



Bibliography

- [1] M Abadi, "Explicit Communications Revisited: Two New Attacks on Authentication Protocols", in *IEEE Transactions on Software Engineering* v 23 no 3 (Mar 97) pp 185–186
- [2] M Abadi, RM Needham, "Prudent Engineering Practice for Cryptographic Protocols", *IEEE Transactions on Software Engineering* v 22 no 1 (Jan 96) pp 6–15; also as DEC SRC Research Report no 125 (June 1 1994) at <ftp://gatekeeper.pa.dec.com/pub/DEC/SRC/research-reports/SRC-125.pdf>
- [3] A Abbasi, HC Chen, "Visualizing Authorship for Identification", in *ISI 2006*, LNCS 3975 pp 60–71
- [4] H Abelson, RJ Anderson, SM Bellovin, J Benaloh, M Blaze, W Diffie, J Gilmore, PG Neumann, RL Rivest, JI Schiller, B Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption", in *World Wide Web Journal* v 2 no 3 (Summer 1997) pp 241–257
- [5] A Abulafia, S Brown, S Abramovich-Bar, "A Fraudulent Case Involving Novel Ink Eradication Methods", in *Journal of Forensic Sciences* v 41 (1996) pp 300–302
- [6] DG Abraham, GM Dolan, GP Double, JV Stevens, "Transaction Security System", in *IBM Systems Journal* v 30 no 2 (1991) pp 206–229
- [7] N Achs, "VISA confronts the con men", *Cards International* (20 Oct 1992) pp 8–9

- [8] A Acquisti, A Friedman, R Telang, "Is There a Cost to Privacy Breaches?", *Fifth Workshop on the Economics of Information Security* (2006)
- [9] EN Adams, "Optimising preventive maintenance of software products", *IBM Journal of Research and Development*, v 28 no 1 (1984) pp 2–14
- [10] J Adams, 'Risk', University College London Press (1995), ISBN 1-85728-067-9
- [11] J Adams, "Cars, Cholera and Cows: the management of risk and uncertainty", in *Policy Analysis* no 335, Cato Institute, Washington, 1999; at <http://www.cato.org/pubs/pas/pa-335es.html>
- [12] B Adida, M Bond, J Clulow, A Lin, RJ Anderson, RL Rivest, "A Note on EMV Secure Messaging in the IBM 4758 CCA", at www.ross-anderson.com
- [13] Y Adini, Y Moses, S Ullman, "Face recognition: The Problem of Compensating for Changes in Illumination Direction", in *IEEE Transactions on Pattern Analysis and Machine Intelligence* v 19 no 7 (July 97) pp 721–732
- [14] A Adler, "Sample images can be independently restored from face recognition templates", in *Proc. Can. Conf. Elec. Comp. Eng.* (2003) pp 1163–1166; at <http://www.sce.carleton.ca/faculty/adler/publications/publications.html>
- [15] A Adler, "Vulnerabilities in biometric encryption systems", in *NATO RTA Workshop: Enhancing Information Systems Security–Biometrics* (IST-044-RWS-007), at <http://www.sce.carleton.ca/faculty/adler/publications/publications.html>
- [16] The AES Lounge, <http://www.iaik.tu-graz.ac.at/research/krypto/AES/>
- [17] C Ajluni, "Two New Imaging Techniques Promise To Improve IC Defect Identification", in *Electronic Design* v 43 no 14 (10 July 1995) pp 37–38
- [18] Y Akdeniz, "Regulation of Child Pornography on the Internet" (Dec 1999), at <http://www.cyber-rights.org/reports/child.htm>
- [19] G Akerlof, "The Market for 'Lemons: Quality Uncertainty and the Market Mechanism", in *The Quarterly Journal of Economics* v 84 no 3 (1970) pp 488–500

- [20] R Albert, HW Jeong, AL Barabási, "Error and attack tolerance of complex networks", in *Nature* v 406 no 1 (2000) pp 387–482
- [21] J Alfke, "Facebook and Decentralized Identifiers", in *Thought Palace* Dec 2 2007; at <http://mooseyard.com/Jens/2007/12/facebook-and-decentralized-identifiers>
- [22] Alliance to Outfox Phone Fraud, hosted by Verizon at <http://www.bell-atl.com/security/fraud/> but now withdrawn; as of August 2007, Verizon had its own scam alert page at <http://www22.verizon.com/pages/securityalerts/>
- [23] M Allman, V Paxson, "Issues and Etiquette Concerning Use of Shared Measurement Data", in *Internet Measurement Conference (IMC 2007)*, at <http://www.imconf.net/imc-2007/papers/imc80.pdf>
- [24] F Almgren, G Andersson, T Granlund, L Ivansson, S Ulfberg, "How We Cracked the Code Book Ciphers", at <http://codebook.org>
- [25] American Society for Industrial Security, <http://www.asisonline.org>
- [26] American Statistical Association, *Privacy, Confidentiality, and Data Security web site*, at <http://www.amstat.org/comm/cmtepc/>
- [27] E Amoroso, 'Fundamentals of Computer Security Technology', Prentice Hall (1994); ISBN 0-13-10829-3
- [28] B Andersen, M Frenz, "The Impact of Music Downloads and P2P File-Sharing on the Purchase of Music: A Study for Industry Canada", 2007, at http://strategis.ic.gc.ca/epic/site/ippd-dppi.nsf/en/h_ip01456e.html
- [29] J Anderson, 'Computer Security Technology Planning Study', ESD-TR-73-51, US Air Force Electronic Systems Division (1973) <http://csrc.nist.gov/publications/history/index.html>
- [30] M Anderson, C North, J Griffin, R Milner, J Yesberg, K Yiu, "Starlight: Interactive Link", in *12th Annual Computer Security Applications Conference* (1996) proceedings published by the IEEE, ISBN 0-8186-7606-XA, pp 55–63
- [31] M Anderson, W Seltzer, *Official Statistics and Statistical Confidentiality: Recent Writings and Essential Documents*, at <http://www.uwm.edu/%7Emargo/govstat/integrity.htm>
- [32] RJ Anderson, "Solving a Class of Stream Ciphers", in *Cryptologia* v XIV no 3 (July 1990) pp 285–288

- [33] RJ Anderson, "Why Cryptosystems Fail" in *Communications of the ACM* v 37 no 11 (November 1994) pp 32–40; earlier version at <http://www.cl.cam.ac.uk/users/rja14/wcf.html>
- [34] RJ Anderson, "Liability and Computer Security: Nine Principles", in *Computer Security—ESORICS 94*, Springer LNCS v 875 pp 231–245
- [35] RJ Anderson, "Crypto in Europe—Markets, Law and Policy", in *Cryptography: Policy and Algorithms*, Springer LNCS v 1029 pp 75–89
- [36] RJ Anderson, "Clinical System Security—Interim Guidelines", in *British Medical Journal* v 312 no 7023 (13th January 1996) pp 109–111; <http://www.cl.cam.ac.uk/ftp/users/rja14/guidelines.txt>
- [37] RJ Anderson, 'Security in Clinical Information Systems', published by the British Medical Association (1996); ISBN 0-7279-1048-5
- [38] RJ Anderson, "A Security Policy Model for Clinical Information Systems", in *Proceedings of the 1996 IEEE Symposium on Security and Privacy* pp 30–43 <http://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html>
- [39] RJ Anderson, "An Update on the BMA Security Policy", in [43] pp 233–250; <http://www.cl.cam.ac.uk/ftp/users/rja14/bmaupdate.ps.gz>
- [40] RJ Anderson, C Manifavas, C Sutherland, "NetCard — A Practical Electronic Cash Scheme" in *Security Protocols* (1996), Springer LNCS v 1189 pp 49–57
- [41] RJ Anderson, "The Eternity Service", in *Proceedings of Pragocrypt 96* (GC UCMP, ISBN 80-01-01502-5) pp 242–252
- [42] RJ Anderson (ed), *Proceedings of the First International Workshop on Information Hiding* (1996), Springer LNCS v 1174
- [43] RJ Anderson (ed), 'Personal Medical Information—Security, Engineering and Ethics', Springer-Verlag (1997) ISBN 3-540-63244-1
- [44] RJ Anderson, "GSM hack—operator flunks the challenge", in *comp.risks* v 19.48: <http://catless.ncl.ac.uk/Risks/19.48.html>
- [45] RJ Anderson, "On the Security of Digital Tachographs", in *Computer Security—ESORICS 98*, Springer LNCS v 1485 pp 111–125; <http://www.cl.cam.ac.uk/ftp/users/rja14/tacho5.ps.gz>

- [46] RJ Anderson, "Safety and Privacy in Clinical Information Systems", in *'Rethinking IT and Health'*, J Lenaghan (ed), IPPR (Nov 98) (ISBN 1-86030-077-4) pp 140–160
- [47] RJ Anderson, "The DeCODE Proposal for an Icelandic Health Database"; part of this was published in *Læknablaðið* (The Icelandic Medical Journal) v 84 no 11 (Nov 98) pp 874–5; full text available from <http://www.cl.cam.ac.uk/users/rja14/#Med>
- [48] RJ Anderson, "The Formal Verification of a Payment System", in *Industrial Strength Formal Methods: A Practitioners Handbook*, MG Hinchey and JP Bowen (editors), Springer Verlag (Sep 1999, 1-85233-640-4) pp 43–52
- [49] RJ Anderson, "How to Cheat at the Lottery (or, Massively Parallel Requirements Engineering)", in *15th Annual Computer Security Application Conference* (1997); proceedings published by IEEE Computer Society, ISBN 0-7695-0346-2, pp xix–xxvii; at <http://www.cl.cam.ac.uk/~rja14/lottery/lottery.html>
- [50] RJ Anderson, "The Millennium Bug—Reasons not to Panic", at <http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/y2k.html>
- [51] RJ Anderson, "Comments on the Security Targets for the Icelandic Health Database", at <http://www.cl.cam.ac.uk/ftp/users/rja14/iceland-admiral.pdf>
- [52] "The Correctness of Crypto Transaction Sets", in *Proceedings of Protocols 2000*, Springer LNCS v 2133 pp 125–141
- [53] Ross Anderson, "Cryptography and Competition Policy—Issues with 'Trusted Computing' ", *Second Workshop on Economics and Information Security* (2003)
- [54] Ross Anderson, "Open and Closed Systems are Equivalent (that is, in an ideal world)", in *Perspectives on Free and Open Source Software*, MIT Press 2005, pp 127–142
- [55] RJ Anderson, "Closing the Phishing Hole—Fraud, Risk and Nonbanks", at *Nonbanks in the Payments System: Innovation, Competition, and Risk*, US Federal Reserve, Santa Fe, May 2–4 2007
- [56] RJ Anderson, "RFID and the Middleman", in *Proceedings of the Eleventh International Conference on Financial Cryptography and Data Security*, February 2007

- [57] RJ Anderson, "Searching for Evil", Tech talk given at Google, Aug 24 2007, at <http://video.google.com/videoplay?docid=-1380463341028815296>
- [58] RJ Anderson, 'Security Economics Resource Page', at <http://www.cl.cam.ac.uk/~rja14/econsec.html>
- [59] RJ Anderson, SJ Bezuidenhout, "On the Reliability of Electronic Payment Systems", in *IEEE Transactions on Software Engineering* v 22 no 5 (May 1996) pp 294–301; <http://www.cl.cam.ac.uk/ftp/users/rja14/prepay-meters.pdf>
- [60] RJ Anderson, E Biham, LR Knudsen, "Serpent: A Proposal for the Advanced Encryption Standard", submitted to NIST as an AES candidate; a short version of the paper appeared at the AES conference, August 1998; both papers available at [61]
- [61] RJ Anderson, E Biham, L Knudsen, 'The Serpent Home Page', <http://www.cl.cam.ac.uk/~rja14/serpent.html>
- [62] RJ Anderson, R Böhme, R Clayton, T Moore, 'Security Economics and the Internal Market', ENISA, 2008
- [63] RJ Anderson, M Bond, "API-Level Attacks on Embedded Systems", in *IEEE Computer* v 34 no 10 (October 2001) pp 67–75
- [64] RJ Anderson, M Bond, "Protocol Analysis, Composability and Computation" in *Computer Systems: Theory, Technology and Applications*, Springer 2003, pp 7–10
- [65] RJ Anderson, M Bond, J Clulow, S Skorobogatov, 'Cryptographic processors—a survey', Cambridge University Computer Laboratory Technical Report no 641 (July 2005); shortened version in *Proc. IEEE* v 94 no 2 (Feb 2006) pp 357–369
- [66] RJ Anderson, I Brown, R Clayton, T Dowty, D Korff, E Munro, 'Children's Databases—Safety and Privacy', Information Commissioner's Office, UK, Nov 2006
- [67] RJ Anderson, B Crispo, JH Lee, C Manifavas, V Matyás, FAP Petitcolas, 'The Global Internet Trust Register', MIT Press (1999) (ISBN 0-262-51105-3) <http://www.cl.cam.ac.uk/Research/Security/Trust-Register/>
- [68] RJ Anderson, MG Kuhn, "Tamper Resistance—a Cautionary Note", in *Proceedings of the Second Usenix Workshop on Electronic Commerce* (Nov 96) pp 1–11; <http://www.cl.cam.ac.uk/users/rja14/tamper.html>

- [69] RJ Anderson, MG Kuhn, "Low Cost Attacks on Tamper Resistant Devices", in *Security Protocols—Proceedings of the 5th International Workshop* (1997) Springer LNCS v 1361 pp 125–136
- [70] RJ Anderson, MG Kuhn, "Soft Tempest—An Opportunity for NATO", at *Protecting NATO Information Systems In The 21st Century*, Washington DC, Oct 25–26, 1999
- [71] RJ Anderson, JH Lee, "Jikzi: A New Framework for Secure Publishing", in *Security Protocols 99*, Springer LNCS v 1976 pp 21–36
- [72] RJ Anderson, TW Moore, "Information Security Economics—and Beyond", in *Advances in Cryptology—Crypto 2007*, Springer LNCS 4622, pp 68–91
- [73] RJ Anderson, RM Needham, "Robustness principles for public key protocols", in *Advances in Cryptology—Crypto 95* Springer LNCS v 963 pp 236–247; <http://www.cl.cam.ac.uk/ftp/users/rja14/robustness.ps.gz>
- [74] RJ Anderson, RM Needham, "Programming Satan's Computer" in *Computer Science Today*, Springer Lecture Notes in Computer Science v 1000 (1995) pp 426–441; <http://www.cl.cam.ac.uk/ftp/users/rja14/satan.ps.gz>
- [75] RJ Anderson, RM Needham, A Shamir, "The Steganographic File System", in *Proceedings of the Second International Workshop on Information Hiding*, Springer LNCS v 1525 pp 74–84
- [76] RJ Anderson, MR Roe, "The GCHQ Protocol and Its Problems", in *Advances in Cryptology—Eurocrypt 97*, Springer LNCS v 1233 pp 134–148; <http://www.cl.cam.ac.uk/ftp/users/rja14/euroclipper.ps.gz>
- [77] CM Andrew, V Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, Basic Books (1999) ISBN 0-46500310-9
- [78] M Andrews, JA Whitaker, *How to Break Web Software*, Addison-Wesley 2006
- [79] <http://www.anonymizer.com>
- [80] JC Anselmo, "US Seen More Vulnerable to Electromagnetic Attack", in *Aviation Week and Space Technology* v 146 no 4 (28/7/97) p 67

- [81] A Antón, "Is That Vault Really Protecting Your Privacy?", at *theprivacyplace.org* Oct 9 2007; at <http://theprivacyplace.org/2007/10/09/is-that-vault-really-protecting-your-privacy/>
- [82] *Anonymity Bibliography*, 2007, at <http://freehaven.net/anonbib/>
- [83] APACS, "Fraud abroad drives up card fraud losses", October 3 2007; at http://www.apacs.org.uk/media_centre/press/03.10.07.html; see also *The Register*, http://www.theregister.co.uk/2007/10/03/card_fraud_trends/
- [84] APACS, "Payment Advice—Protect Your PIN", Aug 16 2007; at http://www.apacs.org.uk/media_centre/press/08.16.07.html and www.cardwatch.org.uk
- [85] T Appleby, "Chilling debit-card scam uncovered", in *The Globe and Mail* (10/12/1999) p 1
- [86] Arbor Networks Inc., 'Infrastructure Security Report', 2007, at <http://www.arbornetworks.com/report>
- [87] US Army, 'Electromagnetic Pulse (EMP) and Tempest Protection for Facilities', Corps of Engineers Publications Depot, Hyattsville (1990)
- [88] A Arora, R Krishnan, A Nandkumar, R Telang, YB Yang, "Impact of Vulnerability Disclosure and Patch Availability—An Empirical Analysis", *Third Workshop on the Economics of Information Security* (2004)
- [89] A Arora, CM Forman, A Nandkumar, R Telang, "Competitive and strategic effects in the timing of patch release", in *Workshop on the Economics of Information Security* (2006)
- [90] SE Asch, 'Social Psychology', OUP 1952
- [91] D Asonov, R Agrawal, "Keyboard Acoustic Emanations", IBM Almaden Research Center, 2004
- [92] 'ASPECT—Advanced Security for Personal Communications Technologies', at <http://www.esat.kuleuven.ac.be/cosic/aspect/index.html>
- [93] Associated Press, "Charges dropped against Ex-HP chairwoman—Three others charged in boardroom spying case receive no jail time", Mar 14 2007, at <http://www.msnbc.msn.com/id/17611695/>
- [94] R Atkinson, "The single most effective weapon against our deployed forces" and "The IED problem is getting out of control. We've got to stop the bleeding", in the *Washington Post*, Sep 30 2007; "There was a two-year learning curve . . . and a lot of people died in those two years", Oct 1 2007; "You can't armor your way out of this problem",

- Oct 2 2007; "If you don't go after the network, you're never going to stop these guys. Never", Oct 3 2007; all linked from <http://smallwarsjournal.com/blog/2007/09/print/weapon-of-choice/>
- [95] D Aubrey-Jones, "Internet — Virusnet?", in *Network Security* (Feb 97) pp 15–19
- [96] D Aucsmith, "Tamper-Resistant Software: An Implementation", in [42] pp 317–333
- [97] D Aucsmith (editor), *Proceedings of the Second International Workshop on Information Hiding* (Portland, Apr 98), Springer LNCS v 1525
- [98] B Audone, F Bresciani, "Signal Processing in Active Shielding and Direction-Finding Techniques", *IEEE Transactions on Electromagnetic Compatibility* v 38 no 3 (August 1996) pp 334–340
- [99] R Axelrod, *The Evolution of Cooperation*, Basic Books (1984)
- [100] I Ayres, SD Levitt, "Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack", in *Quarterly Journal of Economics* v 108 no 1 (Feb 1998), <http://www.nber.org/papers/w5928>
- [101] "Barclays winning card fraud war", D Austin, in *Banking Technology* (April 94) p 5
- [102] D Austin, "Flood warnings", in *Banking Technology* (Jul–Aug 1999) pp 28–31
- [103] "Computer Combat Rules Frustrate the Pentagon", in *Aviation Week and Space Technology* v 147 no 11 (15/9/97) pp 67–68
- [104] J Bacon, *Concurrent Systems*, Addison-Wesley (1997); ISBN 0-201-17767-6
- [105] J Bacon, K Moody, J Bates, R Hayton, CY Ma, A McNeil, O Seidel, M Spiteri, "Generic Support for Distributed Applications", in *IEEE Computer* (March 2000) pp 68–76
- [106] L Badger, DF Sterne, DL Sherman, KM Walker, SA Haghghat, "Practical Domain and Type Enforcement for UNIX," in *Proceedings of the 1995 IEEE Symposium on Security and Privacy* pp 66–77
- [107] M Baggott, "The smart way to fight fraud", *Scottish Banker* (Nov 95) pp 32–33
- [108] B Bain, "Justice says no to private PCs for telework", in *FCW.com*, Sep 13 2007; at <http://www.fcw.com/article103746-09-13-07>

