhealing.org/clear. Cited on November 18, 2004.

[Hor05] Darik Horn. Darik's boot and nuke, March 2005. dban.sourceforget.net. Cited on April 2, 2005.

[Hos00] Hilary H. Hosmer. Visualizing risks: Icons for information attack scenarios. In *23rd National Information Systems Security Conference*. National Institute of Standards and Technology, October 16–19 2000.

[Hos04] Philipp Hoschka. W3c interaction domain, October 28 2004. http://www.w3.org/Interaction/.

[How04] Michael Howard. Attack surface: Mitigate security risks by minimizing the code you expose to untrusted users. *MSDN Magazine*, November 2004. http://msdn.microsoft.com/msdnmag/issues/04/11/AttackSurface/default.aspx.

[HPZ04] Stephanie Hackett, Bambang Parmanto, and Xiaoming Zeng. Accessibility of internet websites through time. In *The 6th International ACM/SIGCAPH Conference on Assistive Technologies*, pages 32–39. ACM Press, October 18–20 2004.

[Hug93] Eric Hughes. A cypherpunk's manifesto, March 9 1993. http://www.activism.net/cypherpunk/manifesto.html.

[Hus05] Hushmail.com. How Hushmail works, 2005. http://www.hushmail.com/about-how. Accessed on March 20, 2005.

[Ile04] Dan Ilett. Trojan poses as lycos europe screensaver. *CNET News.com*, December 7 2004. http://news.com.com/Trojan+poses+as+Lycos+Europe+screensaver/2100-7349_3-5481674.html.

[Ing05] Cheridan Inglis. Personal communication from thawte public relations, February 26 2005.

[Ins98] American National Standards Institute. ANSI Z535.4 product safety signs and labels, 1998.

[ISO00] ISO. *BS ISO/IEC 17799: 2000 (BS 7799-1:2000): Information Technology — Code of Practice for Information Security Management*. British Standards Institute, 2000.

[Jen97] Brian Michael Jenkins. Protecting surface transportation systems and patrons from terrorist activities case studies of security practices and a chronology of attacks, December 1997. http://citeseer.ist.psu.edu/jenkins97protecting.html.

[Joh91] John C. Brezina. Digital ID (service mark), 1991. Serial Number 74208016.

[Joh00] Jeff Johnson. *GUI Bloopers: Dont's and Do's for Software Developers and Web Designers*. Morgan Kaufmann Publishers, 2000.

[Joh04] Alex Johnson. Shhh ... someone might hear you: Access to information sharply curtailed under ashcroft. *MSNBC*, November 18 2004. http://msnbc.msn.com/id/6512840/.

[JRS03] A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy, 2003. citeseer.nj.nec.com/juels03blocker.html.

[JtM00] Uwe Jendricke and Daniela Gerd tom Markotten. Usability meets security - the identity-manager as your personal security assistant for the internet. In *ACSAC '00: Proceedings of the 16th Annual Computer Security Applications Conference*, page 344. IEEE Computer Society, December 2000. ISBN 0-7695-0859-6. http://www.acsac.org/2000/papers/90.pdf.

[Jur05] Juran Institute. Our founder, 2005. http://www.juran.com/lower_2.cfm?article_id=21. Discussion of the so-called Pareto principle at the Juran Institute's website.

[Jus04] Mike Just. Designing and evaluating challenge-question systems. *Security & Privacy Magazine*, 2:32–39, Sept–Oct 2004.

[Jus05] Mike Just. Designing authentication systems with challenge questions. In Lorrie Cranor and Simson Garfinkel, editors, *Security and Usability*. O'Reilly, 2005. To appear in August 2005.

[Kar89] Clare-Marie Karat. Iterative usability testing of a security application. In *Proceedings of the Human Factors Society 33rd Annual Meeting—1989*, pages 273–277. Human Factors & Ergonomics Society, 1989.

[Kas01] Frank Kastenholz. Re: skeeter & bubba tcp options?, November 30 2001. http://www.postel.org/pipermail/internet-history/2001-November/000071.html. in message 200111300021.fAU0LW508101@boreas.isi.edu sent to the Internet-History mailing list.

[KBK05] Clare-Marie Karat, Carolyn Brodie, and John Karat. Usability design and evaluation for privacy and security solutions. In Lorrie Cranor and Simson Garfinkel, editors, *Security and Usability*. O'Reilly, 2005. To appear in August 2005.

[KBS04] Gene Kim, Kevin Behr, and George Spafford. *The Visible Ops Handbook: Starting ITIL in 4 Practical Steps*. Information Technology Process Institute, June 2004.

[KDP02] D. Kirovski, M. Drinic, and M. Potkonjak. Enabling trusted software integrity, 2002. http://citeseer.ist.psu.edu/kirovski02enabling.html.

[Kei03] Richard Keightley. Encase version 3.0 manual revision 3.18, 2003. http://www.guidancesoftware.com/.

[Ken93] S. Kent. RFC 1422: Privacy enhancement for Internet electronic mail: Part II: Certificate-based key management, February 1993. Obsoletes RFC1114. Status: PROPOSED STANDARD.

[Kic03] Russ Kick. The justice dept's attorney workforce diversity study—uncensored, October 21 2003. http://www.thememoryhole.org/feds/doj-attorney-diversity.htm.

[Kil86] S. E. Kille. RFC 987: Mapping between X.400 and RFC 822, June 1, 1986. Obsoleted by RFC2156 [Kil98]. Updated by RFC1026, RFC1138, RFC1148 [Kil87, Kil89, Kil90]. Status: UNKNOWN.

[Kil87] S. E. Kille. RFC 1026: Addendum to RFC 987: (mapping between X.400 and RFC-822), September 1, 1987. Obsoleted by RFC1327, RFC1495, RFC2156 [HK92, AKM+93, Kil98]. Updates RFC0987 [Kil86]. Updated by RFC1138, RFC1148 [Kil89, Kil90]. Status: UNKNOWN.

[Kil89] S. E. Kille. RFC 1138: Mapping between X.400(1988) /ISO 10021 and RFC 822, December 1, 1989. Obsoleted by RFC1327, RFC1495, RFC2156 [HK92, AKM+93, Kil98]. Updates RFC0822, RFC0987, RFC1026 [Cro82a, Kil86, Kil87]. Updated by RFC1148 [Kil90]. Status: EXPERIMENTAL.

[Kil90] S. E. Kille. RFC 1148: Mapping between X.400(1988) /ISO 10021 and RFC 822, March 1, 1990. Obsoleted by RFC1327, RFC1495, RFC2156 [HK92, AKM+93, Kil98]. Updates RFC0822, RFC0987, RFC1026, RFC1138 [Cro82a, Kil86, Kil87, Kil89]. Status: EXPERIMENTAL.