- [109] SA Baker, PR Hurst, *The Limits of Trust*, Kluwer Law International (1998) ISBN 9-0411-0639-1
- [110] "Card Fraud: Banking's Boom Sector", in *Banking Automation Bulletin for Europe* (Mar 92) pp 1–5
- [111] D Balfanz, EW Felten, "Hand-Held Computers Can Be Better Smart Cards", in *Eighth USENIX Security Symposium* (1999), ISBN 1-880446-28-6, pp 15–23
- [112] J Bamford, *The Puzzle Palace: A Report on NSA, America's Most Secret Agency*, Houghton, Mifflin (1982–3rd Printing–revised edition due out shortly), ISBN 0-395-31286-8
- [113] Bank for International Settlements, *Security and Reliability in Electronic Systems for Payments*, British Computer Society (1982–no ISBN)
- [114] Bank for International Settlements, <http://www.bis.org/>
- [115] E Bangeman, "The insanity of France's anti-file-sharing plan: L'État, c'est IFPI", in *Ars Technica* Nov 25 2007; at <http://arstechnica.com/news.ars/post/20071125-the-insanity-and-genius-of-frances-anti-file-sharingplan.html>
- [116] M Barbaro, T Zeller, "A Face Is Exposed for AOL Searcher No. 4417749", in *New York Times* Aug 9 2006, at <http://query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63>
- [117] E Barkan, E Biham, N Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication" Technion Technical Report CS-2006-07, at <http://www.cs.technion.ac.il/~biham/>
- [118] RL Barnard, *Intrusion Detection Systems*, Butterworths (1988) ISBN 0-409-90030-3
- [119] A Barnett, "Britain's UFO secrets revealed", in *The Observer* (4/6/2000) at <http://www.observer.co.uk/uknews/story/0,6903,328010,00.html>
- [120] S Baron-Cohen, *The Essential Difference: Men, Women, and the Extreme Male Brain*, Penguin, 2003 ISBN 0141011017
- [121] J Barr, "The Gates of Hades", in *Linux World* April 2000; at <http://www.linuxworld.com/linuxworld/lw-2000-04/lw-04-vcontrol3.html>
- [122] B Barrow, B Quinn, "Millions in danger from chip and pin fraudsters" in *Daily Mail* June 5th 2006

- [123] R Baskerville, "Information Systems Security Design Methods: Implications for Information Systems Development", in *ACM Computing Surveys* v 265 (1993) pp 375–414
- [124] PJ Bass, "Telephone Cards and Technology Development as Experienced by GPT Telephone Systems", in *GEC Review* v 10 no 1 (95) pp 14–19
- [125] J Battelle, *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*, Portfolio, 2005
- [126] W Bax, V Dekker, "Met zijn allen meekijken in de medische kaartenbak", in *Trouw* Dec 11 2007, at <http://www.trouw.nl/deverdieping/overigeartikelen/article867144.ece/>
- [127] S Baxter, "US hits panic button as air force 'loses' nuclear missiles", in *Sunday Times* Oct 21 2007; at http://www.timesonline.co.uk/tol/news/world/us_and_americas/article2702800.ece
- [128] "Great Microprocessors of the Past and Present", at <http://www.cs.uregina.ca/~bayko/cpu.html>
- [129] BBC News Online, "Tax records 'for sale' scandal", Jan 16 2003, at <http://news.bbc.co.uk/1/hi/business/2662491.stm>
- [130] BBC News Online, " 'Relief' over fingerprint verdict", Feb 7 2006, at <http://news.bbc.co.uk/1/hi/scotland/4689218.stm>
- [131] BBC News Online, "UN warns on password 'explosion' ", Dec 4 2006, at <http://news.bbc.co.uk/1/hi/technology/6199372.stm>
- [132] BBC News Online, "Schools get rules on biometrics", July 23 2007, at <http://news.bbc.co.uk/1/hi/education/6912232.stm>
- [133] BBC News Online, "Mobile phone technology turns 20", Sep 7 2007, at <http://news.bbc.co.uk/1/hi/technology/6983869.stm>
- [134] BBC News Online, "PC stripper helps spam to spread", Oct 30 2007, at <http://news.bbc.co.uk/1/hi/technology/7067962.stm>
- [135] S Beattie, S Arnold, C Cowan, P Wagle, C Wright, "Timing the Application of Security Patches for Optimal Uptime", in *LISA XVI* (2002) pp 101–110
- [136] F Beck, *Integrated Circuit Failure Analysis—A Guide to Preparation Techniques*, Wiley (1998), ISBN 0-471-97401-3
- [137] J Beck, "Sources of Error in Forensic Handwriting Examination", in *Journal of Forensic Sciences* v 40 (1995) pp 78–87

- [138] GS Becker, "Crime and Punishment: An Economic Approach", in *Journal of Political Economy* v 76 no 2 (March/April 1968) pp 169–217
- [139] L Beckwith, M Burnett, V Grigoreanu, S Weidenbeck, "Gender HCI: What About the Software?", in *Computer* (Nov 2006) pp 97–101
- [140] L Beckwith, C Kissinger, M Burnett, S Weidenbeck, J Lowrance, A Blackwell, C Cook, "Tinkering and Gender in End-User Programmers' Debugging", in *CHI '06*, Montreal, April 2006; at <http://eusesconsortium.org/gender/>
- [141] S Begley, "Fingerprint Matches Come Under More Fire As Potentially Fallible", *Wall Street Journal* Oct 7 2005 p B1; at http://online.wsj.com/article_print/SB112864132376462238.html
- [142] HA Beker, C Amery, "Cryptography Policy", at <http://www.baltimore.com/library/whitepapers/mn.cryptography.html>
- [143] HJ Beker, JMK Friend, PW Halliden, "Simplifying key management in electronic fund transfer point of sale systems", in *Electronics Letters* v 19 (1983) pp 442–443
- [144] H Beker, F Piper, 'Cipher Systems', Northwood (1982)
- [145] H Beker, M Walker, "Key management for secure electronic funds transfer in a retail environment", in *Advances in Cryptology—Crypto 84* Springer LNCS v 196 pp 401–410
- [146] DE Bell, L LaPadula, 'Secure Computer Systems', ESD-TR-73-278, Mitre Corporation; v I and II: November 1973, v III: Apr 1974
- [147] M Bellare, J Kilian, P Rogaway, "The Security of Cipher Block Chaining" in *Advances in Cryptology—Crypto 94* Springer LNCS v 839 pp 341–358
- [148] M Bellare, P Rogaway, "Optimal Asymmetric Encryption", in *Advances in Cryptology—Eurocrypt 94*, Springer LNCS v 950 pp 103–113; see also RFC 2437, <http://sunsite.auc.dk/RFC/rfc/rfc2437.html>
- [149] SM Bellovin, "Packets Found on an Internet", in *Computer Communications Review* v 23 no 3 (July 1993) pp 26–31
- [150] SM Bellovin, "Defending Against Sequence Number Attacks", RFC 1948 (May 1996) at <http://sunsite.auc.dk/RFC/rfc/rfc1948.html>
- [151] SM Bellovin, "Problem Areas for the IP Security Protocols," in *Proceedings of the Sixth Usenix Unix Security Symposium* (1996); at <http://www.cs.columbia.edu/~smb/papers/badesp.pdf>

- [152] SM Bellovin, "Debit-card fraud in Canada", in *comp.risks* v 20.69; at <http://catless.ncl.ac.uk/Risks/20.69.html>
- [153] SM Bellovin, "Permissive Action Links", at <http://www.research.att.com/~smb/nsam-160/>
- [154] SM Bellovin, 'ICMP Traceback Messages', Internet Draft, March 2000, at <http://search.ietf.org/internet-drafts/draft-bellovin-itrace-00.txt>
- [155] SM Bellovin, "More on Comcast Blocking Peer-to-Peer Traffic", Oct 22 2007, at <http://www.cs.columbia.edu/~smb/blog/2007-10/2007-10-22.html>; and "Comcast Apparently Blocking Some Peer-to-Peer Traffic", Oct 19 2007, *ibid.*
- [156] S Bellovin, M Blaze, E Brickell, C Brooks, V Cerf, W Diffie, S Landau, J Peterson, J Treichler, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP" <http://www.itaa.org/news/docs/CALEAVOIPreport.pdf>
- [157] SM Bellovin, WR Cheswick, 'Firewalls and Internet Security: Repelling the Wily Hacker', Addison-Wesley (1994); ISBN: 0-201-63357-4
- [158] SM Bellovin, M Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", in *Proceedings of the IEEE Symposium on Security and Privacy* (1992) pp 72–84
- [159] M Benantar, R Guski, KM Triodle, "Access control systems: From host-centric to network-centric computing", in *IBM Systems Journal* v 35 no 1 (96) pp 94–112
- [160] W Bender, D Gruhl, N Morimoto, A Lu, "Techniques for Data Hiding", in *IBM Systems Journal* v 35 no 3–4 (96) pp 313–336
- [161] T Benkart, D Bitzer, "BFE Applicability to LAN Environments", in *Seventeenth National Computer Security Conference* (1994); proceedings published by NIST, pp 227–236
- [162] AD Biderman, H Zimmer, 'The Manipulation of Human Behavior', Wiley 1961; at <http://www.archive.org/details/TheManipulationOfHumanBehavior>
- [163] F Bergadano, B Crispo, G Ruffo, "Proactive Password Checking with Decision Trees", in *4th ACM Conference on Computer and Communications Security* (1997), proceedings published by the ACM, ISBN 0-89791-912-2, pp 67–77
- [164] DJ Bernstein, 'Cache-Timing Attacks on AES', preprint, 2005

- [165] T Berson, "Skype Security Evaluation", Oct 18 2005, from http://share.skype.com/sites/security/2005/10/skype_security_and_encryption.html
- [166] T Berson, G Barksdale, "KSOS: Development Methodology for a Secure Operating System", *AFIPS Conference proceedings* (1979)
- [167] Bewert, "All About NSA's and AT&T's Big Brother Machine, the Narus 6400", in *Dailykos* Apr 7 2006; at <http://www.dailykos.com/storyonly/2006/4/8/14724/28476/>
- [168] K Biba, '*Integrity Considerations for Secure Computer Systems*', Mitre Corporation MTR-3153 (1975)
- [169] E Biham, A Biryukov, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials" in *Advances in Cryptology—Eurocrypt 97*, Springer LNCS v 1592 pp 12–23
- [170] E Biham, A Shamir, '*Differential Cryptanalysis of the Data Encryption Standard*', Springer (1993) ISBN 0-387-97930-1
- [171] E Biham, A Shamir, "Differential Fault Analysis of Secret Key Cryptosystems", in *Advances in Cryptology—Crypto 97* Springer LNCS v 1294 pp 513–525
- [172] E Biham, O Dunkelman, S Indestege, N Keller, B Preneel, "How To Steal Cars—A Practical Attack on KeeLoq", 2007, at <http://www.cosic.esat.kuleuven.be/keeloq/>
- [173] A Biryukov, A Shamir, D Wagner, "Real Time Cryptanalysis of A5/1 on a PC", in *Fast Software Encryption* (2000)
- [174] R Bishop, R Bloomfield, "A Conservative Theory for Long-Term Reliability-Growth Prediction", in *IEEE Transactions on Reliability* v 45 no 4 (Dec 96) pp 550–560
- [175] DM Bishop, "Applying COMPUSEC to the battle field", in *17th Annual National Computer Security Conference* (1994) pp 318–326
- [176] M Bishop, M Dilger, "Checking for Race Conditions in File Accesses", in *Computing Systems Usenix* v 9 no 2 (Spring 1996) pp 131–152
- [177] Wolfgang Bitzer, Joachim Opfer '*Schaltungsanordnung zum Messen der Korrelationsfunktion zwischen zwei vorgegebenen Signalen*' [Circuit arrangement for measuring the correlation function between two provided signals]. German Patent DE 3911155 C2, Deutsches Patent amt, November 11, 1993

- [178] J Blackledge, "Making Money from Fractals and Chaos: Microbar", in *Mathematics Today* v 35 no 6 (Dec 99) pp 170–173
- [179] RD Blackledge, "DNA versus fingerprints", in *Journal of Forensic Sciences* v 40 (1995) p 534
- [180] B Blair, "Keeping Presidents in the Nuclear Dark", in *Bruce Blair's Nuclear Column*, Feb 11 2004, at <http://www.cdi.org/blair/permisiveaction-links.cfm>
- [181] GR Blakley, "Safeguarding cryptographic keys", in *Proceedings of NCC AFIPS* (1979), pp 313–317
- [182] B Blakley, R Blakley, RM Soley, 'CORBA Security: An Introduction to Safe Computing with Objects' Addison-Wesley (1999) ISBN 0-201-32565-9
- [183] MA Blaze, "Protocol Failure in the Escrowed Encryption Standard", in *Second ACM Conference on Computer and Communications Security*, 2–4 November 1994, Fairfax, Va; proceedings published by the ACM ISBN 0-89791-732-4, pp 59–67; at <http://www.crypto.com/papers/>
- [184] Matt Blaze, "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks", at *IEEE Symposium on Security and Privacy* 2003, at <http://www.crypto.com/papers/mk.pdf>
- [185] MA Blaze, "Toward a Broader View of Security Protocols", in *Security Protocols 2004*, Springer LNCS v 3957, pp 106–132
- [186] MA Blaze, "Safecracking for the computer scientist", U. Penn Technical Report (2004), at <http://www.crypto.com/papers/>
- [187] MA Blaze, SM Bellovin, "Tapping, Tapping On My Network Door", in *Communications of the ACM* (Oct 2000), *Inside Risks* 124; at <http://www.crypto.com/papers/carnivore-risks.html>
- [188] MA Blaze, J Feigenbaum, J Lacy, "Decentralized Trust Management", in *Proceedings of the 1996 IEEE Symposium on Security and Privacy* pp 164–173
- [189] D Bleichenbacher, "Chosen Ciphertext Attacks against Protocols Based on the RSA Encryption Standard PKCS #1", in *Advances in Cryptology—Crypto 98* Springer LNCS v 1462 pp 1–12
- [190] G Bleumer, 'Electronic Postage Systems—Technology, Security, Economics', Springer 2006; ISBN 0-387-29313-2
- [191] G Bleumer, M Schunter, "Digital patient assistants: privacy vs cost in compulsory health insurance", in *Health Informatics Journal* v 4 nos 3–4 (Dec 1998) pp 138–156

- [192] B Blobel, "Clinical record Systems in Oncology. Experiences and Developments on Cancer Registers in Eastern Germany", in [43] pp 39–56
- [193] JA Bloom, IJ Cox, T Kalker, JPMG Linnartz, ML Miller, CBS Traw, "Copy Protection for DVD Video", in *Proceedings of the IEEE* v 87 no 7 (July 1999) pp 1267–1276
- [194] P Bloom, 'Descartes' Baby: How Child Development Explains What Makes Us Human', Arrow (2005)
- [195] ER Block, 'Fingerprinting', Franklin Wells (1970), SBN 85166-435-0
- [196] S Blythe, B Fraboni, S Lall, H Ahmed, U de Riu, "Layout Reconstruction of Complex Silicon Chips", in *IEEE Journal of Solid-State Circuits* v 28 no 2 (Feb 93) pp 138–145
- [197] WE Boebert, "Some Thoughts on the Occasion of the NSA Linux Release", in *Linux Journal*, Jan 24 2001; at <http://www.linuxjournal.com/article/4963>
- [198] WE Boebert, RY Kain, "A Practical Alternative to Hierarchical Integrity Policies", in *8th National Computer Security Conference* (1985), proceedings published by NIST p 18
- [199] BW Boehm, 'Software Engineering Economics', Prentice Hall (1981), ISBN 0-13-822122-7
- [200] Rainer Boehme and Gaurav Kataria, "Models and Measures for Correlation in Cyber-Insurance", at *WEIS 2006*
- [201] N Bohm, I Brown, B Gladman, 'Electronic Commerce—Who Carries the Risk of Fraud?', Foundation for Information Policy Research (2000), available from <http://www.fipr.org>
- [202] M Bond, 'Understanding Security APIs', PhD Thesis, Cambridge, 2004
- [203] M Bond, "BOOM! HEADSHOT! (Building Neo-Tactics on Network-Level Anomalies in Online Tactical First-Person Shooters)" (2006), at <http://www.lightbluetouchpaper.org/2006/10/02/>
- [204] M Bond, "Action Replay Justice", Nov 22 2007, at <http://www.lightbluetouchpaper.org/2007/11/22/action-replay-justice/>
- [205] M Bond, SJ Murdoch, J Clulow, 'Laser-printed PIN Mailer Vulnerability Report', 2005, at <http://www.cl.cam.ac.uk/~sjm217/>
- [206] D Boneh, RA Demillo, RJ Lipton, "On the Importance of Checking Cryptographic Protocols for Faults", in *Advances in Cryptology—Eurocrypt 97*, Springer LNCS v 1233 pp 37–51

- [207] D Boneh, M Franklin, "Identity-Based Encryption from the Weil Pairing", in *Advances in Cryptology—Proceedings of CRYPTO 2001*, Springer LNCS 2139 pp 213–29
- [208] L Boney, AH Tewfik, KN Hamdy, "Digital Watermarks for Audio Signals", in *Proceedings of the 1996 IEEE International Conference on Multimedia Computing and Systems*, pp 473–480
- [209] V Bontchev, "Possible macro virus attacks and how to prevent them", in *Computers and Security* v 15 no 7 (96) pp 595–626
- [210] N Borisov, I Goldberg, D Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", at *Mobicom 2001*
- [211] NS Borenstein, "Perils and Pitfalls of Practical Cybercommerce", in *Communications of the ACM* v 39 no 6 (June 96) pp 36–44
- [212] E Bovenlander, invited talk on smartcard security, *Eurocrypt 97*, reported in [69]
- [213] E Bovenlander, RL van Renesse, "Smartcards and Biometrics: An Overview", in *Computer Fraud and Security Bulletin* (Dec 95) pp 8–12
- [214] C Bowden, Y Akdeniz, "Cryptography and Democracy: Dilemmas of Freedom", in *Liberating Cyberspace: Civil Liberties, Human Rights, and the Internet* Pluto Press (1999) pp 81–125
- [215] D Bowen, 'Top-to-Bottom Review', Aug 2007, at http://www.sos.ca.gov/elections/elections_vsr.htm
- [216] D Boyd "Facebook's 'Privacy Trainwreck': Exposure, Invasion, and Drama", in *Apophenia Blog* Sep 8th 2006, at <http://www.danah.org/papers/FacebookAndPrivacy.html>
- [217] M Brader, "Car-door lock remote control activates another car's alarm", in *comp.risks* 21.56 (Jul 2001)
- [218] M Brader, "How to lose 10,000,000 pounds", in *comp.risks* v 24 no 25, Apr 19 2006, at <http://archives.neohapsis.com/archives/risks/2006/0012.html>
- [219] RM Brady, RJ Anderson, RC Ball, 'Murphy's law, the fitness of evolving species, and the limits of software reliability', Cambridge University Computer Laboratory Technical Report no 471 (1999)
- [220] S Brands, 'Rethinking Public Key Infrastructures and Digital Certificates—Building in Privacy', MIT Press (2000) <http://www.freetechbooks.com/about390.html>

- [221] JT Brassil, S Low, NF Maxemchuk, "Copyright Protection for the Electronic Distribution of Text Documents", in *Proceedings of the IEEE* v 87 no 7 (July 1999) pp 1181–1196
- [222] H Bray, " 'Face testing' at Logan is found lacking", in *Boston Globe* July 17 2002
- [223] M Brelis, "Patients' files allegedly used for obscene calls", in *Boston Globe* April 11, 1995; also in *comp.risks* v 17 no 7
- [224] DFC Brewer, MJ Nash, "Chinese Wall model", in *Proceedings of the 1989 IEEE Computer Society Symposium on Security and Privacy* pp 215–228
- [225] B Brewin, "CAC use nearly halves DOD network intrusions, Croom says", in *fcw.com*, Jan 25 2007, at <http://www.fcw.com/article97480-01-25-07>
- [226] M Briceno, I Goldberg, D Wagner, "An implementation of the GSM A3A8 algorithm", at <http://www.scard.org/gsm/a3a8.txt>
- [227] D Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Perseus Press (1999) ISBN: 0-73820144-8; magazine version in *Wired*, Dec 1996, at <http://www.wired.com/wired/archive/4.12/fftransparent.html>
- [228] R Briol "Emanation: How to keep your data confidential", in *Symposium on Electromagnetic Security For Information Protection, SEPI 91*, Rome, 1991
- [229] British Standard 8220-1:2000, 'Guide for Security of Buildings Against Crime—Part 1: Dwellings'
- [230] M Broersma, "Printer makers rapped over refill restrictions", *ZDnet* Dec 20 2002, at <http://news.zdnet.co.uk/story/0,,t269-s2127877,00.html>
- [231] F Brooks, *The Mythical Man-Month: Essays on Software Engineering*, Addison-Wesley (1995 Anniversary Edition)
- [232] D Brown, "Techniques for Privacy and Authentication in Personal Communications Systems", in *IEEE Personal Communications* v 2 no 4 (Aug 95) pp 6–10
- [233] D Brumley, D Boneh, "Remote timing attacks are practical", in *Computer Networks* v 48 no 5 (Aug 2005) pp 701–716
- [234] D Brown, "Unprovable Security of RSA-OAEP in the Standard Model", IACR eprint no 2006/223, at <http://eprint.iacr.org/2006/223>

- [235] I Brown, L Edwards, C Marsden, "Stalking 2.0: privacy protection in a leading Social Networking Site", in *Gikii 2-law, technology and popular culture* (2007); at <http://www.law.ed.ac.uk/ahrc/gikii/docs2/edwards.pdf>
- [236] JDR Buchanan, RP Cowburn, AV Jausovec, D Petit, P Seem, XO Gang, D Atkinson, K Fenton DA Allwood, MT Bryan, "'Fingerprinting' documents and packaging", in *Nature* v 436 no 28 (July 2005) p 475
- [237] JM Buchanan, "The Constitution of Economic Policy", 1986 Nobel Prize Lecture, at http://nobelprize.org/nobel_prizes/economics/laureates/1986/buchanan-lecture.html
- [238] H Buehler, interview with Swiss Radio International, 4/7/1994, at <http://www.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/rpub.cl.msu.edu/crypt/docs/hans-buehler-crypto-spy.txt>
- [239] *Bug Traq* <http://archives.neohapsis.com/archives/bugtraq/>
- [240] Bull, Dassault, Diebold, NCR, Siemens Nixdorf and Wang Global, 'Protection Profile: Automatic Cash Dispensers / Teller Machines', version 1.0 (1999), at <http://www.commoncriteriaportal.org/>
- [241] Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency), 'Common Criteria Protection Profile-Health Professional Card (HPC)-Heilberufsausweis (HPA)', BSI-PP-0018, at <http://www.commoncriteriaportal.org/>
- [242] Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency), 'Schutzmaßnahmen gegen Lauschangriffe' [Protection against bugs], Faltblätter des BSI v 5, Bonn, 1997; <http://www.bsi.bund.de/literat/faltbl/laus005.htm>
- [243] Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency), 'Elektromagnetische Schirmung von Gebäuden, 2007, BSI TR-03209
- [244] Bundesverfassungsgericht, "Beschluss des Ersten Senats", Apr 4 2006, 1 BvR 518/02 Absatz-Nr. (1-184), at http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html
- [245] J Bunnell, J Podd, R Henderson, R Napier, J Kennedy-Moffatt, "Cognitive, associative and conventional passwords: Recall and guessing rates", in *Computers and Security* v 16 no 7 (1997) pp 645-657

- [246] J Burke, P Warren, "How mobile phones let spies see our every move", in *The Observer* Oct 13 2002; at http://observer.guardian.co.uk/uk_news/story/0,6903,811027,00.html
- [247] RW Butler, GB Finelli, "The infeasibility of experimental quantification of life-critical software reliability", in *ACM Symposium on Software for Critical Systems* (1991), ISBN 0-89791-455-4, pp 66–76
- [248] Buro Jansen & Janssen, 'Making up the rules: interception versus privacy', 8/8/2000, at <http://www.xs4all.nl/~respub/crypto/english/>
- [249] M Burrows, M Abadi, RM Needham, "A Logic of Authentication", in *Proceedings of the Royal Society of London A* v 426 (1989) pp 233–271; earlier version published as DEC SRC Research Report 39, <ftp://gatekeeper.pa.dec.com/pub/DEC/SRC/research-reports/SRC-039.pdf>
- [250] RW Byrne, A Whiten, 'Machiavellian Intelligence—Social Expertise and the Evolution of Intellect in Monkeys, Apes and Humans', Oxford, 1988; see also A Whiten, RW Byrne, 'Machiavellian Intelligence II—Extensions and Evaluations', Cambridge 1997
- [251] "Long Distance Phone Scam Hits Internet Surfers", in *business-knowhow.com*, at <http://www.businessknowhow.com/newlong.htm>
- [252] F Caldicott, 'Report on the review of patient-identifiable information', Department of Health, 1997
- [253] California Secretary of State, 'A Report on the Feasibility of Internet Voting' (January 2000), at <http://www.ss.ca.gov/executive/ivote/>
- [254] J Calvert, P Warren, "Secrets of McCartney bank cash are leaked", in *The Express*, February 9 2000, pp 1–2
- [255] J Camenisch, JM Piveteau, M Stadler, "An Efficient Fair Payment System", in *3rd ACM Conference on Computer and Communications Security* (1996), proceedings published by the ACM, ISBN 0-89791-829-0, pp 88–94
- [256] J Camp, C Wolfram, "Pricing Security", in *Proceedings of the CERT Information Survivability Workshop* (Oct 24–26 2000) pp 31–39
- [257] J Camp, S Lewis, 'Economics of Information Security', Springer 2004
- [258] D Campbell, "Somebody's listening", in *The New Statesman* (12 August 1988) pp 1, 10–12; at <http://jya.com/echelon-dc.htm>

- [259] D Campbell, "Making history: the original source for the 1988 first Echelon report steps forward" (25 February 2000), at <http://cryptome.org/echelon-mndc.htm>
- [260] D Campbell, "Operation Ore Exposed", *PC Pro*, July 2005, at <http://www.pcpro.co.uk/features/74690/operation-ore-exposed/page1.html>
- [261] D Campbell, "Sex, Lies and the Missing Videotape", *PC Pro*, April 2007, at http://ore-exposed.obu-investigators.com/PC_PRO_Operation_Ore_Exposed2.html
- [262] D Campbell, P Lashmar, "The new Cold War: How America spies on us for its oldest friend—the Dollar", in *The Independent* (2 July 2000), at <http://www.independent.co.uk/news/World/Americas/2000-07/coldwar020700.shtml>
- [263] JC Campbell, N Ikegami, *The Art of Balance in Health Policy—Maintaining Japan's Low-Cost, Egalitarian System*, Cambridge University Press (1998) ISBN 0-521-57122-7
- [264] JP Campbell, "Speaker Recognition: A Tutorial", in *Proceedings of the IEEE* v 85 no 9 (Sep 97) pp 1437–1462
- [265] K Campbell, L Gordon, M Loeb and L Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", in *Journal of Computer Security* v 11 no 3 (2003) pp 431–448
- [266] C Cant, S Wiseman, "Simple Assured Bastion Hosts", in *13th Annual Computer Security Application Conference* (1997); proceedings published by IEEE Computer Society, ISBN 0-8186-8274-4 ACSAC, pp 24–33
- [267] "Dark horse in lead for fingerprint ID card", *Card World Independent* (May 94) p 2
- [268] "German A555 takes its toll", in *Card World International* (12/94–1/95) p 6
- [269] "High tech helps card fraud decline" in *Cards International* no 117 (29 Sep 94)
- [270] "Visa beefs up its anti-fraud technology", in *Cards International* no 189 (12/12/97) p 5
- [271] JM Carlin, "UNIX Security Update", at *Usenix Security 93* pp 119–130

- [272] J Carr, "Doing nothing is just not an option", in *The Observer* (18/6/2000), at <http://www.guardian.co.uk/technology/2000/jun/18/onlinesecurity.politics>
- [273] J Carroll, *Big Blues: The Unmaking of IBM*, Crown Publishers (1993), ISBN 0-517-59197-9
- [274] H Carter, "Car clock fixer jailed for nine months", in *The Guardian* (15/2/2000) p 13
- [275] R Carter, "What You Are ... Not What You Have", in *International Security Review Access Control Special Issue* (Winter 93/94) pp 14–16
- [276] S Castano, M Fugini, G Martella, P Samarati, *Database Security*, Addison-Wesley, 1994; ISBN 0-201-59375-0
- [277] L Cauley, "NSA has massive database of Americans' phone calls", in *USA Today* Nov 11 2005, at http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm
- [278] Center for Democracy and Technology, <http://www.cdt.org/>
- [279] "The Nature and Scope of Governmental Electronic Surveillance Activity", Center for Democracy and Technology, July 2006, at http://www.cdt.org/wiretap/wiretap_overview.html
- [280] DW Chadwick, PJ Crook, AJ Young, DM McDowell, TL Dornan, JP New, "Using the internet to access confidential patient records: a case study", in *British Medical Journal* v 321 (9 September 2000) pp 612–614; at <http://bmj.com/cgi/content/full/321/7261/612>
- [281] Chaos Computer Club, *How to fake fingerprints?*, at <http://www.ccc.de/biometrie/fingerabdruck.kopieren.xml?language=en>
- [282] L Chapman, *Your disobedient servant*, Penguin Books (1979)
- [283] Chartered Institute of Building Services Engineers, *Security Engineering*, Applications Manual AM4 (1991)
- [284] D Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", in *Communications of the ACM* v 24 no 2 (Feb 1981)
- [285] D Chaum, "Blind signatures for untraceable payments", in *Crypto 82*, Plenum Press (1983) pp 199–203
- [286] D Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability", in *Journal of Cryptology* v 1 (1989) pp 65–75

- [287] D Chaum, A Fiat, M Naor, "Untraceable Electronic Cash", in *Advances in Cryptology — CRYPTO '88*, Springer LNCS v 403 pp 319–327
- [288] R Chellappa, CL Wilcon, S Sirohey, "Human and Machine Recognition of Faces: A Survey", in *Proceedings of the IEEE* v 83 no 5 (May 95) pp 705–740
- [289] HJ Choi, private discussion
- [290] 'Security Protocols–5th International Workshop', B Christianson et al (ed), Springer LNCS v 1360 (1998)
- [291] 'Security Protocols–6th International Workshop', B Christianson et al (ed), Springer LNCS v 1550 (1999). Later workshops had proceedings as follows: 2000, v 2133; 2001, v 2467; 2002, 2845; 2003, v 3364; 2004, v 3957.
- [292] F Church (chairman), 'Intelligence Activities–Senate Resolution 21', US Senate, 94 Congress, First Session, at <http://cryptome.org/nsa-4th.htm>
- [293] WS Ciciora, "Inside the set-top box", in *IEEE Spectrum* v 12 no 4 (Apr 95) pp 70–75
- [294] T Claburn, "Former DuPont Scientist Sentenced For Trade Secret Theft", in *Information Week* Nov 8 2007; at <http://www.information-week.com/shared/printableArticle.jhtml?articleID=202804057>
- [295] D Clark, D Wilson, "A Comparison of Commercial and Military Computer Security Policies", in *Proceedings of the 1987 IEEE Symposium on Security and Privacy* pp 184–194
- [296] R Clark, 'The man who broke Purple', Little, Brown (1977) ISBN 0-316-14595-5
- [297] I Clarke, 'The Free Network Project Homepage', at <http://freenet.sourceforge.net/>
- [298] RW Clarke, "The Theory of Crime prevention Though Environmental Design", at www.cutr.usf.edu/security/documents%5CCPTED%5CTheory%20of%20CPTED.pdf; see also 'Situational Crime Prevention: successful case studies' (2nd edition), Harrow and Heston (1997) and "Situational Crime Prevention–Everybody's Business", ACPC95, at <http://www.acpc.org.au/CONF95/Clarke.htm>
- [299] R Clayton, "Techno-Risk", at *Cambridge International Symposium on Economic Crime* (2003), at <http://www.cl.cam.ac.uk/~rnc1/talks/030910-TechnoRisk.pdf>
- [300] R Clayton, 'Anonymity and traceability in cyberspace', PhD Thesis, 2005; Cambridge University Technical Report UCAM-CL-TR-653

- [301] R Clayton, "Insecure Real-Word Authentication Protocols (or Why Phishing Is So Profitable)", at *Cambridge Security Protocols Workshop 2005*, at <http://www.cl.cam.ac.uk/~rnc1/phishproto.pdf>
- [302] R Clayton, private conversation, 2006
- [303] R Clayton, "The Rising Tide: DDoS by Defective Designs and Defaults", at SRUTI 06; at <http://www.cl.cam.ac.uk/~rnc1/rising-tide.pdf>
- [304] R Clayton, "When firmware attacks! (DDoS by D-Link)", *Light Blue Touchpaper*, at <http://www.lightbluetouchpaper.org/2006/04/07/>
- [305] R Clayton, "There aren't that many serious spammers any more", *Light Blue Touchpaper*, at <http://www.lightbluetouchpaper.org/2007/04/03/>
- [306] R Clayton, M Bond, "Experience Using a Low-Cost FPGA Design to Crack DES Keys", *CHES Workshop* (2002), Springer LNCS 2523 pp 579–592
- [307] R Clayton, G Davies, C Hall, A Hilborne, K Hartnett, D Jones, P Mansfield, K Mitchell, R Payne, N Titley, D Williams, 'LINX Best Current Practice– Traceability', Version 1.0, 18/5/1999, at <http://www.linx.net/noncore/bcp/traceability-bcp.html>
- [308] R Clayton, S Murdoch, R Watson, "Ignoring the Great Firewall of China", at *6th Workshop on Privacy Enhancing Technologies* (2006), at <http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf>
- [309] J Clulow, 'The Design and Analysis of Cryptographic APIs for Security Devices', MSc Thesis, University of Natal 2003
- [310] A Cohen, 'A Perfect Store', Back Bay Books, 2003
- [311] FB Cohen, 'A Short Course on Computer Viruses', Wiley (1994) ISBN 0-471-00769-2
- [312] JL Colbert, PL Bowen, 'A Comparison of Internal Controls: COBIT, SAC, COSO and SAS 55/78', at http://www.isaca.org/bkr_cbt3.htm
- [313] A Collins, "Court decides software time-locks are illegal", in *Computer Weekly* (19 August 93) p 1
- [314] D Cohen, J Hashkes, "A system for controlling access to broadcast transmissions", European Patent no EP0428252

- [315] P Collier, A Hoeffler, "Greed and grievance in civil war", in *Oxford Economic Papers* v 56 (2004) pp 563–595, at <http://oep.oxfordjournals.org/cgi/content/abstract/56/4/563>
- [316] D Comer, "Cryptographic techniques — secure your wireless designs", in *EDN* (18/1/96) pp 57–68
- [317] "Telecomms Fraud in the Cellular Market: How Much is Hype and How Much is Real?", in *Computer Fraud and Security Bulletin* (Jun 97) pp 11–14
- [318] Committee of Sponsoring Organizations of the Treadway Commission (CSOTC), '*Internal Control—Integrated Framework*' (COSO Report, 1992); from <http://www.coso.org/>
- [319] '*Communicating Britain's Future*', at <http://www.fipr.org/polarch/labour.html>
- [320] "Kavkaz-Tsentr says Russians hacking Chechen web sites"; "Information war' waged on web sites over Chechnya", in *Communications Law in Transition Newsletter* v 1 no 4 (Feb 2000), at <http://pcmlp.socleg.ox.ac.uk/transition/issue04/russia.htm>
- [321] Computer Emergency Response Team Coordination Center, at <http://www.cert.org/>
- [322] JB Condat, "Toll fraud on French PBX systems", in *Computer Law and Security Report* v 10 no 2 (Mar/April 94) pp 89–91
- [323] J Connolly, "Operation Chain Link: The Deployment of a Firewall at Hanscom Air Force Base", *Twelfth Annual Computer Security Applications Conference* (1996), proceedings published by the IEEE, ISBN 0-8186-7606-X, pp 170–177
- [324] E Constable, "American Express to reduce the risk of online fraud"
- [325] US Consumer Reports, '*State of the Net*', Sep 6 2007, reported in <http://www.webknowhow.net/news/news/060831ConsumerReport-OnlineThreats.html>
- [326] D Coppersmith, '*The Data Encryption Standard (DES) and its Strength Against Attacks*', IBM report RC 18613 (81421)
- [327] Council of Europe, '*Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data*', European Treaty Series no 108 (January 28, 1981): at http://www.privacy.org/pi/intl.orgs/coe/dp_convention_108.txt

- [328] R Cordery, L Pintsov, "History and Role of Information Security in Postage Evidencing and Payment", in *Cryptologia* v XXIX no 3 (Jul 2005) pp 257–271
- [329] C Cowan, C Pu, D Maier, H Hinton, J Walpole, P Bakke, S Beattie, A Grier, P Wagle, Q Zhang, "StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks", *7th Usenix Security Conference* (1998) pp 63–77
- [330] LH Cox, JP Kelly, R Patil, "Balancing quality and confidentiality for multivariate tabular data" in *Privacy in Statistical Data Bases* (2004) Springer LNCS v 3050 pp 87–98
- [331] JW Coyne, NC Kluksdahl, " 'Mainstreaming' Automated Information Systems Security Engineering (A Case Study in Security Run Amok)", in *Second ACM Conference on Computer and Communications Security* (1994) proceedings published by the ACM, ISBN 0-89791-732-4, pp 251–257; at <http://www.acm.org/pubs/contents/proceedings/commsec/191177/>
- [332] J Cradden, "Printer-makers hit by new EU law", in *Electricnews.net* December 19 2002, at <http://www.electricnews.net/news.html?code=8859027>
- [333] L Cranor, S Garfinkel, 'Security Usability', O'Reilly 2005, ISBN 0-596-80827-9
- [334] S Craver, "On Public-key Steganography in the Presence of an Active Warden", in *Proceedings of the Second International Workshop on Information Hiding* (1998), Springer LNCS v 1525 pp 355–368
- [335] SA Craver, M Wu, BD Liu, A Stubblefield, B Swartzlander, DS Wallach, D Dean, EW Felten, "Reading Between the Lines: Lessons from the SDMI Challenge", in *Usenix Security Symposium* (2000), at <http://www.cs.princeton.edu/~felten>
- [336] RJ Creasy, "The origin of the VM/370 time-sharing system", in *IBM Journal of Research and Development* v 25 no 5 (Sep 1981) pp 483–490, at <http://www.research.ibm.com/journal/rd/255/libmrd2505M.pdf>
- [337] B Crispo, M Lomas, "A Certification Scheme for Electronic Commerce", in *Security Protocols* (1996), Springer LNCS v 1189 pp 19–32
- [338] Cryptome.org, Deepwater documents, May 2007; at <http://cryptome.org/deepwater/deepwater.htm>

- [339] W Curtis, H Krasner, N Iscoe, "A Field Study of the Software Design Process for Large Systems", in *Communications of the ACM* v 31 no 11 (Nov 88) pp 1268–87
- [340] D Cvrcek, "Counters, Freshness, and Implementation", Oct 2 2007, at <http://www.lightbluetouchpaper.org/>
- [341] F D'Addario, "Testing Security's Effectiveness", in *Security Management Online* October 2001, at http://www.securitymanagement.com/library/Security_D'Addario1001.html
- [342] J Daemen, V Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*, Springer (2002) ISBN 3-540-42580-2
- [343] "Beating the credit card telephone fraudsters", in *Daily Telegraph* (9 Oct 1999), at <http://www.telegraph.co.uk:80/>
- [344] G Danezis, Roger Dingledine, N Mathewson, "Mixminion: Design of a Type III Anonymous Remailer Protocol", in *IEEE Symposium on Security and Privacy* (2003) pp 2–15; at <http://mixminion.net/miniondesign.pdf>
- [345] G Danezis, B Wittneben, "The Economics of Mass Surveillance", *Fifth Workshop on the Economics of Information Security* (2006)
- [346] G Danezis, R Clayton, "Introducing Traffic Analysis", Jan 2007, in *Digital Privacy: Theory, Technologies, and Practices*, Taylor and Francis 2007, at <http://homes.esat.kuleuven.be/~gdanezis/TAIntro-book.pdf>
- [347] G Danezis, C Diaz, "Survey of Privacy Technology", 2007, at <http://homes.esat.kuleuven.be/~gdanezis/anonSurvey.pdf>
- [348] M Darman, E le Roux, "A new generation of terrestrial and satellite microwave communication products for military networks", in *Electrical Communication* (Q4 94) pp 359–364
- [349] Two statements, made by the Data Protection Commissioners of EU and EES countries and Switzerland, *20th International Conference on Data Protection*, Santiago de Compostela, 16–18 September 1998; available at <http://www.dataprotection.gov.uk/20dpcom.html>
- [350] *Daubert v. Merrell Dow Pharmaceuticals*, 113 S. Ct. 2786 (1993)
- [351] J Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", in *IEEE Transactions on Pattern Analysis and Machine Intelligence* v 15 no 11 (Nov 93) pp 1148–1161