[Kil98] S. Kille. RFC 2156: MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME, January 1998. Obsoletes RFC0987, RFC1026, RFC1138, RFC1148, RFC1327, RFC1495 [Kil86, Kil87, Kil89, Kil90, HK92, AKM+93]. Updates RFC0822 [Cro82a]. Status: PROPOSED STANDARD.

[Kin01] Kingpin. Palm OS password lockout bypass, March 2001. `http://www.atstake.com/research/advisories/2001/a030101-1.txt`. CAN-2001-0157.

[KMRT96] T. Krauskopf, J. Miller, P. Resnick, and W. Treese. Pics label distribution label syntax and communication protocols, version 1.1, 1996. W3C Recommendation REC-PICS-labels-961031.

[Koh78] Loren M. Kohnfelder. Towards a practical public-key cryptosystem, May 1978. Undergraduate thesis supervised by L. Adleman.

[Koo99] Bert-Jaap Koops. *The Crypto Controversy: A Key Conflict in the Information SOciety*. Kluwer Law International, 1999.

[Koz04] Charles M. Kozierok. Extended prml (eprml). *PCGuide.com*, 2004. `http://www.pcguide.com/ref/hdd/geom/dataEPRML-c.html`.

[KPS02] Charlie Kaufman, Radia Perlman, and Mike Speciner. *Network Security: Private Communication in a Public World*. Prentice Hall, second edition, 2002.

[KS94] Gene H. Kim and Eugene H. Spafford. The design and implementation of tripwire: A file system integrity checker. In *ACM Conference on Computer and Communications Security*, pages 18–29. ACM Press, 1994. `citeseer.ist.psu.edu/article/kim93design.html`.

[KSS+97] Jeffrey O. Kephart, Gregory B. Sorkin, Morton Swimmer, , and Steve R. White. Blueprint for a computer immune system. In *Proceedings of the 1997 Virus Bulletin International Conference*. Virus Bulletin Ltd., October 1–3 1997. `http://www.research.ibm.com/antivirus/SciPapers/Kephart/VB97/`.

[Lam05] Butler Lampson. Computer security in the real world, March 18 2005. Invited talk at Harvard University.

[Las97] Alex Lash. Utah grants first certificate authority. *C—Net News.Com*, December 3 1997. http://news.com.com/Utah+grants+first+certificate+authority/2100-1023_3-205932.html.

[Lau05] Robin Laurén. Re: PGP fingerprints on business cards and hash visualizations, March 28 2005. Message ID 6a9e4b98050328062248d2551f@mail.gmail.com posted to the hcisec@yahoogroups.com mailing list.

[Lav04] Lavasoft. Protect your privacy, 2004. http://www.lavasoftusa.com/. Cited December 1, 2004.

[Lea94] Doug Lea. Design patterns for avionics control systems. Technical Report DSSA Adage Project ADAGE-OSW-94-01, SUNY Oswego & NY CASE Center, 1994. http://g.oswego.edu/dl/acs/acs/acs.html.

[Lev04] Benjamin Levy. Personal communication, January 19 2004.

[Lew90] Peter H. Lewis. 'Little black boxes' that can save a hard drive. *The New York Times*, April 29 1990.

[Ley04a] John Leyden. Meet the peeping tom worm. *The Register*, August 2004. http://www.theregister.co.uk/2004/08/23/peeping_tom_worm/.

[Ley04b] John Leyden. Oops! firm accidentally ebays customer database. *The Register*, June 7 2004. http://www.theregister.co.uk/2004/06/07/hdd_wipe_shortcomings/.

[LFS92] A. S. Levy, S. B. Fein, and R. E. Schucker. More effective nutrition label formats are not necessarily preferred. *Journal of the American Diet Association*, 10:1230–1234, October 1992. PMID 1401661.

[LHDL04] Scott Lederer, Jason I. Hong, Anid K. Dey, and James A. Landay. Personal privacy through understanding and action: Five pitfalls for designers. In *Personal and Ubiquitious Computing*. Springer-Verlag, 2004.

[LHDL05] Scott Lederer, Jason I. Hong, Anid K. Dey, and James A. Landay. Five pitfalls in the design for privacy. In Lorrie Cranor and Simson Garfinkel, editors, *Security and Usability*. O'Reilly, 2005. To appear in August 2005.

[Lie04] Håkon Wium Lie. personal communication, July 2004.

[Lin87] J. Linn. RFC 989: Privacy enhancement for Internet electronic mail: Part I: Message encipherment and authentication procedures, February 1, 1987. Obsoleted by RFC1040, RFC1113. Status: UNKNOWN.

[Lin93] J. Linn. RFC 1421: Privacy enhancement for Internet electronic mail: Part I: Message encryption and authentication procedures, February 1993. Obsoletes RFC1113. Status: PROPOSED STANDARD.

[LK01] Stefan Ludwig and Winfried Kalfa. File system encryption with integrated user management. *SIGOPS Oper. Syst. Rev.*, 35(4):88–93, 2001. ISSN 0163-5980.

[Loi04] Eleanor T. Loiacono. Cyberaccess: web accessibility and corporate america. *Commun. ACM*, 47(12):82–87, 2004. ISSN 0001-0782.

[Lub04] Alan Luber. Beware of spyware, adware & sneakware. *Smart Computing*, 15:47–50, August 2004. http://www.smartcomputing.com/editorial/article.asp?article=articles/2004/s1508/14s08/14s08.asp.

[Lud02] Stephanie Ludi. Access for everyone: Introducing accessibility issues to students in internet programming courses. In *32nd ASEE/IEEE Frontiers in Education Conference*, pages S1C–7 – 9. IEEE, November 6–9 2002.

[LW04] Jörg Lehmann and André Wobst. Pyx reference manual, December 15 2004. http://pyx.sourceforge.net.

[Lym01] Jay Lyman. Troubled dot-coms may expose confidential client data. *NewsFactor Network*, August 8 2001. http://www.newsfactor.com/perl/story/12612.html.

[M.04] Rich M. SSL's credibility as phishing defense is tested, March 8 2004. http://news.netcraft.com/archives/2004/03/08/ssls_credibility_as_phishing_defense_is_tested.html.

[Mac97] Courtney Macavinta. TRUSTe marks down privacy labels. *CNET News.com*, September 17 1997. http://news.com.com/2100-1023-203339.html.

[Man92] B. Manning. RFC 1348: DNS NSAP RRs, July 1992. Obsoleted by RFC1637 [MC94a]. Updates RFC1034, RFC1035 [Moc87b, Moc87c]. Updated by RFC1637 [MC94a]. Status: EXPERIMENTAL.

[Mar97] John Markoff. Patient files turn up in used computer. *New York Times*, April 1997.

[Mar03] Aaron Marcus. Universal, ubiquitious, user-interface design for the disabled and elderly. *Interactions*, pages 23–27, March/April 2003.

[Mar05a] Gervase Markham. IDN spoofing strategy, February 15 2005. http://weblogs.mozillazine.org/gerv/archives/007556.html.