- [352] J Daugman, 'Biometric decision landscapes', Technical Report no TR482, University of Cambridge Computer Laboratory.
- [353] C Davies, R Ganesan, "BApasswd: A New Proactive Password Checker", in *16th National Computer Security Conference* (1993), proceedings published by NIST, pp 1–15
- [354] DW Davies, WL Price, 'Security for Computer Networks' (John Wiley and Sons 1984)
- [355] G Davies, 'A History of money from ancient times to the present day', University of Wales Press (1996) ISBN 0-7083-1351-5; related material at <http://www.ex.ac.uk/%7ERDavies/arian/llyfr.html>
- [356] H Davies, "Physiognomic access control", in *Information Security Monitor* v 10 no 3 (Feb 95) pp 5–8
- [357] D Davis, "Compliance Defects in Public-Key Cryptography", in *Sixth Usenix Security Symposium Proceedings* (July 1996) pp 171–178
- [358] D Davis, R Ihaka, P Fenstermacher, "Cryptographic Randomness from Air Turbulence in Disk Drives" in *Advances in Cryptology–Crypto 94* Springer LNCS v 839 pp 114–120
- [359] J Davis, "Hackers Take Down the Most Wired Country in Europe", in *Wired*, Aug 21 2007, at http://www.wired.com/politics/security/magazine/15-09/ff_estonia
- [360] D Dean, EW Felten, DS Wallach, "Java Security: From HotJava to Netscape and Beyond", in *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, pp 190–200
- [361] C Deavours, D Kahn, L Kruh, G Mellen, B Winkel, 'Cryptology–Yesterday, Today and Tomorrow', Artech House (1987), ISBN 0-89006-253-6
- [362] C Deavours, D Kahn, L Kruh, G Mellen, B Winkel, 'Selections from Cryptologia–History, People and Technology', Artech House (1997) ISBN 0-89006-862-3
- [363] C Deavours, L Kruh, 'Machine Cryptography and Modern Cryptanalysis', Artech House (1985) ISBN 0-89006-161-0
- [364] JF de Beer, "Constitutional Jurisdiction Over Paracopyright Laws", in 'The Public Interest: The Future of Canadian Copyright Law', Irwin Law (2005)
- [365] B Demoulin, L Kone, C Poudroux, P Degauque, "Electromagnetic Radiation of Shielded Data Transmission Lines", in [481] pp 163–173

- [366] I Denley, S Weston-Smith, "Implementing access control to protect the confidentiality of patient information in clinical information systems in the acute hospital", in *Health Informatics Journal* v 4 nos 3–4 (Dec 1998) pp 174–178
- [367] I Denley, S Weston-Smith, "Privacy in clinical information systems in secondary care" in *British Medical Journal* v 318 (15 May 1999) pp 1328–1331
- [368] DE Denning, "The Lattice Model of Secure Information Flow", in *Communications of the ACM* v 19 no 5 pp 236–248
- [369] DE Denning, *Cryptography and Data Security*, Addison-Wesley (1982) ISBN 0-201-10150-5
- [370] DE Denning, *Information Warfare and Security*, Addison-Wesley (1999) ISBN 0-201-43303-6
- [371] DE Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", InfowarCon 2000, at <http://www.nautilus.org/info-policy/workshop/papers/denning.html>
- [372] DE Denning, PJ Denning, M Schwartz, "The tracker: a threat to statistical database security", in *ACM Transactions on Database Systems* v 4 no 1 (1979) pp 76–96
- [373] DE Denning, PH MacDoran, "Location-Based Authentication: Grounding Cyberspace for Better Security", in *Computer Fraud and Security Bulletin* (Feb 96) pp 12–16
- [374] DE Denning, J Schlorer, "Inference Controls for Statistical Databases", in *IEEE Computer* v 16 no 7 (July 1983) pp 69–82
- [375] Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, DoD 5200.28-STD, December 1985
- [376] Department of Defense, *A Guide to Understanding Covert Channel Analysis of Trusted Systems*, NCSC-TG-030 (Nov 1993)
- [377] Department of Defense, *Password Management Guideline*, CSC-STD-002-85 (1985)
- [378] Department of Defense, *A Guide to Understanding Data Remanence in Automated Information Systems*, NCSC-TG-025 (1991)
- [379] Department of Defense, *Technical Rationale behind CSC-STD-003-85: computer security requirements*, CSC-STD-004-85 (1985)

- [380] Department of Defense, News Transcript, Oct 20 2007, at <http://cryptome.org/af-squirm/af-squirm.htm>
- [381] Department of Justice, 'Guidelines for Searching and Seizing Computers', 1994; at http://www.epic.org/security/computer_search_guidelines.txt
- [382] Y Desmedt, Y Frankel, "Threshold cryptosystems", in *Advances in Cryptology—Proceedings of Crypto 89*, Springer LNCS v 435 pp 307–315
- [383] J Dethloff, "Special Report: Intellectual Property Rights and Smart Card Patents: The Past—The Present—The Future", in *Smart Card News* (Feb 96) pp 36–38
- [384] J Dibbell, "The Life of the Chinese Gold Farmer", in *New York Times* Jun 17 2007; at <http://www.nytimes.com/2007/06/17/magazine/17lootfarmers-t.html?ex=1340769600&en=87f96d5d8676cbad&ei=5124&partner=permalink&exprod=permalink>
- [385] W Diffie, ME Hellman, "New Directions in Cryptography", in *IEEE Transactions on information theory* v 22 no 6 (Nov 76) pp 644–654
- [386] W Diffie, ME Hellman, "Exhaustive cryptanalysis of the NBS Data Encryption Standard", in *Computer* v 10 no 6 (June 77) pp 74–84
- [387] W Diffie, S Landau, 'Privacy on the Line—The Politics of Wiretapping and Encryption', MIT Press (1998) ISBN 0-262-04167-7
- [388] E Dijkstra, "Solution of a problem in concurrent programming control", in *Communications of the ACM* v 8 no 9 (1965) p 569
- [389] Allana Dion, "Rapper Verified?", on *Gridgrind* Dec 8 2007; at <http://www.gridgrind.com/?p=229>
- [390] The Discount Long Distance Digest, at <http://www.thedigest.com/shame/>
- [391] D Dittrich, 'Distributed Denial of Service (DDoS) Attacks/tools', at <http://staff.washington.edu/dittrich/>
- [392] AK Dixit, 'Lawlessness and Economics', Princeton University Press, 2003
- [393] RC Dixon, 'Spread Spectrum Systems with Commercial Applications', Wiley (1994) ISBN 0-471-59342-7
- [394] H Dobbertin, "Cryptanalysis of MD4", *Journal of Cryptology* v 11 no 4 (1998) pp 253–270

- [395] B Dole, S Lodin, E Spafford, "Misplaced Trust: Kerberos 4 Session Keys", in *Internet Society Symposium on Network and Distributed System Security*, proceedings published by the IEEE, ISBN 0-8186-7767-8, pp 60–70
- [396] JR Douceur, "The Sybil Attack", IPTPS 2002, at www.cs.rice.edu/Conferences/IPTPS02/101.pdf
- [397] J Doward, "The friend of the stars who fell from grace", in *The Observer* Aug 26 2007; at <http://www.guardian.co.uk/media/2007/aug/26/radio.television>
- [398] P Drahos, J Braithwaite, 'Information Feudalism—Who Owns the Knowledge Economy?', Earthscan 2002
- [399] S Drimer, "Banks don't help fight phishing", Mar 10 2006, *Light Blue Touchpaper*; at <http://www.lightbluetouchpaper.org/2006/03/10/banks-dont-help-fight-phishing/>
- [400] S Drimer, 'Volatile FPGA design security—a survey', 2007, at http://www.cl.cam.ac.uk/~sd410/papers/fpga_security.pdf
- [401] S Drimer, SJ Murdoch, "Keep your enemies close: Distance bounding against smartcard relay attacks", in *16th USENIX Security Symposium* (2007), at http://www.cl.cam.ac.uk/~sd410/papers/sc_relay.pdf
- [402] IE Dror, D Charlton, AE Péron, "Contextual information renders experts vulnerable to making erroneous identifications", in *Forensic Science International* 156 (2006) 74–78
- [403] IE Dror, D Charlton, "Why Experts Make Errors", in *Journal of Forensic Identification* v 56 no 4 (2006) pp 600–616; at <http://users.ecs.soton.ac.uk/id/biometrics.html>
- [404] IE Dror, "Don't forget us humans", in *The Times*, July 31 2006; at <http://users.ecs.soton.ac.uk/id/biometrics.html>
- [405] I Drury, "Pointing the finger", in *Security Surveyor* v 27 no 5 (Jan 97) pp 15–17; at <http://users.ecs.soton.ac.uk/id/biometrics.html>
- [406] C Dyer, "Europe's concern over UK data protection 'defects' revealed", in *The Guardian* Oct 1 2007; at http://www.guardian.co.uk/uk_news/story/0,,2180729,00.html
- [407] N Eagle, A Pentland, D Lazer, "Inferring Social Network Structure using Mobile Phone Data", 2007, at http://reality.media.mit.edu/pdfs/network_structure.pdf

- [408] W van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" in *Computers and Security* v 4 (1985) pp 269–286
- [409] P Eckersley, "Comcast is also Jamming Gnutella (and Lotus Notes?)", *EFF Deeplinks Blog* Oct 20 2007, at <http://www.eff.org/deeplinks/2007/10/comcast-also-jamming-gnutella-and-lotus-notes>
- [410] *The Economist*, "Digital rights and wrongs" (17/7/1999); see www.economist.com
- [411] *The Economist*, "Living in the global goldfish bowl", 18–24 Dec 1999, Christmas special; see www.economist.com
- [412] *The Economist*, "A price worth paying?", May 19 2005
- [413] *The Economist*, "Cyberwarfare—Newly nasty", May 24 2007
- [414] *The Economist*, "After smart weapons, smart soldiers", Oct 25 2007
- [415] *The Economist*, "Getting the message, at last", Dec 13 2007, at http://www.economist.com/opinion/displaystory.cfm?story_id=10286400
- [416] B Edelman, "Adverse Selection in Online 'Trust' Certificates", at *Fifth Workshop on the Economics of Information Security* (2006); at <http://weis2006.econinfosec.org/>
- [417] J Edge, "IPv6 source routing: history repeats itself", May 7, 2007; at <http://lwn.net/Articles/232781/>
- [418] EDRI, FIPR and VOSN, 'Response to the European commission consultation on the review of the "acquis communautaire" in the field of copyright and related rights', Oct 2004, at <http://www.edri.org/campaigns/copyright>
- [419] A Edwards, "BOLERO, a TTP project for the Shipping Industry", in *Information Security Technical Report* v 1 no 1 (1996) pp 40–45
- [420] M van Eeten, JM Bauer, M de Bruijne, J Groenewegen, W Lenstra, 'The Economics of Malware: Security Decisions, Incentives and Externalities' OECD Report, 2008
- [421] M Eichin, J Rochlis, "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988", in *Proceedings of the 1989 IEEE Symposium on Security and Privacy* pp 326–343
- [422] Electronic Frontier Foundation, <http://www.eff.org>

- [423] Electronic Frontier Foundation, *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design*, EFF (1998); ISBN 1-56592-520-3; <http://cryptome.org/cracking-des.htm>
- [424] Electronic Frontier Foundation, *Felten, et al., v. RIAA, et al.* at http://www.eff.org/IP/DMCA/Felten_v_RIAA/
- [425] Electronic Frontier Foundation, "DocuColor Tracking Dot Decoding Guide", at <http://w2.eff.org/Privacy/printers/docucolor/>
- [426] M Ellims, "Is Security Necessary for Safety?", in *ESCAR 2006*, at http://www.pi-shurlok.com/uploads/documents/security_and_safety.pdf
- [427] JH Ellis, *The History of Non-secret Encryption*, 1987, at <http://www.jya.com/ellisdoc.htm>
- [428] C Ellison, B Schneier, "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure", in *Computer Security Journal* v XIII no 1 (2000); also at <http://www.counterpane.com/pki-risks.html>
- [429] EMV documents available from EMVCo LLP at <http://www.emvco.com/>
- [430] 'Enfopol Papiere', Telepolis archiv special 1998/9, at <http://www.heise.de/tp/deutsch/special/enfo/default.html>
- [431] P Enge, T Walter, S Pullen, CD Kee, YC Chao, YJ Tsai, "Wide Area Augmentation of the Global Positioning System", in *Proceedings of the IEEE* v 84 no 8 (Aug 96) pp 1063–1088
- [432] Electronic Privacy Information Center, <http://www.epic.org>
- [433] EPIC, 'Approvals for Federal Pen Registers and Trap and Trace Devices 1987–1998', at <http://www.epic.org/privacy/wiretap/stats/penreg.html>
- [434] EPIC, 'Report of the Director of the Administrative Office of the United States Courts', at <http://www.epic.org/privacy/wiretap/stats/1999-report/wiretap99.pdf>
- [435] EPIC, 'Wiretapping', at <http://www.epic.org/privacy/wiretap/>
- [436] J Epstein, S Matsumoto, G McGraw, "Software Security and SOA: Danger, Will Robinson!", in *IEEE Security and Privacy*, Jan/Feb 2006,

- pp 80–83, at <http://www.digital.com/papers/download/bsi12-soa.doc.pdf>
- [437] J Epstein, H Orman, J McHugh, R Pascale, M Branstad, A Marmor-Squires, “A High Assurance Window System Prototype”, in *Journal of Computer Security* v 2 no 2–3 (1993) pp 159–190
- [438] J Epstein, R Pascale, “User Interface for a High Assurance Windowing System”, in *Ninth Annual Computer Security Applications Conference* (1993), proceedings published by the IEEE, ISBN 0-8186-4330-7, pp 256–264
- [439] T Escamilla, *Intrusion Detection—Network Security beyond the Firewall*, Wiley (1998) ISBN 0-471-29000-9
- [440] J Essinger, *ATM Networks—Their Organisation, Security and Future*, Elsevier 1987
- [441] A Etzioni, *The Limits of Privacy*, Basic Books (1999) ISBN 0-465-04089-6
- [442] European Commission, *Impact assessment—amending Framework Decision 2002/475/JHA on combating terrorism*, Brussels, Nov 6 2007, SEC (2007) 1424, at [http://www.ipex.eu/ipex/webdav/site/myjahiasite/groups/CentralSupport/public/2007/SEC_2007_1424/COM_SEC\(2007\)1424_EN.pdf](http://www.ipex.eu/ipex/webdav/site/myjahiasite/groups/CentralSupport/public/2007/SEC_2007_1424/COM_SEC(2007)1424_EN.pdf)
- [443] European Parliament, *Development of surveillance technology and risk of abuse of economic information*, Luxembourg (April 1999) PE 166.184/Part 3/4, at <http://www.gn.apc.org/duncan/stoa.htm>
- [444] European Union, *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Directive 95/46/EC, at <http://www.privacy.org/pi/intlorgs/ec/eudp.html>
- [445] European Union, “Draft Council Resolution on the lawful interception of telecommunications in relation to new technologies” 6715/99 (15/3/1999), at <http://www.fipr.org/polarch/enfopol19.html>; for background see <http://www.fipr.org/polarch/>
- [446] European Union, *Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks*, 2006/24/EC
- [447] European Union, “Promoting Data Protection by Privacy Enhancing Technologies (PETs)”, COM(2007) 228 final, Brussels, May 2nd 2007

- [448] Eurosmart, 'Protection Profile—Smart Card Integrated Circuit With Embedded Software', 1999, at <http://www.commoncriteriaportal.org/>
- [449] R Evans, D Leigh, "GM subsidiary paid conman for 'blagged' private data, court told", *The Guardian* Apr 24, 2007; at <http://www.guardian.co.uk/crime/article/0,,2064180,00.html>
- [450] Facebook, *Photos*, at <http://www.facebook.com/help.php?page=7>
- [451] G Faden, "Reconciling CMW Requirements with Those of X11 Applications", in *Proceedings of the 14th Annual National Computer Security Conference* (1991)
- [452] M Fairhurst, "The Hedge End Experiment", in *International Security Review* no 85 (Summer 94) p 20
- [453] M Fairhurst, "Signature verification revisited: promoting practical exploitation of biometric technology", in *Electronics and Communication Engineering Journal* v 9 no 6 (Dec 97) pp 273–280
- [454] B Feder, "Face-Recognition Technology Improves", *New York Times* Mar 14 2003; at <http://www.nytimes.com/2003/03/14/technology/14FACE.html>
- [455] Federal Committee on Statistical Methodology, 'Statistical Policy Working Paper 22' (Revised 2005)—'Report on Statistical Disclosure Limitation Methodology', at <http://www.fcsm.gov/working-papers/spwp22.html>
- [456] Federal Trade Commission v Audiotex Connection, Inc., and others, at <http://www.ftc.gov/os/1997/9711/Adtxamdfcmp.htm>
- [457] Federal Trade Commission and Department of Commerce, 'Electronic Signatures in Global and National Commerce Act—The Consumer Consent Provision in Section 101(c)(1)(C)(ii)', June 2001, at <http://www.ftc.gov/os/2001/06/esign7.htm>
- [458] Federal Trade Commission, 'ID Theft: When Bad Things Happen to Your Good Name', at <http://www.consumer.gov/idtheft/>
- [459] Federal Trade Commission, 'ChoicePoint Settles Data Security Breach Charges; to Pay 10 Million in Civil Penalties, 5 Million for Consumer Redress', Jan 26 2006, at <http://www.ftc.gov/opa/2006/01/choicepoint.shtm>
- [460] Federation of American Scientists, <http://www.fas.org>
- [461] H Federrath, J Thees, "Schutz der Vertraulichkeit des Aufenthaltsorts von Mobilfunkteilnehmern", in *Datenschutz und Datensicherheit* (June 1995) pp 338–348

- [462] P Fellwock (using pseudonym 'Winslow Peck'), "U.S. Electronic Espionage: A Memoir", in *Ramparts* v 11 no 2 (August 1972) pp 35–50; at <http://jya.com/nsa-elint.htm>
- [463] E Felten, "Facebook and the Campus Cops", Mar 20 2006, at <http://www.freedom-to-tinker.com/?p=994>
- [464] JS Fenton, *Information Protection Systems*, PhD Thesis, Cambridge University, 1973
- [465] N Ferguson, B Schneier, "A Cryptographic Evaluation of IPSEC", at <http://www.counterpane.com/ipsec.html>
- [466] D Ferraiolo, R Kuhn, "Role-Based Access Control", in *15th National Computer Security Conference* (1992), proceedings published by NIST, pp 554–563
- [467] D Ferraiolo, R Kuhn, R Chandramouli, *Role-Based Access Control*, Artech House, 2007
- [468] D Fewer, P Gauvin, A Cameron, *Digital Rights Management Technologies and Consumer Privacy—An Assessment of DRM Applications Under Canadian Privacy Law*, September 2007, at www.cippic.ca
- [469] A Fiat, M Naor, "Broadcast Encryption", in *Crypto '93*, Springer LNCS v 773 pp 480–491
- [470] PFJ Fillery, AN Chandler, "Is lack of quality software a password to information security problems?", in *IFIP SEC 94* paper C8
- [471] "Psychologists and banks clash over merits of photographs on cards", in *Financial Technology International Bulletin* v 13 no 5 (Jan 96) pp 2–3
- [472] D Fine, "Why is Kevin Lee Poulsen Really in Jail?", at <http://www.well.com/user/fine/journalism/jail.html>
- [473] G Fiorentini, S Pelzman, *The Economics of Organised Crime*, Cambridge University Press 1995
- [474] B Fischer, talk at Cryptologic History Symposium, NSA, October 1999; reported in *Cryptologia* v 24 no 2 (Apr 2000) pp 160–167
- [475] RA Fisher, *The Genetical Theory of Natural Selection*, Clarendon Press, Oxford (1930); 2nd ed. Dover Publications, NY (1958)
- [476] J Flanagan, "Prison Phone Phraud (or The RISKS of Spanish)", reporting *University of Washington staff newspaper*, in *comp.risks* v 12.47; at <http://catless.ncl.ac.uk/Risks/20.69.html>