[Mar05b] David Martin. Re: [hcisec] test of S/MIME signature: Message 2 of 2 (personal communication), 2005.

[Maz00] David Mazières. *Self-certifying File System*. PhD thesis, Massachusetts Institute of Technology, May 2000.

[MBA05] George Moromisato, Paul Boyd, and Nimisha Asthagiri. Achieving usable security in groove virtual office. In Lorrie Cranor and Simson Garfinkel, editors, *Security and Usability*. O'Reilly, 2005. To appear in August 2005.

[MC94a] B. Manning and R. Colella. RFC 1637: DNS NSAP resource records, June 1994. Obsoleted by RFC1706 [MC94b]. Obsoletes RFC1348 [Man92]. Updates RFC1348 [Man92]. Status: EXPERIMENTAL.

[MC94b] B. Manning and R. Colella. RFC 1706: DNS NSAP resource records, October 1994. Obsoletes RFC1637 [MC94a]. Status: INFORMATIONAL.

[McF03] Paul McFedries. The word spy—bluejacking, November 2003. `http://www.wordspy.com/words/bluejacking.asp`. Cited on September 19, 2004.

[ME91] Scott Muller and Alan C. Elliott. *QueGuide to Data Recovery*. Que Corporation, 1991.

[MGS03] Haralambos Mouratidis, Paolo Giorgini, and Markus Schumacher. Security patterns for agent systems. In *Eighth European Conference on Pattern Languages of Programs*. unknown publisher, June 25–29 2003. `http://dit.unitn.it/~pgiorgio/papers/EuroPLoP03.pdf`.

[Mic00] Microsoft. Microsoft extensible firmware initiative FAT32 file system specification, December 6 2000. `http://www.microsoft.com/hwdev/download/hardware/fatgen103.pdf`.

[Mic01] Microsoft. Farewell Clippy: what's happening to the infamous office assistant in office XP, April 11 2001. `http://www.microsoft.com/presspass/features/2001/apr01/04-11clippy.asp`.

[Mic02] Microsoft. Encrypting file system in windows xp and windows server 2003, August 1 2002. `www.microsoft.com/technet/ prodtechnol/winxppro/deploy/cryptfs.mspx`. Updated April 11, 2003; cited November 11, 2004.

[Mic03a] Microsoft. How to clear the history entries in Internet Explorer, December 16 2003. `http://support.microsoft.com/kb/157729`.

[Mic03b] Microsoft. OL2000: how Outlook promotes and demotes menus based on usage, September 29 2003. `http://support.microsoft.com/default.aspx?scid=kb;en-us;220939`.

[Mic03c] Microsoft. Windows server 2003 security guide. *Microsoft TechNet*, April 23 2003. `http://www.microsoft.com/technet/security/prodtech/windowsserver2003/W2003HG/SGCH00.mspx`.

[Mic04] How and why to clear your cache, 2004. `http://www.microsoft.com/windows/ie/using/howto/customizing/clearcache.mspx`. Cited on November 18, 2004.

[Mic05] Microsoft. Next-generation secure computing base, 2005. `http://www.microsoft.com/resources/ngscb/default.mspx`. Cited on April 2, 2005.

[MIT03] MIT IST. Q: When i log into the web client i am getting a message that says my password is being sent in the clear, is that true?, June 9 2003. http://itinfo.mit.edu/answer.php?id=1187.

[MIT04] MIT. Building 32 – 8th floor, Ray and Maria Stata Center, space accounting floorplan, MIT Department of Facilities, 2004. http://floorplans.mit.edu/pdfs/32_8.pdf.

[MJLF84] Marshall K. McKusick, William N. Joy, Samuel J. Leffler, and Robert S. Fabry. A fast file system for UNIX. *Computer Systems*, 2(3):181–197, 1984. citeseer.ist.psu.edu/article/mckusick84fast.html.

[MN04] M. Granger Morgan and Elaine Newton. Protecting public anonymity. *Issues in Science and Technology*, pages 83–90, Fall 2004.

[Moc83a] P. V. Mockapetris. RFC 882: Domain names: Concepts and facilities, November 1, 1983. Obsoleted by RFC1034, RFC1035 [Moc87b, Moc87c]. Updated by RFC0973 [Moc86]. Status: UNKNOWN.

[Moc83b] P. V. Mockapetris. RFC 883: Domain names: Implementation specification, November 1, 1983. Obsoleted by RFC1034, RFC1035 [Moc87b, Moc87c]. Updated by RFC0973 [Moc86]. Status: UNKNOWN.

[Moc86] P. V. Mockapetris. RFC 973: Domain system changes and observations, January 1, 1986. Obsoleted by RFC1034, RFC1035 [Moc87b, Moc87c]. Updates RFC0882, RFC0883 [Moc83a, Moc83b]. Status: UNKNOWN.

[Moc87a] P. Mockapetris. STD 13: Domain Names — Concepts and Facilities, November 1987. See also RFC1034, RFC1035 [Moc87b, Moc87c].

[Moc87b] P. V. Mockapetris. RFC 1034: Domain names — concepts and facilities, November 1, 1987. Obsoletes RFC0973, RFC0882, RFC0883 [Moc86, Moc83a, Moc83b]. See also STD0013 [Moc87a]. Updated by RFC1101, RFC1183, RFC1348, RFC1876, RFC1982, RFC2065, RFC2181, RFC2308 [Moc89, EMUM90, Man92, DVGD96, EB96, ErK97, EB97, And98]. Status: STANDARD.

[Moc87c] P. V. Mockapetris. RFC 1035: Domain names — implementation and specification, November 1, 1987. Obsoletes RFC0973, RFC0882, RFC0883 [Moc86, Moc83a, Moc83b]. See also STD0013 [Moc87a]. Updated by RFC1101, RFC1183, RFC1348, RFC1876, RFC1982, RFC1995, RFC1996, RFC2065, RFC2181, RFC2136, RFC2137, RFC2308 [Moc89, EMUM90, Man92, DVGD96, EB96, Oht96, Vix96, ErK97, EB97, VTRB97, Eas97, And98]. Status: STANDARD.

[Moc89] P. V. Mockapetris. RFC 1101: DNS encoding of network names and other types, April 1, 1989. Updates RFC1034, RFC1035 [Moc87b, Moc87c]. Status: UNKNOWN.

[Mon02] John Monroe. Personal communication, September 23 2002.

[MS02] Kevin D. Mitnick and William L. Simon. *The Art of Deception*. John Wiley & Sons, 2002.

[MT79] Robert Morris and Ken Thompson. Password security: a case history. *Commun. ACM*, 22(11):594–597, 1979. ISSN 0001-0782.

[Mxx04] Mxxcon. Important patch for all xp-sp2 users!, August 11 2004. `http://forum.emule-project.net/index.php?showtopic=56016`.

[Nat89] National Research Concil, Committee on Risk Perception and Communication. *Improving Risk Communication*. National Academy Press, 1989.