- [477] M Fleet, "Five face sentence over notes that passed ultraviolet tests", in *The Daily Telegraph* (23/12/1999), available at <http://www.telegraph.co.uk:80/>
- [478] B Fletcher, C Roberts, K Risser, "The Design and Implementation of a Guard Installation and Administration Framework", in *Third Annual SELinux Symposium*, at <http://selinux-symposium.org/>
- [479] S Fluhrer, I Mantin, A Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4" in *SAC 2001*
- [480] SN Foley, "Aggregation and separation as noninterference properties", in *Journal of Computer Security* v 1 no 2 (1992) pp 158–188
- [481] Fondazione Ugo Bordoni, 'Symposium on Electromagnetic Security for Information Protection', Rome, Italy, 21–22 November 1991
- [482] S Forrest, SA Hofmeyr, A Somayaji, "Computer Immunology", in *Communications of the ACM* v 40 no 10 (Oct 97) pp 88–96
- [483] DS Fortney, JJ Lim, "A technical approach for determining the importance of information in computerised alarm systems", in *Seventeenth National Computer Security Conference* (1994), proceedings published by NIST; pp 348–357
- [484] The Foundation for Information Policy Research, <http://www.fipr.org>
- [485] B Fox, "How to keep thieves guessing", in *New Scientist* (3rd June 95) p 18
- [486] B Fox, "Do not adjust your set . . . we have assumed radio control", in *New Scientist* 8 Jan 2000, at <http://www.newscientist.com/ns/20000108/newsstory6.html>
- [487] B Fox, "The pirate's tale", in *New Scientist* 18 Dec 1999, at <http://www.newscientist.com/ns/19991218/theirates.html>
- [488] D Fox, "IMSI-Catcher", in *Datenschutz und Datensicherheit* v 21 no 9 (9/97) p 539
- [489] D Foxwell, "Off-the-shelf, on to sea", in *International Defense Review* v 30 (Jan 97) pp 33–38
- [490] D Foxwell, M Hewish, "GPS: is it lulling the military into a false sense of security?", in *Jane's International Defense Review* (Sep 98) pp 32–41
- [491] LJ Fraim, "SCOMP: A Solution to the Multilevel Security Problem", in *IEEE Computer* v 16 no 7 (July 83) pp 26–34

- [492] T Frank, "Tougher TSA bomb tests raise stakes for screeners", in *USA Today* Oct 18 2007, at <http://www.usatoday.com/printedition/news/20071018/a.insidescreeners18.art.htm>
- [493] J Franks, P Hallam-Baker, J Hostetler, S Lawrence, P Leach, A Luotonen, L Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617
- [494] T Fraser, "LOMAC: Low Water-Mark Integrity Protection for COTS Environments", in *Proceedings of the 2000 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, pp 230–245
- [495] J Frizell, T Phillips, T Groover, "The electronic intrusion threat to national security and emergency preparedness telecommunications: an awareness document", in *Seventeenth National Computer Security Conference* (1994); proceedings published by NIST, pp 378–399
- [496] M Frost, *Spyworld: Inside the Canadian & American Intelligence Establishments*, Diane Publishing Co (1994), ISBN 0-78815791-4
- [497] "Banks fingerprint customers to cut cheque fraud", in *Fraud Watch* (1997) no 1 p 9
- [498] "Chip cards reduce fraud in France", in *Fraud Watch* (1996) no 1 p 8
- [499] "Counterfeit and cross border fraud on increase warning", in *Fraud Watch* (1996) no 1 pp 6–7
- [500] "Finger minutiae system leaps the 1:100,000 false refusal barrier", in *Fraud Watch* (1996) no 2 pp 6–9
- [501] "Widespread card skimming causes European concern", in *Fraud Watch* (1997) v 3 pp 1–2
- [502] P Freiburger, M Swaine, *Fire in the Valley — the Making of the Personal Computer*, McGraw-Hill (1999) ISBN 0-07-135892-7
- [503] M Freiss, *Protecting Networks with Satan*, O'Reilly (1997) ISBN 1-56592-425-8
- [504] AM Froomkin, "The Death of Privacy", in *Stanford Law Review* v 52 pp 1461–1543, at <http://www.law.miami.edu/~froomkin/articles/privacy-deathof.pdf>
- [505] D Frye, "Open and Secure: Linux Today and Tomorrow", in *2007 Security Enhanced Linux Symposium*, at <http://selinux-symposium.org/2007/agenda.php>

- [506] DA Fulghum, "Communications Intercepts Pace EP-3s", in *Aviation Week and Space Technology* v 146 no 19 (5/5/97) pp 53–54
- [507] Dr Fun, 'Suddenly, just as Paul was about to clinch the job interview, he received a visit from the Ghost of Usenet Postings Past', 1996, at <http://www.ibiblio.org/Dave/Dr-Fun/df9601/df960124.jpg>
- [508] S Furber, *'ARM System Architecture'*, Addison-Wesley (1996); ISBN 0-210-40352-8
- [509] M Galecotti, "Russia's eavesdroppers come out of the shadows", in *Jane's Intelligence Review* v 9 no 12 (Dec 97) pp 531–535
- [510] Sir F Galton, "Personal identification and description," in *Nature* (21/6/1888) pp 173–177
- [511] Sir F Galton, *'Finger Prints'*, Macmillan, 1892
- [512] HF Gaines, *'Cryptanalysis—a study of ciphers and their solution'*, Dover, ISBN 486-20097-3 (1939, 1956)
- [513] T Gandy, "Brainwaves in fraud busting", *Banking Technology* (Dec 95/Jan 96) pp 20–24
- [514] R Gardner, A Yasinsac, M Bishop, T Kohno, Z Hartley, J Kerski, D Gainey, R Walega, E Hollander, M Gerke, *'Software Review and Security Analysis of the Diebold Voting Machine Software'*, Florida State University, Jul 27 2007, at <http://www.sait.fsu.edu/news/2007-07-31.shtml>
- [515] S Garfinkel, *'Database Nation'*, O'Reilly and Associates (2000) ISBN 1-56592-653-6
- [516] S Garfinkel, *'Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable'*, PhD Thesis, MIT 2005, at <http://www.simson.net/thesis/>
- [517] S Garfinkel, G Spafford, *'Practical Unix and Internet Security'*, O'Reilly and Associates (1996); ISBN 1-56592-148-8
- [518] W Gates, W Buffett, "The Bill & Warren Show", in *Fortune*, 20/7/1998
- [519] B Gellman, D Linzer, CD Leonnig, "Surveillance Net Yields Few Suspects", in *Washington Post*, Feb 5 2006 p A01; at http://www.washingtonpost.com/wp-dyn/content/article/2006/02/04/AR2006020401373_pf.html
- [520] General Accounting Office, USA, *'Medicare—Improvements Needed to Enhance Protection of Confidential Health Information'*, GAO/HEHS-99-140; <http://www.gao.gov/AIndexFY99/abstracts/he99140.htm>

- [521] RM Gerecht, "The Counterterrorist Myth", in *Atlantic Monthly*, Jul–Aug 2001, at <http://www.theatlantic.com/doc/200107/gerecht>
- [522] E German, "Problem Idents", at <http://onin.com/fp/problemidents.html>
- [523] E German, "Legal Challenges to Fingerprints", at http://www.onin.com/fp/daubert_links.html
- [524] A Gidari, JP Morgan, "Survey of State Electronic and Digital Signature Legislative Initiatives", at <http://www.ilpf.org/digsig/digrep.htm>
- [525] D Gifford, A Spector, "The CIRRUS Banking Network", in *Communications of the ACM* v 28 no 8 (Aug 1985) pp 797–807
- [526] D Gilbert, "If only gay sex caused global warming", *LA Times*, July 2, 2006; <http://www.latimes.com/news/opinion/sunday/commentary/la-op-gilbert2jul02,0,4254536.story?coll=la-sunday-commentary>
- [527] M Gill, A Spriggs, 'Assessing the impact of CCTV', UK Home Office Research Study 292, at www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf
- [528] J Gilmore, "Nacchio affects spy probe", in *Denver Post* Oct 20 2007; cited in "NSA solicited illegal Qwest mass wiretaps right after Bush inauguration", *Cryptography List* Oct 20 2007, at <http://www.mailarchive.com/cryptography%40metzdowd.com/msg08213.html>
- [529] T Gilovich, D Griffin, D Kahneman, 'Heuristics and Biases—The Psychology of Intuitive Judgment', Cambridge University Press 2002
- [530] AA Giordano, HA Sunkenberg, HE de Pdero, P Stynes, DW Brown, SC Lee, "A Spread-Spectrum Simulcast MF Radio Network", in *IEEE Transactions on Communications* v TC-30 no 5 (May 1982) pp 1057–1070
- [531] WN Goetzmann, 'Financing Civilization', <http://viking.som.yale.edu/will/finciv/chapter1.htm>
- [532] J Goguen, J Meseguer, "Security Policies and Security Models", in *Proceedings of the 1982 IEEE Computer Society Symposium on Research in Security and Privacy* pp 11–20
- [533] I Goldberg, D Wagner, "Randomness and the Netscape browser", in *Dr Dobbs Journal* no 243 (Jan 96) pp 66–70
- [534] L Goldberg, "Recycled Cold-War Electronics Battle Cellular Telephone Thieves", in *Electronic Design* v 44 no 18 (3 September 1996) pp 41–42

- [535] O Goldreich, *Foundations of Cryptography*, v 1 and 2, 2001 and 2004, at <http://www.wisdom.weizmann.ac.il/~oded/foc-book.html>
- [536] S Goldwasser, S Micali, "Probabilistic encryption", in *J Comp Sys Sci* v 28 (1984) pp 270–299
- [537] D Gollmann, *Computer Security*, Wiley (1999); ISBN 0-471-97884-2
- [538] D Gollmann, "What Is Authentication?", in *Security Protocols* (2000), Springer LNCS 1796 pp 65–72
- [539] L Gong, *Inside Java 2 Platform Security: Architecture, API Design, and Implementation*, Addison-Wesley (1999); ISBN: 0-201-31000-7
- [540] L Gong, DJ Wheeler, "A matrix key-distribution scheme", in *Journal of Cryptology* v 2 no 1 (1990) pp 51–59
- [541] R Gonggrijp, WJ Hengeveld, A Bogk, D Engling, H Mehnert, F Rieger, P Scheffers, B Wels, "Nedap/Groenendaal ES3B voting computer—a security analysis", Oct 2006, at <http://www.wijvertrouwenstem-computersniet.nl/Nedap-en>
- [542] D Goodin, "Anatomy of an eBay scam", in *The Register*, Mar 21 2007; at http://www.theregister.co.uk/2007/03/21/ebay_fraud_anatomy/
- [543] D Goodin, "Firefox leak could divulge sensitive info", in *The Register*, Aug 13 2007; at http://www.theregister.co.uk/2007/08/13/firefox_remote_leakage/
- [544] D Goodin, "TJX agrees to pay banks \$41 m to cover Visa losses", in *The Channel Register*, Dec 3 2007; at http://www.channelregister.co.uk/2007/12/03/tjx_settlement_agreement/print.html
- [545] D Goodin, "Ukrainian eBay scam turns Down Syndrome man into cash machine", in *The Register* Nov 8 2007, at http://www.theregister.co.uk/2007/11/08/ebay_victims_track_their_mules/
- [546] JI Gordon, "Copyright.Protection@Internet.net", in *3W Valparaiso Journal of Law and Technology* v 1 (24/1/1999), at <http://www.wvjolt.wvu.edu/v3i1/gordon.htm>
- [547] KE Gordon, RJ Wong, "Conducting Filament of the Programmed Metal Electrode Amorphous Silicon Antifuse", in *Proceedings of International Electron Devices Meeting*, Dec 93; reprinted as pp 6-3 to 6-10, *QuickLogic Data Book* (1994)
- [548] MF Grady, F Parisi, *The Law and economics of Cybersecurity*, Cambridge University Press, 2006

- [549] RM Graham, "Protection in an Information Processing Utility," in *Communications of the ACM* v 11 no 5 (May 1968) pp 365–369
- [550] FT Grampp, RH Morris, "UNIX Operating System Security", *AT&T Bell Laboratories Technical Journal* v 63 no 8 (Oct 84) pp 1649–1672
- [551] S Granneman, "Electronic Voting Debacle", in *The Register* Nov 18 2003; at http://www.theregister.co.uk/2003/11/18/electronic_voting_debacle/
- [552] RD Graubart, JL Berger, JPL Woodward, '*Compartmented Mode, Workstation Evaluation Criteria, Version 1*', Mitre MTR 10953, 1991 (also published by the Defense Intelligence Agency as document DDS-2600-6243-91)
- [553] J Gray, P Helland, P O'Neil, D Shasha, "The Dangers of Replication and a Solution," in *SIGMOD Record* v 25 no 2 (1996) pp 173–182
- [554] J Gray, P Syverson, "A Logical Approach to Multilevel Security of Probabilistic Systems," in *Distributed Computing* v 11 no 2 (1988)
- [555] TC Greene, "Vista security overview: too little too late", in *The Register* Feb 20 2007, at http://www.theregister.co.uk/2007/02/20/vista_security_oversold/
- [556] T Greening, "Ask and Ye Shall Receive: A Study in Social Engineering", in *SIGSAC Review* v 14 no 2 (Apr 96) pp 9–14
- [557] M Gregory, P Losocco, "Using the Flask Security Architecture to Facilitate Risk Adaptable Access Controls", in *2007 Security Enhanced Linux Symposium*, at <http://selinux-symposium.org/2007/agenda.php>
- [558] A Griew, R Currell, '*A Strategy for Security of the Electronic Patient Record*', Institute for Health Informatics, University of Wales, Aberystwyth, March 1995
- [559] V Groebner, J Peck, M Kyburz, '*Who Are You?: Identification, Deception, and Surveillance in Early Modern Europe*', Zone Books, 2007
- [560] J Gross, "Keeping Patients' Details Private, Even From Kin", in *New York Times* July 3 2007
- [561] D Grover, '*The protection of computer software—its technology and applications*', British Computer Society / Cambridge University Press (1992) ISBN 0-521-42462-3

- [562] D Gruhl, W Bender, "Information Hiding to Foil the Casual Counterfeiter", in *Proceedings of the Second International Workshop on Information Hiding* (Portland, Apr 98), Springer LNCS v 1525 pp 1–15
- [563] LC Guillou, M Ugon, JJ Quisquater, "The Smart Card—A Standardised Security Device Dedicated to Public Cryptology", in [1171] pp 561–613
- [564] R Gupta, SA Smolka, S Bhaskar, "On Randomization in Sequential and Distributed Algorithms", in *ACM Computing Surveys* v 26 no 1 (March 94) pp 7–86
- [565] J Gurnsey, 'Copyright Theft', Aslib, 1997; ISBN 0-566-07631-4
- [566] P Gutmann, "Secure Deletion of Data from Magnetic and Solid-State Memory", in *Sixth USENIX Security Symposium Proceedings* (July 1996) pp 77–89
- [567] P Gutmann, "Software Generation of Practically Strong Random Numbers", in *Seventh Usenix Security Symposium Proceedings* (Jan 1998) pp 243–257
- [568] P Gutmann, "Data Remanence in Semiconductor Devices", in *Usenix Security Symposium* (2001)
- [569] P Gutmann, "Invalid banking cert spooks only one user in 300", *Cryptography List* May 16 2005; at <http://www.mail-archive.com/cryptography%40metzdowd.com/msg03852.html>
- [570] P Gutmann, "A Cost Analysis of Windows Vista Content Protection", April 2007, at http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html
- [571] P Gutmann, "Commercial CAPTCHA-breakers for sale", *Cryptography List* Oct 22 2007, at <http://www.mail-archive.com/cryptography%40metzdowd.com/msg08203.html>; see also <http://www.lafdc.com/captcha/>
- [572] S Haber, WS Stornetta, "How to time-stamp a digital document", in *Journal of Cryptology* v 3 no 2 (1991) pp 99–111
- [573] S Haber, WS Stornetta, "Secure Names for Bit-Strings", in *4th ACM Conference on Computer and Communications Security* (1997) pp 28–35

- [574] W Hackmann, "Asdics at war", in *IEE Review* v 46 no 3 (May 2000) pp 15–19
- [575] "Chris Carey Arrested In New Zealand", in *Hack Watch News* (9/1/1999), at <http://www.iol.ie/~kooltek/legal.html>
- [576] N Hager, *'Secret Power—New Zealand's Role in the International Spy Network'*, Craig Potton Publishing (1996) ISBN 0-908802-35-8
- [577] JA Halderman, "Amazon's MP3 Store Wisely Forgoes Watermarks", Oct 2 2007, at <http://www.freedom-to-tinker.com/?p=1207>
- [578] PS Hall, TK Garland-Collins, RS Picton, RG Lee, *'Radar'*, Brassey's New Battlefield Weapons Systems and Technology Series (v 9), ISBN 0-08-037711-4
- [579] Hall of Shame, at <http://www.pluralsight.com/wiki/default.aspx/Keith.HallOfShame>; see also http://www.threatcode.com/admin_rights.htm
- [580] H Handschuh, P Paillier, J Stern, "Probing attacks on tamper-resistant devices", in *Cryptographic Hardware and Embedded Systems—CHES 99*, Springer LNCS v 1717 pp 303–315
- [581] R Hanley, "Millions in thefts plague New Jersey area", in *New York Times*, February 9, 1981, late city final edition, section A; p 1
- [582] R Hanson, "Can wiretaps remain cost-effective?", in *Communications of the ACM* v 37 no 12 (Dec 94) pp 13–15
- [583] V Harrington, P Mayhew, *'Mobile Phone Theft'*, UK Home Office Research Study 235, January 2002
- [584] MA Harrison, ML Ruzzo, JD Ullman, "Protection in Operating Systems", in *Communications of the ACM* v 19 no 8 (Aug 1976) pp 461–471
- [585] A Hassey, M Wells, "Clinical Systems Security—Implementing the BMA Policy and Guidelines", in [43] pp 79–94
- [586] Health and Safety Executive, nuclear safety reports at <http://www.hse.gov.uk/nsd/>, especially *'HSE Team Inspection of the Control and Supervision of Operations at BNFL's Sellafield Site'*, <http://www.hse.gov.uk/nsd/team.htm>
- [587] LJ Heath, *'An Analysis of the Systemic Security Weaknesses of the US Navy Fleet Broadcasting System 1967–1974, as Exploited by CWO John Walker'*, MSc Thesis, Georgia Tech, at <http://www.fas.org/irp/eprint/heath.pdf>

- [588] T Heim, "Outrage at 500,000 DNA database mistakes", *Daily Telegraph*, Aug 28 2007
- [589] N Heintze, "Scalable Document Fingerprinting", in *Second USENIX Workshop on Electronic Commerce* (1996), ISBN 1-880446-83-9 pp 191–200
- [590] S Helmers, "A Brief History of anon.penet.fi—The Legendary Anonymous Remailer", *CMC Magazine*, Sep 1997; at <http://www.december.com/cmc/mag/1997/sep/helmers.html>
- [591] D Hencke, "Child benefit workers kept out of loop on data security", in *The Guardian* Dec 15 2007, at <http://politics.guardian.co.uk/homeaffairs/story/0,,2227999,00.html>
- [592] E Henning, "The Stamp of Incompetence", *c't magazine*, Sep 3 2007; at <http://www.heise-security.co.uk/articles/95341>
- [593] Sir ER Henry, 'Classification and Uses of Finger Prints' George Rutledge & Sons, London, 1900
- [594] I Herbert, "No evidence against man in child porn inquiry who 'killed himself'", in *The Independent* Oct 1 2005, at <http://news.independent.co.uk/uk/legal/article316391.ece>
- [595] Herodotus, 'Histories'; Book 1 123.4, Book 5 35.3 and Book 7 239.3
- [596] "Interview with David Herson - SOGIS", September 25, 1996, in *Ingeniørenet*, at <http://www.ing.dk/redaktion/herson.htm>
- [597] A Herzberg, M Jakobsson, S Jarecki, H Krawczyk, M Yung, "Proactive Public Key and Signature Systems", *4th ACM Conference on Computer and Communications Security* (1997) pp 100–110
- [598] RA Hettinga, "Credit Card Fraud Higher. Credit Card Fraud Lower", in *nettime* (22/3/2000), at <http://www.nettime.org/nettime.w3archive/200003/msg00184.html>
- [599] M Hewish, "Combat ID advances on all fronts", in *International Defense Review* v 29 (Dec 96) pp 18–19
- [600] Hewlett-Packard, 'IA-64 Instruction Set Architecture Guide', at <http://devresource.hp.com/devresource/Docs/Refs/IA64ISA/index.html>
- [601] TS Heydt-Benjamin, DV Bailey, K Fu, A Juels, T OHare, "Vulnerabilities in First-Generation RFID-enabled Credit Cards", in *Proceedings of Eleventh International Conference on Financial Cryptography and Data Security*, 2007