[Nat05] National Security Agency. Security-Enhanced Linux, 2005. `http://www.nsa.gov/selinux/`.

[NC05] National Security Agency and Central Security Service. Nsa/css storage device declassification manual, 2005. NSA/CSS Policy Manual 9-12 (Draft).

[Net94a] Netscape Communications. Netscape Communications offers new network navigator free on the Internet, October 13 1994. `http://cgi.netscape.com/newsref/pr/newsrelease1.html`.

[Net94b] Netscape Communications. Netscape communications ships release 1.0 of netscape navigator and netscape servers, December 15 1994. `http://cgi.netscape.com/newsref/pr/newsrelease8.html`.

[Net97] Preview release of netscape communicator fuels use of web-based email netscape teams with content and service providers to encourage users to try next-generation email client, 1997. `http://wp.netscape.com/newsref/pr/newsrelease314.html`.

[Net05a] Netcraft. April 2005 web server survey, April 2005. `http://news.netcraft.com/archives/web_server_survey.html`.

[Net05b] Microsoft Developer Network. DeleteFile, 2005. `http://msdn.microsoft.com/library/en-us/fileio/base/deletefile.asp`.

[Neu90] Peter G. Neumann. Inside risks: a few old coincidences. *Commun. ACM*, 33(9):202, 1990. ISSN 0001-0782.

[Nic05] Stuart Nicholson. Re: s/mime (personal communication), January 25 2005.

[Nie89] Jakob Nielsen. Usability engineering at a discount. In G. Salvendy and M. J. Smith, editors, *Designing and Using Human-Computer Interfaces and Knowledge Based Systems*, pages 394–401. Elsevier Science Publishers, 1989.

[Nie90] Jakob Nielsen. Big paybacks from 'discount' usability engineering. *IEEE Software*, 7:107–108, May 1990.

[Nie93a] Jakob Nielsen. Iterative user-interface design. *Computer*, 26(11):32–41, 1993. ISSN 0018-9162.

[Nie93b] Jakob Nielsen. *Usability Engineering*. Academic Press, 1993.

[Nie94] Jakob Nielsen. Guerrilla HCI: using discount usability engineering to penetrate the intimidation barrier. *useit.com*, 1994. http://www.useit.com/papers/guerrilla_hci.html.

[NIS85] Password usage, 1985. http://www.itl.nist.gov/fipspubs/fip112.htm.

[NIS93] Automated password generator (apg), 1993. http://www.itl.nist.gov/fipspubs/fip181.htm.

[Nor83] Donald A. Norman. Design rules based on analyses of human error. *Commun. ACM*, 26(4), April 1983.

[Nor97] Don Norman. Privacy and car navigational systems. *The Risks Digest*, 19, May 31 1997. http://catless.ncl.ac.uk/Risks/19.20.html\#subj3.1.

[Nor05] Eric Norman. Re: [hcisec] PGP fingerprints on business cards and hash visualization. *hcisec@yahoogroups.com*, March 26 2005. Message-ID 0a7a6191c82f5c11d29d3ce53232f35f@doit.wisc.edu.

[NP81] Larry Niven and Jerry Pournelle. *Oath Of Fealty*. Simon & Schuster, September 1981.

[NTK02a] Hard news, July 12 2002. http://www.ntk.net/2002/07/12/.

[NTK02b] Yahoo's seven word fragments you can't say in html email, July 12 2002. http://www.ntk.net/2002/07/12/yahoo.txt.

[NTN02] Samir Nanavati, Michael Thieme, and Raj Nanavati. *Biometrics: Identity Verification in a Networked World*. John Wiley & Sons, Inc., 2002.

[OH04] Timothy L. O'Brien and Saul Hansell. Barbarians at the digital gate. *New York Times*, September 19 2004.

[Oht96] M. Ohta. RFC 1995: Incremental zone transfer in DNS, August 1996. Updates RFC1035 [Moc87c]. Status: PROPOSED STANDARD.

[oM98] National Library of Medicine. Pure food and drugs, April 27 1998. http://www.nlm.nih.gov/exhibition/phs_history/106.html. Cited on April 18, 2005.

[OR04] Diana Oblinger and Laura Ruby. Accessible technology: Opening doors for disabled students. *NACUBO Business Officer*, pages 27–31, January 2004.

[Org80] Organisation for Economic Co-operation and Development. Guidelines on the protection of privacy and transborder flows of personal data, 1980. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[pal05] palmOne, Inc. Resetting your device (soft, system/warm, hard, in-cradle, power down, battery disconnect, zero out), 2005. http://kb.palmone.com/SRVS/CGI-BIN/WEBCGI.EXE?New,Kb=PalmSupportKB,ts=Palm_External2001,case=obj(887). Solution ID 887.

[Per03] Mindy Pereira. *Trusted S/MIME Gateways*. Dartmouth College, May 2003. Senior Honors Thesis: Winter/Spring 2003, Department of Computer Science, Dartmouth College.

[Per05a] Radia Perlman. The ephemerizer: Making data disappear. Technical Report SMLI TR-2005-140, Sun Labs, Sun Microsystems, February 2005. http://research.sun.com/techrep/2005/smli_tr-2005-140.pdf.

[Per05b] Radia Perlman. Personal communication, March 22 2005.

[PEW05] Pew Internet & American Life Project, 2005. http://www.pewinternet.org/.

[PGP98] PGPdisk, 1998. http://www.pgpi.org/products/pgpdisk. version 6.02.

[PKW04] Alan Peacock, Xian Ke, and Matthew Wilkerson. Typing patterns: a key to user identification. *Security & Privacy Magazine*, 2:40–47, Sept–Oct 2004.

[PLF03] Andrew Patrick, A. Chris Long, and Scott Flinn, editors. *Workshop on Human-Computer Interaction and Security Systems, part of CHI2003*. ACM Press, Fort Lauderdale, Florida, April 5-10 2003. http://www.andrewpatrick.ca/CHI2003/HCISEC/.

[Por00a] John D. Porter. Crypt-randpasswd-.0.2, July 21 2000. http://search.cpan.org/~jdporter/Crypt-RandPasswd-0.02/.

[Por00b] John D. Porter. Crypt::randpasswd, 2000. http://search.cpan.org/~jdporter/Crypt-RandPasswd-0.02/lib/Crypt/RandPasswd.pm.

[Pos80a] J. Postel. RFC 768: User datagram protocol, August 28, 1980. Status: STANDARD. See also STD0006 [Pos80b].

[Pos80b] J. Postel. STD 6: User Datagram Protocol, August 1980. See also RFC0768 [Pos80a].

[Pou03] Kevin Poulsen. Justice e-censorship gaffe sparks controversy. *SecurityFocus*, October 23 2003. http://www.theregister.co.uk/2003/10/23/justice_ecensorship_gaffe_sparks_controversy/.

[Pre05] President's Information Technology Advisory Committee. Cyber security: A crisis of prioritization, February 2005. Report to the President.