- [602] HM Heys, "A Tutorial on Linear and Differential Cryptanalysis", in *Cryptologia* v XXVI no 3 (Jul 2002) pp 189–221; at www.engr.mun.ca/~howard/PAPERS/ldc-tutorial.ps
- [603] M Hickley, "Taliban tapping British troops' mobiles to taunt soldiers' families", in *Daily Mail*, Aug 22 2007
- [604] HJ Highland "Electromagnetic Radiation Revisited", in *Computers & Security* v5 (1986) 85–93 and 181–184
- [605] HJ Highland, "Perspectives in Information Technology Security", in *Proceedings of the 1992 IFIP Congress, 'Education and Society', IFIP A-13 v II* (1992) pp 440–446
- [606] TF Himdi, RS Sandhu, "Lattice-Based Models for Controlled Sharing of Confidential Information in the Saudi Hajj System", in *13th Annual Computer Security Applications Conference*, San Diego, California, December 8–12 1997; proceedings published by the IEEE Computer Society, ISBN 0-8186-8274-4; pp 164–174
- [607] Eric von Hippel, "Open Source Software Projects as User Innovation Networks", *Open Source Software Economics 2002* (Toulouse)
- [608] Jack Hirshleifer, "Privacy: Its Origin, Function and Future", in *Journal of Legal Studies* v 9 (Dec 1980) pp 649–664
- [609] Jack Hirshleifer, "From weakest-link to best-shot: the voluntary provision of public goods", in *Public Choice* v 41, (1983) pp 371–386
- [610] Jack Hirshleifer, *Economic behaviour in Adversity*, University of Chicago Press, 1987
- [611] T Hobbes, *Leviathan, or The Matter, Forme and Power of a Common Wealth Ecclesiasticall and Civil, commonly called Leviathan* (1651)
- [612] J Hoffman, "Implementing RBAC on a Type Enforced System", in *13th Annual Computer Security Applications Conference*, San Diego, California, December 8–12 1997; proceedings published by the IEEE Computer Society, ISBN 0-8186-8274-4; pp 158–163
- [613] P Hoffmann, "Microsoft Windows Root Certificate Security Issues", 2007, at <http://www.proper.com/root-cert-problem/>
- [614] S Hoffmann, "Salesforce.com Responds To Phishing Scams", on *CNN*, Nov 8 2007, at <http://www.cnn.com/security/202804065>

- [615] G Hogben, "Security Issues and Recommendations for Online Social Networks", *ENISA Position Paper*, Oct 2007
- [616] G Hoglund, G McGraw, 'Exploiting Software—How to Break Code', Addison Wesley 2004
- [617] G Hoglund, G McGraw, 'Exploiting Online Games—Cheating Massively Distributed Systems', Addison-Wesley 2007
- [618] P Hollinger, "Single language for barcode Babel", in *Financial Times* (25/7/2000) p 15
- [619] C Holloway, "Controlling the Use of Cryptographic Keys", in *Computers and Security* v 14 no 7 (95) pp 587–598
- [620] DI Hopper, "Authorities Sue Adult Web Sites", in *Washington Post* (23/8/2000); at <http://www.washingtonpost.com/>
- [621] G Horn, B Preneel, "Authentication and Payment in Future Mobile Systems", in *ESORICS 98*, Springer LNCS v 1485, pp 277–293; journal version in *Journal of Computer Security* v 8 no 2–3 (2000) pp 183–207
- [622] JD Horton, R Harland, E Ashby, RH Cooper, WF Hyslop, DG Nickerson, WM Stewart, OK Ward, "The Cascade Vulnerability Problem", in *Journal of Computer Security* v 2 no 4 (93) pp 279–290
- [623] V Hougham, "Sociological Skills Used in the Capture of Saddam Hussein", in *Footnotes* (Jul/Aug 2005), at <http://www.asanet.org/footnotes/julyaugust05/fn3.html>
- [624] House of Commons Health Committee, 'The ELeCtronic Patient Record', 6th Report of Session 2006–7, at <http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422.pdf>
- [625] House of Lords Science and Technology Committee, 'Personal Internet Security', 5th Report of Session 2006–7
- [626] JD Howard, 'An Analysis Of Security Incidents On The Internet 1989–1995', PhD thesis (1997), Carnegie Mellon University, at <http://www.cert.org/research/JHThesis/Start.html>
- [627] M Howard, D LeBlanc, 'Writing Secure Code', (second edition), Microsoft Press 2002, ISBN 0-7356-1722-8
- [628] D Howell, "Counterfeit technology forges ahead", in *The Daily Telegraph* (22/3/1999), available at <http://www.telegraph.co.uk:80/>

- [629] A Huang, *'Hacking the Xbox—An Introduction to Reverse Engineering'*, No Starch Press (2003)
- [630] Q Hu, JY Yang, Q Zhang, K Liu, XJ Shen, "An automatic seal imprint verification approach", in *Pattern Recognition* v 28 no 8 (Aug 95) pp 251–266
- [631] G Huber, "CMW Introduction", in *ACM SIGSAC* v 12 no 4 (Oct 94) pp 6–10
- [632] N Htoo-Mosher, R Nasser, N Zunic, J Straw, "E4 ITSEC Evaluation of PRISM on ES/9000 Processors", in *19th National Information Systems Security Conference* (1996), proceedings published by NIST, pp 1–11
- [633] M Hypponen, "Malware goes mobile", in *Scientific American* Nov 2006 pp 70–77
- [634] "Role of Communications in Operation Desert Storm", in *IEEE Communications Magazine* (Special Issue) v 30 no 1 (Jan 92)
- [635] "New England shopping mall ATM scam copied in UK", in *Information Security Monitor* v 9 no 7 (June 94) pp 1–2
- [636] "Pink Death Strikes at US West Cellular", in *Information Security Monitor* v 9 no 2 (Jan 94) pp 1–2
- [637] Independent Security Evaluators Inc., "Content Protection for Optical Media", May 2005, at www.securityevaluators.com/eval/spdc_aacs_2005.pdf
- [638] Information Systems Audit and Control Association, *'Control Objectives for Information and related Technology'*, at <http://www.isaca.org/cobit.htm>
- [639] Information Systems Audit and Control Association, *'Exam Preparation Materials available from ISACA'*, at <http://www.isaca.org/cert1.htm>
- [640] International Atomic Energy Authority (IAEA), *'The Physical Protection of Nuclear Material and Nuclear Facilities'*, INFCIRC/225/Rev 4, <http://www.iaea.org/Publications/Documents/Infcircs/1999/infcirc225r4c/rev4.content.html>
- [641] IBM, *'IBM 4758 PCI Cryptographic Coprocessor—CCA Basic Services Reference and Guide'*, Release 1.31 for the IBM 4758-001, available through <http://www.ibm.com/security/cryptocards/>
- [642] *IEE Electronics and Communications Engineering Journal* v 12 no 3 (June 2000)—special issue on UMTS

- [643] *IEEE Carnahan Conference*, <http://www.carnahanconference.com/>
- [644] *IEEE Spectrum*, special issue on nuclear safekeeping, v 37 no 3 (Mar 2000)
- [645] "Ex-radio chief 'masterminded' TV cards scam", in *The Independent* 17/2/1998; see also "The Sinking of a Pirate", *Sunday Independent*, 1/3/1998
- [646] Intel Corporation, '*Intel Architecture Software Developer's Manual—Volume 1: Basic Architecture*', Order number 243190 (1997)
- [647] Intel Corporation and others, '*Advanced Access Content System (AACSLA)—Technical Overview (informative)*', July 21 2004, at <http://www.aacsla.com/home>
- [648] International Electrotechnical Commission, '*Digital Audio Interface*', IEC 60958, Geneva, February 1989
- [649] T Iwata, K Kurosawa, "OMAC: One-Key CBC MAC", in *Fast Software Encryption* (2003) Springer LNCS v 2887 pp 129–153
- [650] C Jackson, DR Simon, DS Tan, A Barth, "An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks", *USEC 2007*; at www.usablesecurity.org/papers/jackson.pdf
- [651] I Jackson, personal communication
- [652] L Jackson, "BT forced to pay out refunds after free calls fraud", in *The Sunday Telegraph* (9/2/1997); at <http://www.telegraph.co.uk:80/>
- [653] TN Jagatic, NA Johnson, M Jakobsson, F Menczer, "Social Phishing", in *Communications of the ACM* v 50 no 10 (Oct 2007) pp 94–100
- [654] G Jagpal, '*Steganography in Digital Images*', undergraduate thesis, Selwyn College, Cambridge University, 1995
- [655] AK Jain, R Bolle, S Pankanti, '*Biometrics—Personal Identification in Networked Society*', Kluwer (1999); ISBN 0-7923-8346-1
- [656] AK Jain, L Hong, S Pankanti, R Bolle, "An Identity-Authentication System Using Fingerprints", in *Proceedings of the IEEE* v 85 no 9 (Sep 97) pp 1365–1388
- [657] S Jajodia, W List, G McGregor, L Strous (editors), '*Integrity and Internal Control in Information Systems—Volume 1: Increasing the confidence in information systems*', Chapman & Hall (1997) ISBN 0-412-82600-3

- [658] M Jakobsson, "Modeling and Preventing Phishing Attacks", in *Financial Cryptography 2005*, at www.informatics.indiana.edu/markus/papers/phishing-jakobsson.pdf
- [659] M Jakobsson, S Myers, *Phishing and Countermeasures*, Wiley 2007
- [660] M Jakobsson, Z Ramzan, *Crimeware*, Addison-Wesley 2008
- [661] M Jay, "ACPO's intruder policy — underwritten?", in *Security Surveyor* v 26 no 3 (Sep 95) pp 10–15
- [662] D Jedig, "Security by example", 2006, at <http://syneticon.net/support/security/security-by-example.html>
- [663] N Jefferies, C Mitchell, M Walker, "A Proposed Architecture for Trusted Third Party Services", in *Cryptography: Policy and Algorithms*, Springer LNCS v 1029 pp 98–104
- [664] R Jenkins, "Hole-in-wall thief used MP3 player", in *The Times* Nov 15 2006; at <http://www.timesonline.co.uk/article/0,,29389-2453590,00.html>
- [665] A Jerichow, J Müller, A Pfitzmann, B Pfitzmann, M Waidner, "Real-Time Mixes: a Bandwidth-Efficient Anonymity Protocol", in *IEEE Journal on Special Areas in Communications* v 16 no 4 (May 98) pp 495–509
- [666] John Young Architect, <http://www.jya.com>
- [667] K Johnson, "One Less Thing to Believe In: Fraud at Fake Cash Machine", in *New York Times* 13 May 1993 p 1
- [668] RG Johnston, ARE Garcia, "Vulnerability Assessment of Security Seals", in *Journal of Security Administration* v 20 no 1 (June 97) pp 15–27; the Vulnerability Assessment Team's papers are at <http://pearl1.lanl.gov/seals/>, backed up at <http://www.cl.cam.ac.uk/~rja14/preprints/Johnston/for-non-US-readers>
- [669] P Jones, "Protection money", in *Computer Business Review* v 4 no 12 (Dec 96) pp 31–36
- [670] RV Jones, *Most Secret War*, Wordsworth Editions (1978,1998) ISBN 1-85326-699-X
- [671] RV Jones, *Reflections on Intelligence*, Octopus (1989) ISBN 0-7493-0474-X

- [672] J Jonsson, B Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447
- [673] A Jøsang, K Johannesen, "Authentication in Analogue Telephone Access Networks", in *Pragocrypt 96*, proceedings published by CTU Publishing House, Prague, ISBN 80-01-01502-5; pp 324–336
- [674] Dorothy Judd v Citibank, 435 NYS, 2d series, pp 210–212, 107 Misc.2d 526
- [675] MY Jung, "Biometric Market and Industry Overview", *IBG*, Dec 8 2005; at <http://events.wcoomd.org/files/style%20elements/17-Jung-IBG%20-%20Biometric%20Market%20and%20Industry%20overview.pdf>
- [676] D Kahn, *The Codebreakers*, Macmillan (1967)
- [677] D Kahn, *Seizing the Enigma*, Houghton Mifflin (1991); ISBN 0-395-42739-8
- [678] D Kahn, "Soviet Comint in the Cold War", in *Cryptologia* v XXII no 1 (Jan 98) pp 1–24
- [679] D Kahneman, "Maps of Bounded Rationality: a Perspective on Intuitive Judgment and Choice", Nobel Prize Lecture, 2002
- [680] B Kaliski, "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315
- [681] JB Kam, GI Davida, "A Structured Design of Substitution-Permutation Encryption Network", in *Foundations of Secure Computation*, Academic Press (1978)
- [682] M Kam, G Fielding, R Conn, "Writer Identification by Professional Document Examiners", in *Journal of Forensic Sciences* v 42 (1997) pp 778–786
- [683] M Kam, G Fielding, R Conn, "Effects of Monetary Incentives on Performance of Nonprofessionals in Document Examination Proficiency Tests", in *Journal of Forensic Sciences* v 43 (1998) pp 1000–1004
- [684] MS Kamel, HC Shen, AKC Wong, RI Campeanu, "System for the recognition of human faces", in *IBM Systems Journal* v 32 no 2 (1993) pp 307–320
- [685] MH Kang, IS Moskowitz, "A Pump for Rapid, Reliable, Secure Communications", in *1st ACM Conference on Computer and Communications*

- Security*, 3–5/11/93, Fairfax, Virginia; Proceedings published by the ACM, ISBN 0-89791-629-8, pp 118–129
- [686] MH Kang, JN Froscher, J McDermott, O Costich, R Peyton, “Achieving Database Security through Data Replication: The SINTRA Prototype”, in *17th National Computer Security Conference* (1994) pp 77–87
- [687] MH Kang, IS Moskowitz, DC Lee, “A Network Pump”, in *IEEE Transactions on Software Engineering* v 22 no 5 (May 96) pp 329–338
- [688] MH Kang, IS Moskowitz, B Montrose, J Parsonese, “A Case Study of Two NRL Pump Prototypes”, in *12th Annual Computer Security Applications Conference*, San Diego CA, December 9–13 1996; proceedings published by the IEEE, ISBN 0-8186-7606-X, pp 32–43
- [689] MH Kang, JN Froscher, IS Moskowitz, “An Architecture for Multilevel Secure Interoperability”, in *13th Annual Computer Security Applications Conference*, San Diego, California, December 8–12 1997; proceedings published by the IEEE Computer Society, ISBN 0-8186-8274-4; pp 194–204
- [690] CS Kaplan, “Privacy Plan Likely to Kick Off Debate”, in *New York Times* (28 July 2000), at <http://www.nytimes.com/>
- [691] MH Kang, IS Moskowitz, S Chinchek, “The Pump: A Decade of Covert Fun”, at *21st Annual Computer Security Applications Conference* (2005)
- [692] PA Karger, VA Austell, DC Toll, “A New Mandatory Security Policy Combining Secrecy and Integrity”, *IBM Research Report RC 21717* (97406) 15/3/2000
- [693] PA Karger, RR Schell, “Thirty Years Later’: Lessons from the Multics Security Evaluation”, at *ACSAC 2002* pp 119–126
- [694] S Karp, “Facebook’s Public Search Listing Is Problematic for Users”, in *Digitalmediawire* Sep 5 2007, at <http://www.dmwmedia.com/news/2007/09/06/facebook-s-public-search-listing-is-problematic-for-users>
- [695] F Kasiski, ‘*Die Geheimschriften und die Dechiffrier-Kunst*’, Mittler & Sohn, Berlin (1863)
- [696] ‘*KASUMI Specification*’, ETSI/SAGE v 1 (23/12/1999), at <http://www.etsi.org/dvbandca/>
- [697] S Katzenbeisser, FAP Petitcolas, ‘*Information hiding—Techniques for steganography and digital watermarking*’, Artech House (2000) ISBN 1-58053-035-4

- [698] C Kaufman, R Perlman, M Speciner, *'Network Security—Private Communication in a Public World'*, Prentice Hall 1995; ISBN 0-13-061466-1
- [699] DT Keitkemper, SF Platek, KA Wolnik, "DNA versus fingerprints", in *Journal of Forensic Sciences* v 40 (1995) p 534
- [700] GC Kelling, C Coles, *'Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities'* Martin Kessler Books (1996)
- [701] L Kelly, T Young, in *Computing* Jan 25 2007; at <http://www.vnunet.com/computing/news/2173365/uk-firms-naive-usb-stick>
- [702] J Kelsey, B Schneier, D Wagner, "Protocol Interactions and the Chosen Protocol Attack", in *Security Protocols—Proceedings of the 5th International Workshop* (1997) Springer LNCS v 1361 pp 91–104
- [703] J Kelsey, B Schneier, D Wagner, C Hall, "Cryptanalytic Attacks on Pseudorandom Number Generators", in *Fifth International Workshop on Fast Software Encryption* (1998), Springer LNCS v 1372 pp 168–188
- [704] J Kelsey, B Schneier, D Wagner, C Hall, "Side Channel Cryptanalysis of Product Ciphers," in *ESORICS 98*, Springer LNCS v 1485 pp 97–110
- [705] R Kemp, N Towell, G Pike, "When seeing should not be believing: Photographs, credit cards and fraud", in *Applied Cognitive Psychology* v 11 no 3 (1997) pp 211–222
- [706] R Kemmerer, "Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels", in *IEEE Transactions on Computer Systems* v 1 no 3 (1983) pp 256–277
- [707] R Kemmerer, C Meadows, J Millen, "Three Systems for Cryptographic Protocol Analysis", in *Journal of Cryptology* v 7 no 2 (Spring 94) pp 79–130
- [708] MG Kendall, B Babington-Smith, "Randomness and Random Sampling Numbers", part 1 in *Journal of the Royal Statistical Society* v 101 pp 147–166; part 2 in *Supplement to the Journal of the Royal Statistical Society*, v 6 no 1 pp 51–61
- [709] T Kendall, "Pornography, Rape, and the Internet", at *The Economics of the Software and Internet Industries* (Softint 2007), at <http://people.clemson.edu/~tkendal/internetcrime.pdf>
- [710] ST Kent, MI Millett, *'Who Goes There? Authentication Through the Lens of Privacy'*, National Research Council 2003; at http://www.nap.edu/catalog.php?record_id=10656

- [711] JO Kephardt, SR White, "Measuring and Modeling Computer Virus Prevalence", in *Proceedings of the 1993 IEEE Symposium on Security and Privacy* pp 2–15
- [712] JO Kephardt, SR White, DM Chess, "Epidemiology of computer viruses", in *IEEE Spectrum* v 30 no 5 (May 93) pp 27–29
- [713] A Kerckhoffs, "La Cryptographie Militaire", in *Journal des Sciences Militaires*, 9 Jan 1883, pp 5–38; <http://www.cl.cam.ac.uk/users/fapp2/kerckhoffs/>
- [714] OS Kerr, "Computer Records and the Federal Rules of Evidence", in *USA Bulletin* (Mar 2001), at <http://www.usdoj.gov/criminal/cybercrime/usamarch2001.4.htm>
- [715] PJ Kerry, "EMC in the new millennium", in *Electronics and Communication Engineering Journal* v 12 no 2 pp 43–48
- [716] D Kesdogan, H Federrath, A Jerichow, "Location Management Strategies Increasing Privacy in Mobile Communication", in *12th International Information Security Conference (1996)*, Samos, Greece; proceedings published by Chapman & Hall, ISBN 0-412-78120-4, pp 39–48
- [717] J Kilian, P Rogaway, "How to protect DES Against Exhaustive Key Search", in *Advances in Cryptology—Crypto 96* Springer LNCS v 1109 pp 252–267
- [718] J King, "Bolero — a practical application of trusted third party services", in *Computer Fraud and Security Bulletin* (July 95) pp 12–15
- [719] Kingpin, "iKey 1000 Administrator Access and Data Compromise", in *BugTraq* (20/7/2000), at <http://www.L0pht.com/advisories.html>
- [720] DV Klein, "Foiling the Cracker; A Survey of, and Improvements to Unix Password Security", *Proceedings of the USENIX Security Workshop*. (1990); <http://www.deter.com/unix/>
- [721] RL Klevans, RD Rodman, 'Voice Recognition', Artech House (1997); ISBN 0-89006-927-1
- [722] HM Kluepfel, "Securing a Global Village and its Resources: Baseline Security for Interconnected Signaling System # 7 Telecommunications Networks", in *First ACM Conference on Computer and Communications Security* (1993), proceedings published by the ACM, ISBN 0-89791-629-8, pp 195–212; later version in *IEEE Communications Magazine* v 32 no 9 (Sep 94) pp 82–89