[Pri03] Privacy Rights Clearinghouse. RFID position statement of consumer privacy and civil liberties organizations, November 20 2003. http://www.privacyrights.org/ar/RFIDposition.htm.

[Pro04] The Honeynet Project. Trend: Life expectancy increasing for unpatched or vulnerable Linux deployments. *Know Your Enemy — Trend Analysis*, December 17 2004. http://www.honeynet.org/papers/trends/life-linux.pdf.

[PS99] Adrian Perrig and Dawn Song. Hash visualization: a new technique to improve real-world security. In Manuel Blum and C. H. Lee, editors, *Cryptographic Techniques and E-COmmerce: Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce (CryTEC '99)*, pages 131–138. City University of Hong Kong Press, 1999. citeseer.ist.psu.edu/perrig99hash.html.

[Raj03] RajuAbju Inc. History of AOL warez, 2003. http://www.rajuabju.com/warezirc/historyofaolwarez.htm.

[Ram04a] B. Ramsdell. RFC 3850: Secure/multipurpose Internet mail extensions (S/MIME) version 3.1 certificate handling, July 2004.

[Ram04b] B. Ramsdell. RFC 3851: Secure/multipurpose Internet mail extensions (S/MIME) version 3.1 message specification, July 2004.

[Ras00] Jef Raskin. The humane interface (book excerpt). *Ubiquity*, 1(14):3, 2000.

[Ray03] Eric S. Raymond. *The Art of UNIX Programming*, chapter Chapter 11: Interfaces; Applying the Rule of Least Surprise. Addison-Wesley Profesional, 2003. http://www.faqs.org/docs/artu/ch11s01.html.

[Rei87] Brian Reid. Reflections on some recent widespread computer break-ins. *Commun. ACM*, 30(2):103–105, 1987. ISSN 0001-0782.

[Rei04] Tom Reinke, November 9 2004. Telephone interview with Director of Technology.

[Rek99a] Jun Rekimoto. Time-machine computing, 1999. http://www.csl.sony.co.jp/person/rekimoto/tmc/. Cited on April 1, 2005.

[Rek99b] Jun Rekimoto. Time-machine computing: A time-centric approach for the information environment. In *ACM Symposium on User Interface Software and Technology*, pages 45–54. ACM Press, 1999. citeseer.nj.nec.com/rekimoto99timemachine.html.

[Ren05] Karen Renauld. Evaluating authentication mechanisms. In Lorrie Cranor and Simson Garfinkel, editors, *Security and Usability*. O'Reilly, 2005. To appear in August 2005.

[Res01] P. Resnick. RFC 2822: Internet message format, April 2001 2001.

[Ric05] Robert Richardson. Factor x 2: Are passwords really so bad? Are tokens any better? *Computer Security Alert*, pages 1–4, January 2005.

[Riv04] Ronald Rivest. Personal communication, September 2004.

[Rob04a] Mark Roberti. Legislation isn't the answer. *RFID Journal*, July 19 2004. http://www.rfidjournal.com/article/articleview/1031/1/2/.

[Rob04b] Paul Roberts. AOL survey finds rampant online threats, clueless users. *Computerworld*, October 23 2004. http://www.computerworld.com/securitytopics/security/story/0,10801,96918,00.html.

[Ros00] James M. Rosenbaum. In defense of the DELETE key. *The Green Bag*, 3(4):393–396, Summer 2000.

[Ros05] Seth Ross. Ten general security rules 1–5. *Securius.com*, 1(5), 2005. http://www.securius.com/newsletters/Ten_General_Security_Rules_1-5.html.

[Rot05] Volker Roth. A user-centric approach to encrypted e-mail. *International Journal of Human-Computer Studies*, 2005. Tenatively accepted for publication.

[RP94] J. Reynolds and J. Postel. RFC 1700: ASSIGNED NUMBERS, October 1994. See also STD0002. Obsoletes RFC1340. Status: STANDARD.

[RSA99] RSA Laboratories. PKCS #12: Personal information exchange syntax standard, June 24 1999. http://www.rsasecurity.com/rsalabs/node.asp?id=2138.

[RT78] D. M. Ritchie and K. Thompson. The UNIX time-sharing system. *The Bell System Technical Journal*, 57(6 (part 2)):1905+, 1978. citeseer.ist.psu.edu/ritchie74unix.html.

[Rub03] Laura Ruby. Federal regulation creates economic incentives for competition, innovation among technology companies. *Information Technology and Disabilities*, 9(1), October 2003. http://www.rit.edu/~easi/itd/itdv09n1/ruby.htm.

[SÖ2] Eva Söderström. Standardising the business vocabulary of standards. In *SAC '02: Proceedings of the 2002 ACM symposium on Applied computing*, pages 1048–1052. ACM Press, 2002. ISBN 1-58113-445-2.

[SA99] Frank Stajano and Ross Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *1999 AT&T Software Symposium*, pages 172–194. AT&T, September 15 1999. citeseer.ist.psu.edu/stajano99resurrecting.html.

[SA04] Stephen Shankland and Scott Ard. Document shows SCO prepped lawsuit against BofA. *News.Com*, March 4 2004. http://news.com.com/2100-7344_3-5170073.html.

[Sal96] Arto Salomaa. *Public Key Cryptography*. Springer-Verlag, 1996.

[Sal04] Jerome Saltzer. Personal communication, 2004.

[Sam05] Geetanjali Sampemane. Re: [hcisec] test of S/MIME signature: Message 1 of 2 (personal communication), 2005.

[SAN04] SANS Institute. The twenty most critical internet security vulnerabilities (updated) — the experts consensus, October 8 2004. http://www.sans.org/top20/.

[Sas03] M. Angela Sasse. Computer security: Anatomy of a usability disaster, and a plan for recovery. In *Workshop on Human-Computer Interaction and Security Systems, part of CHI2003*. ACM Press, April 2003. citeseer.ist.psu.edu/618589.html.

[Sas04a] M. Angela Sasse. Personal communication, July 2004.

[Sas04b] M. Angela Sasse. Usability and trust in information systems. In Robin Mansell and Brian S. Collins, editors, *Cyber Trust in Information Societies*. Edward Elgar, 2004.

[SB04] Tobias Straub and Harald Baier. A framework for evaluating the usability and the utility of PKI-enabled applications. In *Public Key Infrastructure: First European PKI Workshop: Research and Applications, EuroPKI 2004, Samos Island, Greece, June 25-26, 2004. Proceedings*, volume 3093, pages 112–125. Technische Universitat Darmstadt, 2004. http://www.informatik.tu-darmstadt.de/ftp/pub/TI/TR/TI-04-05.paper_usability.pdf.

[SC04] Securities and Exchange Commission. 17 cfr part 248, disposal of consumer report information. *Federal Register*, 69(235):71322 – 71329, December 8 2004. http://www.sec.gov/rules/final/34-50781.pdf. Final Rule.

[Sca04] Sarah D. Scalet. Scumware out there. *CSO*, November 2004. http://www.csoonline.com/read/110104/sware.html.

[Sch96] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons, 1996.

[Sch03a] Markus Schumacher. *Security Engineering with Patterns*. PhD thesis, Darmstadt University of Technology, May 2003.

[Sch03b] Markus Schumacher. *Security Engineering with Patterns: Origins, Theoretical Models, and Ne Applications*. Springer, 2003. LCNS 2754.

[Sch04a] Jeffrey I. Schiller. Personal communication, August 28 2004. Text originally written for inclusion in [GNM+05] but omitted due to space constraints.

[Sch04b] Sarah Schweitzer. Parties call foul over N. H. phone-jaming suit. *The Boston Globe*, October 23 2004.

[Sec04] RSA Security. American Online and RSA securty launch AOL passcode premium service, September 21 2004. http://www.rsasecurity.com/press_release.asp?doc_id=5033.

[Sec05a] RSA Security. E*TRADE financial offers RSA SecurID two-factor authentication solution to its U.S. retail customers, March 1 2005. http://www.rsasecurity.com/press_release.asp?doc_id=5567.

[Sec05b] SecuritySpace.com. SSL server survey – certificate authority (CA) market share, March 2005. http://www.securityspace.com/sspace/.

[SFJ96] Douglas C. Schmidt, Mohamed Fayad, and Ralph E. Johnson. Software patterns. *Commun. ACM*, 39(10):37–39, 1996. ISSN 0001-0782.

[SFPM04] Paul Slovic, Melissa L. Finucane, Ellen Peters, and Donald G. MacGregor. Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk and rationality. *Risk Analysis*, 24(2), 2004.

[SG02] D. K. Smetters and R. E. Grinter. Moving from the design of usable security technologies to the design of useful secure applications. In *NSPW '02: Proceedings of the 2002 workshop on New security paradigms*, pages 82–89. ACM Press, 2002. ISBN 1-58113-598-X.

[SGS+00] John D. Strunk, Garth R. Goodson, Michael L. Scheinholtz, Craig A.N. Soules, and Gregory R. Ganger. Self-securing storage: Protecting data in compromised systems. In *Proceedings of the 4th USENIX OSDI Symposium*, pages 165–180. Usenix, October 23–25 2000. http://www.usenix.org/events/osdi2000/full_papers/strunk/strunk_html/.

[Sha85] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 47–53. Springer-Verlag New York, Inc., New York, NY, USA, 1985. ISBN 0-387-15658-5.

[Sha04] Sharman Networks. Kazaa — the guide, 2004. http://www.kazaa.com/us/help/new_nospy.htm.

[SHF97] Anil Somayaji, Steven Hofmeyr, and Stephanie Forrest. Principles of a computer immune system. In *Meeting on New Security Paradigms*, pages 75–82. New York, NY, USA : ACM, 1998, September 23–26 1997. ISBN 0897919866. citeseer.ist.psu.edu/11313.html.

[Shn82] Ben Shneiderman. The future of interactive systems and the emergence of direct manipulation. *Behaviour and Information Technology*, 1:237–256, 1982.

[Sho95] Adam Shostack. An overview of shttp, May 1995. http://www.homeport.org/~adam/shttp.html. Unpublished.

[Sip95] Janice C. Sipior. The ethical and legal quandary of email privacy. *Communications of the ACM*, 38(12):48–54, December 1995.

[SK03] Kimberly Stone and Richard Keightley. Can computer investigations survive Windows XP? Technical report, Guidance Software, 2003. http://www.guidancesoftware.com/corporate/whitepapers/downloads/XPwhitepaper.pdf.

[SK05] Jerome H. Saltzer and M. Frans Kaashoek. Topics in the engineering of computer systems (working title), 2005. http://mit.edu/6.033/www/reference.html. draft release 2.0.

[SMM00] P. Slovic, J. Monahan, and D. M. MacGregor. Violence risk assessment and risk communication: The effects of using actual cases, providing instructions, and employing probability vs. frequency formats. *Law and Human Behavior*, 24:271–296, 2000.

[Som02] Anil Somayaji. *Operating System Stability and Security through Process Homeostasis*. PhD thesis, University of New Mexico, July 2002. http://www.cs.unm.edu/~immsec/publications/soma-diss.pdf.

[Sop04] Sophos. W32/rbot-gr, October 2004. http://www.sophos.com/virusinfo/analyses/w32rbotgr.html.

[Sot05] Lisa J. Sotto. New Federal rule on disposal of consumer information. *Privacy Officers Advisor*, pages 12–14, January 2005.

[SP98] Perdita Stevens and Rob Pooley. Systems reengineering patterns. In *SIGSOFT '98/FSE-6: Proceedings of the 6th ACM SIGSOFT international symposium on Foundations of software engineering*, pages 17–23. ACM Press, 1998. ISBN 1-58113-108-9.

[Spi03] Diomidis Spinellis. Organized pruning of file sets. *;login:*, 28:39–42, June 2003. http://www.spinellis.gr/pubs/trade/2003-login-prune/html/prune.html.

[Spr03] Tom Spring. Hard drives exposed: We bought or salvaged ten used drives and found sensitive business and personal data on all but one. *PCWorld*, May 2003. http://www.pcworld.com/news/article/0,aid,110012,00.asp.

[SQ95] Michelle Slatalla and Joshua Quittner. *Masters of Deception: The Gang That Ruled Cyberspace*. Harper-Collins, 1995.

[SR03] Arvind Singhal and Everett M. Rogers. *Combatting AIDS: Communication Strategies in Action*. Sage Publications, 2003.

[SS75] Jerome H. Saltzer and Michael D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63:1278–1308, September 1975.

[Sta01] Richard M. Stallman. GNU general public license, 2001. http://www.gnu.org/copyleft/gpl.html. Cited November 16, 2004.

[Sta03] William Stallings. *Cryptography and Network Security*. Prentice Hall, 2003.

[Sti97] Harrell W. Stiles. Credit card check digit validation, 1997. http://www.beachnet.com/~hstiles/cardtype.html.

[Sto04] Debbie Stolper. Personal communication, January 1 2004.

[Swe04] Claire Swedberg. California RFID legislation rejected. *RFID Journal*, July 5 2004. http://www.rfidjournal.com/article/articleview/1015/1/1/.

[Sym04] Symantec. Symantec security response—w32.klez.h@mm, June6 2004. http://securityresponse.symantec.com/avcenter/venc/data/w32.klez.h@mm.html.

[Tan97] John C. Tang. *Eliminating a hardware switch: weighing economics and values in a design decision*. Center for the Study of Language and Information, Stanford, CA, USA, 1997. ISBN 1-57586-080-5. 259–269 pp.