- [723] N Koblitz, *'A Course in Number Theory and Cryptography'*, Springer Graduate Texts in Mathematics no 114 (1987), ISBN 0-387-96576-9
- [724] N Koblitz, A Menezes, "Another Look at 'Provable Security' ", in *Journal of Cryptology* v 20 no 1 (2007) pp 3–37
- [725] ER Koch, J Sperber, *'Die Datenmafia'*, Rohwolt Verlag (1995) ISBN 3-499-60247-4
- [726] M Kochanski, "A Survey of Data Insecurity Devices", in *Cryptologia* v IX no 1 pp 1–15
- [727] P Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", in *Advances in Cryptology–Crypto 96* Springer LNCS v 1109 pp 104–113
- [728] P Kocher, "Differential Power Analysis", in *Advances in Cryptology–Crypto 99* Springer LNCS v 1666 pp 388–397; a brief version was presented at the rump session of Crypto 98
- [729] P Kocher, "Design and Validation Strategies for Obtaining Assurance in Countermeasures to Power Analysis and Related Attacks", at *FIPS Physical Security Workshop*, Hawaii 2005; at <http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper09.pdf>
- [730] KJ Koelman, "A Hard Nut to Crack: The Protection of Technological Measures", in *European Intellectual Property Review* (2000) pp 272–288; at <http://www.ivir.nl/Publicaties/koelman/hardnut.html>
- [731] T Kohno, A Stubblefield, AD Rubin, DS Wallach, "Analysis of an Electronic Voting System", Johns Hopkins TR 2003-19; also published in *IEEE Symposium on Security and Privacy* (2004)
- [732] S Kokolakis, D Gritzalis, S Katsikas, "Generic Security Policies for Health Information Systems", in *Health Informatics Journal* v 4 nos 3–4 (Dec 1998) pp 184–195
- [733] O Kömmerling, MG Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors", in *Usenix Workshop on Smartcard Technology*, proceedings published by Usenix (1999), ISBN 1-880446-34-0 pp 9–20
- [734] A Kondi, R Davis, "Software Encryption in the DoD", in *20th National Information Systems Security Conference* (1997), proceedings published by NIST, pp 543–554

- [735] LD Koontz, VC Melvin, "Health Information Technology—Efforts Continue but Comprehensive Privacy Approach Needed for National Strategy", GAO, 2007; at <http://www.gao.gov/new.items/d07988t.pdf>
- [736] BJ Koops, 'Crypto Law Survey', at <http://rechten.uvt.nl/koops/cryptolaw/>; see also his thesis 'The Crypto Controversy: A Key Conflict in the Information Society'
- [737] C Kopp, "Electromagnetic Bomb—Weapon of Electronic Mass Destruction", at <http://www.abovetopsecret.com/pages/ebomb.html>
- [738] DP Kormann, AD Rubin, "Risks of the Passport Single Signon Protocol", in *Computer Networks* (July 2000); at <http://avirubin.com/vita.html>
- [739] M Kotadia, "Citibank e-mail looks phishy: Consultants", *Zdnet* Nov 9 2006; at <http://www.zdnet.com.au/news/security/soa/Citibank-e-mail-looks-phishy-Consultants/0,130061744,339272126,00.htm>
- [740] KPHO, "Sodomized Ex-McDonald's Employee Wins \$6.1 M", KPHO, Oct 6 2007; at <http://www.kpho.com/news/14277937/detail.html>
- [741] H Krawczyk, M Bellare, R Canetti, 'HMAC: Keyed-Hashing for Message Authentication', RFC 2104 (Feb 1997), at <http://www.faqs.org/rfcs/rfc2104.html>
- [742] B Krebs, "Just How Bad Is the Storm Worm?", in *The Washington Post* Oct 1 2007; at http://blog.washingtonpost.com/securityfix/2007/10/the_storm_worm_maelstrom_or_te.html
- [743] B Krebs, "Salesforce.com Acknowledges Data Loss", in *The Washington Post* Nov 6 2007; at http://blog.washingtonpost.com/securityfix/2007/11/salesforcecom_acknowledges_dat.html
- [744] S Krempel, "Lauschangriff am Geldautomaten", in *Der Spiegel* Jan 8 1999; at <http://web.archive.org/web/20001031024042/http://www.spiegel.de/netzwelt/technologie/0,1518,13731,00.html>
- [745] HM Kriz, "Phreaking recognised by Directorate General of France Telecom", in *Chaos Digest* 1.03 (Jan 93)
- [746] I Krsul, EH Spafford, "Authorship analysis: identifying the author of a program", in *Computers and Security* v 16 no 3 (1996) pp 233–257
- [747] D Kügler, " 'Man in the Middle' Attacks on Bluetooth", in *Financial Cryptography 2004*, Springer LNCS v 2742 pp 149–161

- [748] MG Kuhn, "Cipher Instruction Search Attack on the Bus-Encryption Security Microcontroller DS5002FP", in *IEEE Transactions on Computers* v 47 no 10 (Oct 1998) pp 1153–1157
- [749] MG Kuhn, private communication
- [750] MG Kuhn, "Optical Time-Domain Eavesdropping Risks of CRT Displays" in *IEEE Symposium on Security and Privacy* (2002)
- [751] MG Kuhn, "An Asymmetric Security Mechanism for Navigation Signals", in *Information Hiding 2004* Springer LNCS 3200 pp 239–252
- [752] MG Kuhn, "Electromagnetic Eavesdropping Risks of Flat-Panel Displays", in *PET 2004*, at <http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf>
- [753] MG Kuhn, RJ Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations", in *Proceedings of the Second International Workshop on Information Hiding* (Portland, Apr 98), Springer LNCS v 1525 pp 126–143
- [754] R Kuhn, P Edfors, V Howard, C Caputo, TS Philips, "Improving Public Switched Network Security in an Open Environment", in *Computer*, August 1993, pp 32–35
- [755] S Kumar, C Paar, J Pelzl, G Pfeiffer, M Schimmler, "Breaking Ciphers with COPACOBANA—A Cost-Optimized Parallel Code Breaker", in *CHES 2006* and at <http://www.copacobana.org/>
- [756] J Kuo, "Storm Drain", in *Anti-Malware Engineering Team blog*, Sep 20 2007, at <http://blogs.technet.com/antimalware/default.aspx>
- [757] GD Kutz, G Aloise, JW Cooney, 'NUCLEAR SECURITY—Actions Taken by NRC to Strengthen Its Licensing Process for Sealed Radioactive Sources Are Not Effective', GAO Report GAO-07-1038T, July 12, 2007
- [758] Greg L, "ID Theft, RMT and Lineage", *Terra Nova* Jul 2007, at http://terranova.blogs.com/terra_nova/2006/07/id_theft_rmt_nc.html#more
- [759] 'L0phtCrack 2.52 for Win95/NT', at <http://www.l0pht.com/l0phtcrack/>
- [760] J Lacy, SR Quackenbush, A Reibman, JH Snyder, "Intellectual Property Protection Systems and Digital Watermarking", in *Proceedings of the Second International Workshop on Information Hiding* (Portland, Apr 98), Springer LNCS v 1525 pp 158–168
- [761] RJ Lackey, DW Upmal, "Speakeasy: The Military Software Radio", in *IEEE Communications Magazine* v 33 no 5 (May 95) pp 56–61

- [762] P Ladkin, "Flight Control System Software Anomalies", *comp.risks* v 24 no 03, Aug 31 2005, at <http://www.mail-archive.com/risks@csl.sri.com/msg00319.html>
- [763] Lamarr/Antheil Patent Story Home Page, <http://www.ncafe.com/chris/pat2/index.html>; contains US patent no 2,292,387 (HK Markey et al., Aug 11 1942)
- [764] G Lambourne, *The Fingerprint Story*, Harrap (1984) ISBN 0-245-53963-8
- [765] L Lamont, "And the real Lotto winner is . . . that man at the cash register", *Sydney Morning Herald*, May 3 2007, at <http://www.smh.com.au/articles/2007/05/02/1177788228072.html>
- [766] L Lamport, "Time, Clocks and the Reordering of Events in a Distributed System", in *Communications of the ACM* v 21 no 7 (July 1978) pp 558–565
- [767] L Lamport, R Shostak, M Pease, "The Byzantine Generals Problem", in *ACM Transactions on Programming Languages and Systems* v 4 no 3 (1982) pp 382–401
- [768] B Lampson, "A Note on the Confinement problem", in *Communications of the ACM* v 16 no 10 (Oct 1973) pp 613–615
- [769] P Lamy, J Martinho, T Rosa, MP Queluz, "Content-Based Watermarking for Image Authentication", in *Proceedings of the Third International Workshop on Information Hiding* (1999), Springer LNCS v 1768 pp 187–198
- [770] S Landau, S Kent, C Brooks, S Charney, D Denning, W Diffie, A Lauck, D Miller, P Neumann, D Sobel, "Codes, Keys and Conflicts: Issues in US Crypto Policy", *Report of the ACM US Public Policy Committee*, June 1994
- [771] M Landler, "Fine-Tuning For Privacy, Hong Kong Plans Digital ID", in *New York Times*, Feb 19 2002; at <http://www.nytimes.com/2002/02/18/technology/18KONG.html>
- [772] R Landley, "Son of DIVX: DVD Copy Control", *Motley Fool*, <http://www.fool.com/portfolios/rulemaker/2000/rulemaker000127.htm>
- [773] P Landrock, "Roles and Responsibilities in BOLERO", in *TEDIS EDI trusted third parties workshop* (1995), proceedings published as ISBN 84-7653-506-6, pp 125–135

- [774] CE Landwehr, AR Bull, JP McDermott, WS Choi, 'A Taxonomy of Computer Program Security Flaws, with Examples', US Navy Report NRL/FR/5542-93-9591 (19/11/93)
- [775] D Lane, "Where cash is king", in *Banking Technology*, Oct 92, pp 38–41
- [776] J Leake, "Workers used forged passes at Sellafield", in *Sunday Times* (2/4/2000) p 6
- [777] S LeBlanc, KE Register, 'Constant Battles: Why We Fight', St Martin's, 2003
- [778] HC Lee, RE Guesslen (eds), 'Advances in Fingerprint Technology', Elsevier (1991) ISBN 0-444-01579-5
- [779] D Leigh, "Crackdown on firms stealing personal data", in *The Guardian* Nov 15 2006; at <http://www.guardian.co.uk/crime/article/0,,1948016,00.html>
- [780] AK Lenstra, HW Lenstra, 'The development of the number field sieve', Springer Lecture Notes in Mathematics v 1554 (1993) ISBN 0-387-57013-6
- [781] AK Lenstra, E Tromer, A Shamir, W Kortsmit, B Dodson, J Hughes, P Leyland, "Factoring estimates for a 1024-bit RSA modulus", in *Asiacrypt 2003*, Springer LNCS 2894 pp 331–346
- [782] K Leonard, "Face Recognition Technology: Security Enhancements v. Civil Rights", 2001 B.C. Intell. Prop. & Tech. F. 120301, at http://www.bc.edu/bc_org/avp/law/st_org/iptf/headlines/content/2001120301.html
- [783] D Leppard, P Nuki, "BA staff sell fake duty-free goods", in *Sunday Times* Sep 12 1999; at http://home.clara.net/brescom/Documents/BA_Fakes.htm
- [784] L Lessig, 'Code and Other Laws of Cyberspace', Basic Books (2000); 'Code: Version 2.0', Basic Books (2006); at <http://www.lessig.org/>
- [785] L Lessig, 'Free Culture: The Nature and Future of Creativity', Penguin (2005); at <http://www.lessig.org/>
- [786] NG Leveson, 'Safeware—System Safety and Computers', Addison-Wesley (1994) ISBN 0-201-11972-2
- [787] S Levitt, SJ Dubner, 'Freakonomics: A Rogue Economist Explores the Hidden Side of Everything', William Morrow, 2005

- [788] A Lewcock, "Bodily Power", in *Computer Business Review* v 6 no 2 (Feb 98) pp 24–27
- [789] O Lewis, "Re: News: London nailbomber used the Net", post to ukcrypto mailing list, 5/6/2000, archived at <http://www.chiark.greenend.org.uk/mailman/listinfo/ukcrypto>
- [790] Lexmark International, Inc., vs Static Control Components, Inc., US Court of Appeals (6th Circuit), Oct 26 2004, at www.eff.org/legal/cases/Lexmark_v_Static_Control/20041026_Ruling.pdf
- [791] J Leyden, "Russian bookmaker hackers jailed for eight years", in *The Register* Oct 4 2006, at http://www.theregister.co.uk/2006/10/04/russian_bookmaker_hackers_jailed/
- [792] J Leyden, "Thai police crack credit card wiretap scam", in *The Register* Aug 4 2006, at http://www.theregister.co.uk/2006/08/04/thai_wiretap_scam/
- [793] J Leyden, "Hacked to the TK Maxx", in *The Register* Jan 19 2007; at http://www.theregister.co.uk/2007/01/19/tjx_hack_alert/
- [794] J Leyden, "Italy tops global wiretap league", in *The Register*, Mar 7 2007; at http://www.theregister.co.uk/2007/03/07/wiretap_trends_ss8/
- [795] J Leyden, "Feds told they need warrants for webmail", in *The Register* June 19 2007; at http://www.theregister.co.uk/2007/06/19/webmail_wiretaps_appeal/
- [796] J Leyden, "MySpace phishing scam targets music fans", in *The Register*, Oct 14 2006; at http://www.theregister.co.uk/2006/10/14/myspace_phishing_scam/
- [797] J Leyden, "Program Names govern admin rights in Vista, in *The Register*, Apr 23 2007; at http://www.theregister.co.uk/2007/04/23/vista_program_naming_oddness/
- [798] CC Lin, WC Lin, "Extracting facial features by an inhibiting mechanism based on gradient distributions", in *Pattern Recognition* v 29 no 12 (Dec 96) pp 2079–2101
- [799] R Linde, "Operating Systems Penetration," *National Computer Conference*, AFIPS (1975) pp 361–368

- [800] JPMG Linnartz, "The 'Ticket' Concept for Copy Control Based on Embedded Signalling", *Fifth European Symposium on Research in Computer Security* (ESORICS 98), Springer LNCS 1485 pp 257–274
- [801] E Linos, E Linos, G Colditz, "Screening programme evaluation applied to airport security", *British Medical Journal* v 335, Dec 22 2007 pp 1290–1292; <http://www.bmj.com/cgi/content/full/335/7633/1290>
- [802] J Linsky and others, 'Bluetooth-simple pairing whitepaper', from www.bluetooth.com
- [803] JPMG Linnartz, M van Dijk, "Analysis of the Sensitivity Attack Against Electronic Watermarks in Images", in [97] pp 258–272
- [804] D Litchfield, C Anley, J Heasman, B Grindlay, *The Database Hacker's Handbook: Defending Database Servers*, Wiley 2005
- [805] B Littlewood, "Predicting software reliability", in *Philosophical Transactions of the Royal Society of London* A327 (1989), pp 513–527
- [806] WF Lloyd, *Two Lectures on the Checks to Population*, Oxford University Press (1833)
- [807] Lockheed Martin, "Covert Surveillance using Commercial Radio and Television Signals", at <http://silentsentry.external.lmco.com>
- [808] L Loeb, *Secure Electronic Transactions—Introduction and technical Reference*, Artech House (1998) ISBN 0-89006-992-1
- [809] London School of Economics & Political Science, *The Identity Project—An assessment of the UK Identity Cards Bill & its implications*, 2005, at www.lse.ac.uk/collections/pressAndInformationOffice/PDF/IDreport.pdf
- [810] J Long, *Google Hacking Database*, at <http://johnny.ihackstuff.com/ghdb.php>
- [811] D Longley, S Rigby, "An Automatic Search for Security Flaws in Key Management", *Computers & Security* v 11 (March 1992) pp 75–89
- [812] PA Loscocco, SD Smalley, PA Muckelbauer, RC Taylor, SJ Turner, JF Farrell, "The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments", in *20th National Information Systems Security Conference*, proceedings published by NIST (1998 pp 303–314)

- [813] PA Loscocco, SD Smalley, "Integrating Flexible Support for Security Policies into the Linux Operating System", in *Proceedings of the FREENIX Track: 2001 USENIX Annual Technical Conference (FREENIX '01)* (June 2001). See also NSA SELinux site: <http://www.nsa.gov/selinux>
- [814] JR Lott, *More Guns, Less Crime: Understanding Crime and Gun-Control Laws*, University of Chicago Press 2000
- [815] J Loughry, DA Umphress, "Information leakage from optical emanations", in *ACM Transactions on Information and System Security* v 5 no 3 (Aug 2002) pp 262–289
- [816] WW Lowrance, *Privacy and Health Research*, Report to the US Secretary of Health and Human Services (May 1997)
- [817] M Ludwig, *The Giant Black Book of Computer Viruses*, American Eagle Publishers (1995) ISBN 0-929408-10-1
- [818] J Lukàš, J Fridrich, M Goljan, "Digital 'bullet scratches' for images", in *ICIP 05*; at <http://www.ws.binghamton.edu/fridrich/Research/ICIP05.pdf>
- [819] M Lyu, *Software Reliability Engineering*, IEEE Computer Society Press (1995), ISBN 0-07-039400-8
- [820] D Mackett, "A Pilot on Airline Security", in *Hot Air*, July 16 2007, at <http://hotair.com/archives/2007/07/16/a-pilot-on-airline-security/>
- [821] Macnn, "iPhone unlock firm threatened by AT&T", Aug 25 2007, at <http://www.macnn.com/articles/07/08/25/iphone.unlock.firm.threat/>
- [822] B Macq, "Special Issue—Identification and protection of Multimedia Information", *Proceedings of the IEEE* v 87 no 7 (July 1999)
- [823] W Madsen, "Airline passengers to be subject to database monitoring", in *Computer Fraud and Security Bulletin* (Mar 97) pp 7–8
- [824] W Madsen, "Crypto AG: The NSA's Trojan Whore?", in *Covert Action Quarterly* (Winter 1998), at <http://www.mediafilter.org/caq/cryptogate/>
- [825] W Madsen, "Government-Sponsored Computer Warfare and Sabotage", in *Computers and Security* v 11 (1991) pp 233–236
- [826] M Maes, "Twin Peaks: The Histogram Attack on Fixed Depth Image Watermarks", in *Proceedings of the Second International Workshop on Information Hiding* (1998), Springer LNCS v 1525 pp 290–305

- [827] M Magee, "HP inkjet cartridges have built-in expiry dates—Carly's cunning consumable plan", *The Inquirer*, 29 April 2003, at <http://www.theinquirer.net/?article=9220>
- [828] K Maguire, "Muckraker who feeds off bins of the famous", in *The Guardian* (27/7/2000), at <http://www.guardianunlimited.co.uk/Labour/Story/0,2763,347535,00.html>
- [829] S Maguire, *Debugging the Development Process*, Microsoft Press, ISBN 1-55615-650-2 p 50 (1994)
- [830] F Main, "Your phone records are for sale", *Chicago Sun-Times*, Jan 5 2006, at <http://blogs.law.harvard.edu/jim/2006/01/08/your-phone-records-are-for-sale-fbi-as-reported-in-the-chicago-sun-times/>
- [831] D Maio, D Maltoni, "Direct Gray-Scale Minutiae Detection in Fingerprints", in *IEEE Transactions on Pattern Analysis and Machine Intelligence* v 19 no 1 (Jan 97) pp 27–40
- [832] D Maltoni, D Maio, AK Jain, S Prabhakar, 'Handbook of Fingerprint Recognition', Springer-Verlag New York, 2003
- [833] S Mangard, E Oswald, T Popp, 'Power Analysis Attacks—Revealing the Secrets of Smartcards', Springer 2007
- [834] T Mansfield, G Kelly, D Chandler, J Kane, 'Biometric Product Testing Final Report, Issue 1.0, 19 March 2001, National Physical Laboratory; at www.cesg.gov.uk/site/ast/biometrics/media/BiometricTest-Reportpt1.pdf
- [835] J Markoff, 'What the Dormouse Said: How the 60s Counterculture Shaped the Personal Computer', Viking Adult (2005)
- [836] L Marks, *Between Silk and Cyanide—a Codemaker's War 1941–1945*, Harper Collins (1998) ISBN 0-68486780-X
- [837] L Martin, "Using Semiconductor Failure Analysis Tools for Security Analysis", FIPS Physical Security Workshop, Hawaii 2005; at <http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper11.pdf>
- [838] S Mason, 'Electronic Evidence—Disclosure, Discovery and Admissibility', LexisNexis Butterworths (2007)
- [839] M Mastanduno, "Economics and Security in Statecraft and Scholarship", *International Organization* v 52 no 4 (Autumn 1998)
- [840] "Reducing the Price of Convenience", B Masuda, *International Security Review* no 82 (Autumn 93) pp 45–48