[Tec04] Pointsec Mobile Technologies. A fiver buys access & log-in codes to major financial services group, June 8 2004. http://www.pointsec.com/news/news_pressrelease.asp?PressID=2004_June_8.

[Tec05] TechSmith. Camtasia studio, 2005. http://www.techsmith.com/products/studio/.

[Tel01] Telecommunication Standardizaton Sector. *ITU-T recommendation X.509 — ISO/ITEC 9594-8: Information Technology—Open Systems Interconnection—The Directory: Public-Key and Attribute Certificate Frameworks*. International Telecommunication Union, February 23 2001. COM 7-250-E Revision 1.

[The04] The Mozilla Organization. Mozilla jargon file, September 9 2004. http://www.mozilla.org/docs/jargon.html.

[The05a] The Council of European National TLD Registries. Centr statement on IDN homograph attacks, February 22 2005. http://www.centr.org/docs/2005/02/homographs.html.

[The05b] The Japan Times. Bug in antivirus software hits LANs at JR east, some media. *The Japan Times Online*, April 24 2005. http://www.japantimes.com/cgi-bin/getarticle.pl5?nn20050424a2.htm.

[Tog05] Bruce Tognazzini. Design for usability. In Lorrie Cranor and Simson Garfinkel, editors, *Security and Usability*. O'Reilly, 2005. To appear in August 2005.

[TR03] Mary Frances Theofanos and Janice Redish. Bridging the gap between accessibility and usability. *Interactions*, pages 36–45, November/December 2003.

[Tre04] Ambrose Treacy. Re: Bug in handling of S/MIME-signed mail in outlook 2003 (personal communication), October 27 2004.

[Tro05] Trolltech. Qt 3.3 whitepaper, 2005. http://www.trolltech.com/products/whitepapers.html.

[TRU04] TRUSTe. TRUSTe's mission, 2004. http://www.truste.org/about/mission_statement.php. Cited on April 17, 2005.

[TW03] Jamie Twycross and Matthew M. Williamson. Implementing and testing a virus throttle. In *12th Usenix Security Symposium*. Usenix, 2003. http://www.usenix.org/events/sec03/tech/full_papers/twycross/twycross_html/implementation.html.

[UDoHoAPDS73] Education US Department of Health and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems. *Records, Computers, and Rights of Citizens; report*. MIT Press, 1973.

[US 04] Usability: Usability basics, 2004. http://www.usability.gov/basics/.

[US88] California v. Greenwood, May 16 1988. 486 US 35.

[US03] The fair and accurate credit transactions act of 2003, 2003. Public Law 108-159, 117 Stat. 1952.

[U.S04] VISA U.S.A. Payment card industry data security standard, December 2004. http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf.

[USA04] United States of America v. Bradford C. Councilman, June 29 2004. http://www.ca1.uscourts.gov/pdf.opinions/03-1383-01A.pdf. No. 03-1383 (1st Cir).

[Uta95] Utah. Utah Digital Signature Act, Utah Code §§46-3-101 to 46-3-504, 1995. ch. 61.

[vdBG05] Stephen R. van den Berg and Philip Guenther. Procmail homepage, 2005. http://www.procmail.org.

[Ver96] VeriSign, Inc. Digital ID (service mark), 1996. Serial Number 75160774.

[Ver05a] VeriSign. Certificate interoperability service, 2005. http://www.verisign.com/products-services/security-services/pki/cert-interoperability/. Last accessed April 15, 2005.

[Ver05b] VeriSign. Verisign certification practice statement, version 3.0, April 1 2005. http://www.verisign.com/repository/CPS/VeriSignCPSv3_03.15.05.pdf.

[Ver05c] Inc. VeriSign. Manage SSL certificates from VeriSign, Inc., 2005. http://www.verisign.com/products-services/security-services/ssl/current-ssl-customers/manage-ssl-certificates/index.html. Cited on March 22, 2005.

[Vic01] Kim J. Vicente. Crazy clocks: Counterintuitive consequences of "intelligent" automation. *IEEE Intelligent Systems*, pages 74–76, November / December 2001.

[Vil02] Matt Villano. Hard-drive magic: Making data disappear forever. *New York Times*, May 2 2002.

[Vir04] Virginia Joint Commission on Technology & Science. 2004–2005 commission work plan, May 26 2004. `http://jcots.state.va.us/publications/work\%20plans/workplan04.htm`.

[VIS05] VISA. Cardholder information security program, 2005. `http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html`.

[Vix96] P. Vixie. RFC 1996: A mechanism for prompt notification of zone changes (DNS NOTIFY), August 1996. Updates RFC1035 [Moc87c]. Status: PROPOSED STANDARD.

[VTRB97] P. Vixie, Editor, S. Thomson, Y. Rekhter, and J. Bound. RFC 2136: Dynamic updates in the domain name system (DNS UPDATE), April 1997. Updates RFC1035 [Moc87c]. Status: PROPOSED STANDARD.

[Wal02] Carl A. Waldspurger. Memory resource management in VMware ESX server. *SIGOPS Oper. Syst. Rev.*, 36(SI):181–194, 2002. ISSN 0163-5980.

[Wat05] Watchfire Corporation. Welcome to Bobby WorldWide, 2005. `http://bobby.watchfire.com/bobby`.

[WBG+87] Charles Cresson Wood, William W. Banks, Sergio B. Guarro, Abel A. Garcia, Viktor E. Hampel, and Henry P. Sartorio. *Computer Security: A Comprehensive Controls Checklist*. John Wiley & Sons, 1987. Edited by Abel A. Garcia.

[WCO00] Larry Wall, Tom Christiansen, and Jon Orwant. *Programming Perl (3rd Edition)*. O'Reilly, 2000.

[WCSJ02] Michael S. Wogalter, Vincent C. Conzola, and Tonya L. Smith-Jackson. Research-based guidelines for warning design and evaluation. *Applied Ergonomics*, 33, 2002.

[WDL99] M. S. Wogalter, D. M. DeJoy, and K. R. Laughery. *Warnings and Risk Communication*. Taylor and Francis, 1999.

[Wei03] S. A. Weis. Security and privacy in radio-frequency identification devices, 2003.

[WFSB93] Michael S. Wogalter, R. M. Forbes, L. J. Van't Slot, and T. Barlow. Facilitating communication of label information and warnings by increasing the surface area and print size on small product containers. In *Proc Interface 93*, pages 181–186. Human Factors Society, 1993.

[Whi00] Alma Whitten. People to invite. *chisec@groups.yahoo.com*, May 12 2000. `http://groups.yahoo.com/group/hcisec/message/1`.

[Whi03] Alma Whitten. personal website., 2003. `http://www.gaudior.net/alma/`.

[Whi04a] Alma Whitten. *Making Security Usable*. PhD thesis, School of Computer Science, Carnegie Mellon University, 2004.

[Whi04b] Alma Whitten. Personal communication, December 6 2004.

[Wik] Wikipedia. X.400. http://en.wikipedia.org/wiki/X.400. Cited on March 22, 2005.

[Wil03] Matthew M. Williamson. Design, implementation and test of an email virus throttle, June 2003. citeseer.ist.psu.edu/705198.html. HPL-2003-118.

[Wil05] Jeff Williams. Unsafe at any (CPU) speed, April 30 2005. http://www.aspectsecurity.com/documents/Aspect_HCSS_Brief.ppt.

[WKH97] M. Wahl, S. Kille, and T. Howes. RFC 2253: Lightweight Directory Access Protocol (v3): UTF-8 string representation of distinguished names, December 1997. Status: PROPOSED STANDARD.

[Won00] Edward Wong. Web site lists Iran coup names. *The New York Times*, June 24 2000. http://www.library.cornell.edu/colldev/mideast/irnytrep.htm.

[Woo84] Charles C. Wood. Logging, security experts, data base, and crypto key management. In *Proceedings ACM'84 Annual Conference: The Fifth Generation Challenge*. ACM Press, October 8–10 1984.

[Woo04] Paul Woolverton. Computer files hang around, Theer trial shows. *The Fayetteville (NC) Observer*, October 25 2004. http://www.fayettevillenc.com/story.php?Template=local&Story=6645176.

[Wor96] Anthony Worsley. Which nutrition information do shoppers want on food labels? *Asia Pacific Journal of Clinical Nutrition*, 5:70–78, 1996. http://elecpress.monash.edu.au/APJCN/Vol5/Num2/52p70.htm.

[WR95] Suzanne P. Weisband and Bruce A. Reinig. Managing user perceptions of email privacy. *Commun. ACM*, 38(12):40–47, 1995. ISSN 0001-0782.

[WRA04] Theer found guilty of murder, conspiracy, December 3 2004. http://www.wral.com/fayettevillenews/3969062/detail.html.

[WT98] Alma Whitten and J. D. Tygar. Usability of security: A case study. Technical report, Carnegie Mellon University, December 1998. citeseer.ist.psu.edu/whitten98usability.html.

[WT99] Alma Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *8th USENIX Security Symposium*, pages 169–184. Usenix, 1999. citeseer.nj.nec.com/whitten99why.html.

[WT03] Alma Whitten and J. D. Tygar. Safe staging for computer security. In *Workshop on Human-Computer Interaction and Security Systems, part of CHI2003*. CHI, ACM SIGCHI, 2003. http://132.246.128.219/CHI2003/HCISEC/hcisec-workshop-whitten.pdf.

[WY94] Michael S. Wogalter and Stephen L. Young. The effect of alternative product-label design on warning compliance. *Applied Ergonomics*, 25:53–57, 1994.

[XSC04] Jun Xiao, John Stasko, and Richard Catrambone. An empirical study of the effect of agent competence on user performance and perception. In *AAMAS '04: Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems*, pages 178–185. IEEE Computer Society, Washington, DC, USA, 2004. ISBN 1-58113-864-4.

[Yam97] K. Yamagishi. When a 12.86% mortality rate is more dangerous than 24.14%: Implications for risk communication. *Applied Cognitive Psychology*, 11:495–506, 1997.

[YBAG04] Jeff Yan, Alan Blackwell, Ross Anderson, and Alasdair Grant. Password memorability and security: empirical results. *Security & Privacy Magazine*, 2:25–31, Sept–Oct 2004.

[Yee02] Ka-Ping Yee. User interaction design for secure systems. In *Proceedings of the 4th International Conference on Information and Communications Security*. Springer-Verlag, 2002. LNCS 2513.

[Yee03] Ka-Ping Yee. Secure interaction design and the principle of least authority. In *Workshop on Human-Computer Interaction and Security Systems, part of CHI2003*. ACM SIGCHI, 2003. `http://sims.berkeley.edu/~ping/sid/yee-sid-chi2003-workshop.pdf`.

[Yee04] Ka-Ping Yee. Aligning security and usability. *Security & Privacy Magazine*, 2: 48–55, Sept–Oct 2004.

[Yee05a] Ka-Ping Yee. Goals for strategies for secure interaction design, 2005.

[Yee05b] Ka-Ping Yee. Guidelines and strategies for secure interaction design. In Lorrie Cranor and Simson Garfinkel, editors, *Security and Usability*. O'Reilly, 2005. To appear in August 2005.

[Ylo96] T. Ylonen. SSH - secure login connections over the Internet. In *Proceedings of the 6th Security Symposium) (USENIX Association: Berkeley, CA)*, page 37. Usenix, 1996. `http://citeseer.nj.nec.com/ylonen96ssh.html`.

[YS02] Zishuang (Eileen) Ye and Sean Smith. Trusted paths for browsers. In 11^{th} *Usenix Security Symposium*. Usenix, August 2002.

[ZE01] Panayiotis Zaphiris and R. Darin Ellis. Website usability and content accessibility of the top usa universities. In *In Proceedings of WebNet 2001 Conference*. Association for the Advancement of Computing in Education, October 23–27 2001.

[Zel04] Kim Zelonis. Avoiding the cyber pandemic: A public health approach to preventing malware propagation, Fall 2004. Master's Thesis.

[Zim91a] Philip Zimmermann. pgp.c, June 1991.

[Zim91b] Philip Zimmermann. Pretty good privacy: Rsa public key cryptography for the masses, June 5 1991.

[Zim91c] Philip Zimmermann. Public key crypto freeware protects e-mail. *RISKS Digest*, June 7 1991.

[Zim95] Philip R. Zimmermann. *The Official PGP User's Guide*. MIT Press, 1995.

[Zim00] Philip Zimmermann. Statement made at the 'future of PGP luncheon' at the the eleventh conference on computers, freedom and privacy, 2000.

[Zon04] Zone Labs. Internet security products, online safety, software, protection, 2004. `http://www.zonelabs.com/`. Cited December 1, 2004.

[ZS96] Mary Ellen Zurko and Richard T. Simon. User-centered security. In *NSPW '96: Proceedings of the 1996 workshop on New security paradigms*, pages 27–33. ACM Press, New York, NY, USA, 1996. ISBN 0-89791-944-0.

[Zur05a] Mary Ellen Zurko. *Designing Secure Systems that People Can Use*, chapter Embedding Security in Collaborative Applications: A Lotus Notes/Domino Perspective. O'Reilly, 2005.

[Zur05b] Mary Ellen Zurko. Lotus notes/domino: Embedding security in collaborative applications. In Lorrie Cranor and Simson Garfinkel, editors, *Security and Usability*. O'Reilly, 2005. To appear in August 2005.

[ZZ01] Panayiotis Zaphiris and Giorgos Zacharia. Website content accessibility of 30,000 cypriot web sites. In *Proceedings of the 8th Panhellenic Conference on Informatics. Nicosia, Cyprus*, pages 128–136. Springer-Verlag, November 8–10 2001. `citeseer.ist.psu.edu/442526.html`.