- [841] JM Matey, O Naroditsky, K Hanna, R Kolczynski, DJ Lolocono, S Mangru, M Tinker, TM Zappia, WY Zhao, "Iris on the Move: Acquisition of Images for Iris recognition in Less Constrained Environments", in *Proc IEEE* v 94 no 11 (Nov 2006) pp 1936–1947
- [842] SA Mathieson. "Gone phishing in Halifax—UK bank sends out marketing email which its own staff identify as a fake", in *Infosecurity News*, Oct 7 2005, at http://www.infosecurity-magazine.com/news/051007_halifax_email.htm
- [843] M Matsui, "Linear Cryptanalysis Method for DES Cipher", in *Advances in Cryptology — Eurocrypt 93*, Springer LNCS v 765 pp 386–397
- [844] M Matsui, "New Block Encryption Algorithm MISTY", in *Fourth International Workshop on Fast Software Encryption* (1997), Springer LNCS v 1267 pp 54–68
- [845] T Matsumoto, H Matsumoto, K Yamada, S Hoshino, "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems" *Proceedings of SPIE* v 4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002
- [846] R Matthews, "The power of one", in *New Scientist* (10/7/1999) pp 26–30; at <http://www.newscientist.com/ns/19990710/thepowerof.html>
- [847] V Matyás, "Protecting the identity of doctors in drug prescription analysis", in *Health Informatics Journal* v 4 nos 3–4 (Dec 1998) pp 205–209
- [848] J Maynard Smith, G Price, "The Logic of Animal Conflict", in *Nature* v 146 (1973) pp 15–18
- [849] D Mazières, MF Kaashoek, "The Design, Implementation and Operation of an Email Pseudonym Server", in *Proceedings of the 5th ACM Conference on Computer and Communications Security* (1998), <http://www.pdos.lcs.mit.edu/~dm>
- [850] J McCormac. 'European Scrambling Systems—The Black Book', version 5 (1996), Waterford University Press, ISBN 1-873556-22-5
- [851] D McCullagh, "U.S. to Track Crypto Trails", in *Wired*, 4/5/2000, at <http://www.wired.com/news/politics/0,1283,36067,00.html>; statistics at <http://www.uscourts.gov/wiretap99/contents.html>
- [852] D McCullagh, R Zarate, "Scanning Tech a Blurry Picture", in *Wired*, Feb 16 2002; at <http://www.wired.com/politics/law/news/2002/02/50470>

- [853] K McCurley, Remarks at IACR General Meeting. *Crypto 98*, Santa Barbara, Ca., Aug 1998
- [854] D McCullough, "A Hook-up Theorem for Multi-Level Security", in *IEEE Transactions on Software Engineering* v 16 no 6 (June 1990) pp 563–568
- [855] P McDaniel, K Butler, W Enck, H Hursti, S McLaughlin, P Traynor, MA Blaze, A Aviv, P Černý, S Clark, E Cronin, G Shah, M Sherr, A Vigna, R Kemmerer, D Balzarotti, G Banks, M Cova, V Felmetser, W Robertson, F Valeur, JL Hall, L Quilter, 'EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing', Final Report, Dec 7, 2007; at <http://www.sos.state.oh.us/sos/info/EVEREST/14-AcademicFinaleVERESTReport.pdf>
- [856] AD McDonald, MG Kuhn, "StegFS: A Steganographic File System for Linux", in [1022] pp 463–477
- [857] D MacEoin, 'The hijacking of British Islam—How extremist literature is subverting mosques in the UK', Policy Exchange (2007)
- [858] G McGraw, 'Software Security—Building Security In', Addison-Wesley, 2006
- [859] G McGraw, EW Felten, 'Java Security', Wiley (1997) ISBN 0-471-17842-X
- [860] J McGroddy, HS Lin, 'A Review of the FBI's Trilogy Information Technology Modernization Program', National Academies Press, 2004, at http://www7.nationalacademies.org/cstb/pub_fbi.html
- [861] J McHugh, "An EMACS Based Downgrader for the SAT" in *Computer and Network Security*, IEEE Computer Society Press (1986) pp 228–237
- [862] D McGrew, J Viega, "The Galois/Counter Mode of Operation (GCM)", Submission to NIST Modes of Operation Process, January 2004; updated May 2005
- [863] J McLean, "The Specification and Modeling of Computer Security", in *Computer* v 23 no 1 (Jan 1990) pp 9–16
- [864] J McLean, "Security Models," in *Encyclopedia of Software Engineering*, John Wiley & Sons (1994)
- [865] J McLean, "A General Theory of Composition for a Class of 'Possibilistic' Properties," in *IEEE Transactions on Software Engineering* v 22 no 1 (Jan 1996) pp 53–67

- [866] I McKie, "Total Vindication for Shirley McKie!" (23/6/2000), at <http://onin.com/fp/mckievindication.html>
- [867] I McKie, M Russell, *'Shirley McKie—The Price of Innocence'*, Birlinn, 2007; ISBN 1-84150-575-0
- [868] J McMillan, "Mobile Phones Help Secure Online Banking", in *PC World*, Sep 11 2007; at <http://www.pcworld.com/printable/article/id,137057/printable.html>
- [869] J McNamara, "The Complete, Unofficial TEMPEST Information Page", at <http://www.eskimo.com/~joelm/tempest.html>
- [870] B McWilliams, "Sex Sites Accused of Gouging Visitors with Phone Scam", in *InternetNews.com* (7/4/2000), at <http://www.internetnews.com/bus-news/print/0,,3337101,00.html>
- [871] J Meek, "Robo Cop", in *The Guardian*, June 13 2002, at <http://www.guardian.co.uk/Archive/Article/0,4273,4432506,00.html>
- [872] AJ Menezes, PC van Oorschot, SA Vanstone, *'Handbook of Applied cryptography'*, CRC Press (1997); ISBN 0-8493-8523-7; also available online at <http://www.cacr.math.uwaterloo.ca/hac/>
- [873] CG Menk, "System Security Engineering Capability Maturity Model and Evaluations: Partners within the Assurance Framework", in *19th National Information Systems Security Conference* (1996) pp 76–88
- [874] J Mercer, "Document Fraud Deterrent Strategies: Four Case Studies", in *Optical Security and Counterfeit Deterrence Techniques II* (1998), IS&T (The Society for Imaging Science and Technology) and SPIE (The International Society for Optical Engineering) v 3314 ISBN 0-8194-2754-3, pp 39–51
- [875] R Mercuri, "Physical Verifiability of Computer Systems", *5th International Computer Virus and Security Conference* (March 1992)
- [876] R Mercuri, *'Electronic Vote Tabulation Checks & Balances'*, PhD Thesis, U Penn, 2000; see <http://www.notablessoftware.com/evote.html>
- [877] TS Messergues, EA Dabish, RH Sloan, "Investigations of Power Analysis Attacks on Smartcards", in *Usenix Workshop on Smartcard Technology*, pp 151–161
- [878] E Messmer, "DOD looks to put pizzazz back in PKI", *Network World* Aug 15 2005; at <http://www.networkworld.com/news/2005/081505-pki.html?nl>

- [879] "Gamer may face jail for £1m racket", *Metro* Oct 25 2007, at http://www.metro.co.uk/news/article.html?in_article_id=72887&in_page_id=34; see also "Neil Higgs, aka Mr Modchips, 'guilty'", Oct 25 2007, at <http://www.p2pnet.net/story/13780>
- [880] CH Meyer and SM Matyas, *'Cryptography: A New Dimension in Computer Data Security'*, Wiley, 1982
- [881] R Meyer-Sommer, "Smartly analyzing the simplicity and the power of simple power analysis on Smartcards", in *Workshop on Cryptographic Hardware and Embedded Systems* (2000); Springer LNCS v 1965 pp 78–92
- [882] J Micklethwait, A Wooldridge, *'The Witch Doctors—What the management gurus are saying, why it matters and how to make sense of it'*, Random House (1997) ISBN 0-7493-2645-X
- [883] Microsoft Inc, *'Architecture of Windows Media Rights Manager'*, May 2004, at <http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx>
- [884] Microsoft Inc, "Sony DRM Rootkit", Nov 12 2005, at <http://blogs.technet.com/antimalware/archive/2005/11/12/414299.aspx>
- [885] Microsoft Inc, *'Understanding and Configuring User Account Control in Windows Vista'*, Dec 2007, at <http://technet2.microsoft.com/WindowsVista/en/library/00d04415-2b2f-422c-b70e-b18ff918c2811033.msp>
- [886] A Midgley, "R.I.P. and NHSNet", post to ukcrypto mailing list, 1/7/2000, archived at <http://www.cs.ucl.ac.uk/staff/I.Brown/archives/ukcrypto/>
- [887] S Mihm, *'A Nation of Counterfeiters'*, Harvard 2007
- [888] S Milgram, *'Obedience to Authority: An Experimental View'*, HarperCollins, (1974, reprinted 2004)
- [889] J Millen, "A Resource Allocation Model for Denial of Service Protection", in *Journal of Computer Security* v 2 no 2–3 (1993) pp 89–106
- [890] B Miller, "Vital Signs of Security", in *IEEE Spectrum* (Feb 94) pp 22–30
- [891] GA Miller, "The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information", in *Psychological Review* v 63 (1956) pp 81–97
- [892] ML Miller, IJ Cox, JA Bloom, "Watermarking in the Real World: An Application to DVD" in *Sixth ACM International Multimedia Conference*

- (1998); Workshop notes published by GMD–Forschungszentrum Informationstechnik GmbH. as v 41 of *GMD Report*, pp 71–76
- [893] JR Minkel, “Confirmed: The U.S. Census Bureau Gave Up Names of Japanese-Americans in WW II”, in *Scientific American* Mar 30 2007, at <http://www.sciam.com/article.cfm?articleID=A4F4DED6-E7F2-99DF-32E46B0AC1FDE0FE&sc=I100322>
- [894] SF Mires, “Production, Distribution, and Use of Postal Security Devices and Information-Based Indicia”, *Federal Register* v 65 no 191 Oct 2, 2000 pp 58682–58698; at http://www.cs.berkeley.edu/~tygar/papers/IBIP/Production_PSD.pdf
- [895] KD Mitnick, Congressional testimony, as reported by AP (03/02/00); see also <http://www.zdnet.com/zdnn/stories/news/0,4586,2454737,00.html> and <http://news.cnet.com/category/0-1005-200-1562611.html>
- [896] KD Mitnick, *The Art of Deception: Controlling the Human Element of Security*, John Wiley and Sons (2002)
- [897] Mobile Payment Forum, ‘Risks and Threats Analysis and Security Best Practices–Mobile 2-Way Messaging Systems’ (Dec 2002), at <http://www.mobilepaymentforum.org/documents/Risk.and.Threats.Analysis.and.Security.Best.Practices.Mobile.2.Way.Messaging.December.2002.pdf>
- [898] B Moghaddam, A Pentland, “Probabilistic Visual Learning for Object Representation”, in *IEEE Transactions on Pattern Analysis and Machine Intelligence* v 19 no 7 (July 97) pp 696–710
- [899] U Möller, L Cottrell, P Palfrader, L Sassaman, “Mixmaster Protocol–Version 2”, IETF draft (2003) at <http://www.abditum.com/mix-master-spec.txt>
- [900] “Card fraud nets Esc6 billion’, F Mollet, *Cards International* (22/9/95) p 3
- [901] E Montegrosso, “Charging and Accounting Mechanisms” (3G TR 22.924 v 3.1.1), from *Third Generation Partnership Project*, at http://www.3gpp.org/TSG/Oct_status_list.htm
- [902] J Moore, “Hacking Friendster, Part 1”, Feb 5 2004, at <http://more.theory.org/archives/000106.html>; “Hacking Social Networks Part 2: Don’t Search Private Data”, Feb 10 2004 at <http://more.theory.org/archives/000110.html>

- [903] SW Moore, RJ Anderson, R Mullins, G Taylor, J Fournier, "Balanced Self-Checking Asynchronous Logic for Smart Card Applications", in *Microprocessors and Microsystems Journal* v 27 no 9 (Oct 2003) pp 421–430
- [904] R Morris, "A Weakness in the 4.2BSD Unix TCP/IP Software", Bell Labs Computer Science Technical Report no 117, February 25, 1985; at <http://www.cs.berkeley.edu/~daw/security/seq-attack.html>
- [905] R Morris, Invited talk, *Crypto 95*
- [906] R Morris, K Thompson, "Password security: A case history", in *Communications of the ACM* v 22 no 11 (November 1979) pp 594–597
- [907] DP Moynihan, '*Secrecy—The American Experience*', Yale University Press (1999) ISBN 0-300-08079-4
- [908] C Mueller, S Spray, J Grear, "The Unique Signal Concept for Detonation Safety in Nuclear Weapons", Sand91-1269, UC-706. Available via National Technical Information Service
- [909] J Mueller, *Overblown—How Politicians and the Terrorism Industry Inflate National Security Threats, and Why we Believe Them*, Simon and Schuster 2006
- [910] P Mukherjee, V Stavridou, "The Formal Specification of Safety Requirements for Storing Explosives", in *Formal Aspects of Computing* v 5 no 4 (1993) pp 299–336
- [911] T Mulhall, "Where Have All The Hackers Gone? A Study in Motivation, Deterrence and Crime Displacement", in *Computers and Security* v 16 no 4 (1997) pp 277–315
- [912] S Mullender (ed), '*Distributed Systems*', Addison-Wesley (1993); ISBN 0-201-62427-3
- [913] SJ Murdoch, "Browser storage of passwords: a risk or opportunity?", Apr 18 2006 in *Light Blue Touchpaper*; at <http://www.lightbluetouchpaper.org/2006/04/18/browser-storage-of-passwords-a-risk-or-opportunity/>
- [914] SJ Murdoch, "Hot or Not: Revealing Hidden Services by their Clock Skew", in *13th ACM Conference on Computer and Communications Security*. 2006
- [915] SJ Murdoch, "Chip & PIN relay attacks", at <http://www.lightbluetouchpaper.org/2007/02/06/chip-pin-relay-attacks/>

- [916] SJ Murdoch, *'Covert channel vulnerabilities in anonymity systems'*, PhD Thesis, Cambridge 2007
- [917] SJ Murdoch, "Embassy email accounts breached by unencrypted passwords", Sep 10 2007; at <http://www.lightbluetouchpaper.org/2007/09/10/>
- [918] SJ Murdoch, RJ Anderson, "Shifting Borders", in *Index on censorship* Dec 18 2007; at <http://www.cl.cam.ac.uk/~sjm217/papers/index07-borders.pdf>
- [919] SJ Murdoch, G Danezis, "Low-Cost Traffic Analysis of Tor", in *IEEE Symposium on Security and Privacy* (2005), at <http://www.cl.cam.ac.uk/users/sjm217/papers/oakland05torta.pdf>
- [920] SJ Murdoch, Piotr Zieliński, "Sampled Traffic Analysis by Internet-Exchange-Level Adversaries", at PET 2007; at <http://www.cl.cam.ac.uk/~sjm217/>
- [921] JC Murphy, D Dubbel, R Benson, "Technology Approaches to Currency Security", in *Optical Security and Counterfeit Deterrence Techniques II* (1998), IS&T (The Society for Imaging Science and Technology) and SPIE (The International Society for Optical Engineering) v 3314 ISBN 0-8194-2754-3, pp 21–28
- [922] K Murray, "Protection of computer programs in Ireland", in *Computer Law and Security Report* v 12 no 3 (May/June 96) pp 57–59
- [923] Major General RFH Nalder, *'History of the Royal Corps of Signals'*, published by the Royal Signals Institution (1958)
- [924] Shishir Nagaraja and Ross Anderson, "The Topology of Covert Conflict", *Fifth Workshop on the Economics of Information Security* (2006)
- [925] E Nakashima, "Verizon Says It Turned Over Data Without Court Orders", in *The Washington Post* Oct 16 2007 p A01; at <http://www.washingtonpost.com/wp-dyn/content/article/2007/10/15/AR2007101501857.html>
- [926] E Nakashima, "A Story of Surveillance—Former Technician 'Turning In' AT&T Over NSA Program", in *The Washington Post* Nov 7 2007 p D01; at <http://www.washingtonpost.com/wp-dyn/content/article/2007/11/07/AR2007110700006.html>
- [927] E Nakashima, "FBI Prepares Vast Database Of Biometrics—\$1 Billion Project to Include Images of Irises and Faces", in *The Washington Post*

- Dec 22 2007, p A01; at <http://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544.html>
- [928] A Narayanan, V Shmatikov, "How To Break Anonymity of the Netflix Prize Dataset" (Nov 2007) at <http://arxiv.org/abs/cs/0610105>
- [929] M Nash, "MS Security VP Mike Nash Replies", on *Slashdot* Jan 26 2006, at <http://interviews.slashdot.org/interviews/06/01/26/131246.shtml>
- [930] National Audit Office, 'Minister of Defence: Combat Identification', 2002; at www.nao.gov.uk/publications/nao_reports/01-02/0102661.pdf
- [931] Wikipedia, *Napster*, <http://en.wikipedia.org/wiki/Napster>
- [932] M Nash, R Kennett, "Implementing Security policy in a Large Defence Procurement" in *12th Annual Computer Security Applications Conference*, San Diego CA, December 9–13 1996; proceedings published by the IEEE, ISBN 0-8186-7606-X; pp 15–23
- [933] National Information Infrastructure Task Force, 'Options for Promoting Privacy on the National Information Infrastructure' (April 1997), at <http://www.iitf.nist.gov/ipc/privacy.htm>
- [934] National Institute of Standards and Technology, archive of publications on computer security, <http://csrc.nist.gov/publications/history/index.html>
- [935] National Institute of Standards and Technology, 'Common Criteria for Information Technology Security Evaluation', Version 2.0 / ISO IS 15408 (May 1998); Version 3.1 (Sep 2006–Sep 2007), at <http://www.commoncriteriaportal.org>
- [936] National Institute of Standards and Technology, 'Data Encryption Standard (DES)' FIPS 46-3, Nov 1999 incorporating upgrade to triple DES, at <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>
- [937] National Institute of Standards and Technology, 'Escrowed Encryption Standard', FIPS 185, Feb 1994
- [938] National Institute of Standards and Technology, 'Security Requirements for Cryptographic Modules' (11/1/1994), at <http://www.itl.nist.gov/fipspubs/0-toc.htm#cs>
- [939] National Institute of Standards and Technology, 'SKIPJACK and KEA Algorithms', 23/6/98, <http://csrc.nist.gov/encryption/skipjack-kea.htm>

- [940] National Institute of Standards and Technology, '*Advanced Encryption Standard*', FIPS 197, Nov 26, 2001
- [941] National Institute of Standards and Technology, '*Digital Signature Standard (DSS)*', FIPS 186-2, Jan 2000, with change notice Oct 2001
- [942] National Institute of Standards and Technology, '*Digital Signature Standard (DSS)*', FIPS 186-3, draft, Mar 2006
- [943] National Institute of Standards and Technology, '*PBX Vulnerability Analysis—Finding Holes in Your PBX Before Somebody Else Does*', Special Publication 800-24, at <http://csrc.nist.gov/publications/PubsSPs.html>
- [944] National Institute of Standards and Technology, '*Recommendation for Block Cipher Modes of Operation*', Special Publication 800-38A 2001 Edition, at <http://csrc.nist.gov/CryptoToolkit/modes/>
- [945] National Institute of Standards and Technology, '*Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*', Special Publication 800-38B, May 2005
- [946] National Institute of Standards and Technology, '*Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*', Special Publication 800-38C, May 2004
- [947] National Institute of Standards and Technology, '*Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*' NIST Special Publication 800-38D, November 2007
- [948] National Institute of Standards and Technology, '*Recommendation for Key Management—Part 1: General (Revised)*', Special Publication 800-57, May 2006
- [949] National Institute of Standards and Technology, '*Announcing request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family*', in *Federal Register* v 72 no 212, Nov 2 2007, pp 62212–20
- [950] National Research Council, '*Cryptography's Role in Securing the Information Society*', National Academy Press (1996) ISBN 0-309-05475-3
- [951] National Research Council, '*For the Record: Protecting Electronic Health Information*', National Academy Press (1997) ISBN 0-309-05697-7
- [952] National Security Agency, '*The NSA Security Manual*', at <http://www.cl.cam.ac.uk/ftp/users/rja14/nsaman.tex.gz>

- [953] National Statistics, "Protocol on Data Access and Confidentiality", at <http://www.statistics.gov.uk>
- [954] P Naur, B Randell, 'Software Engineering—Report on a Conference', NATO Scientific Affairs Division, Garmisch 1968
- [955] R Neame, "Managing Health Data Privacy and Security", in [43] pp 225–232
- [956] GC Necula, P Lee, "Safe, Untrusted Agents Using Proof-Carrying Code", in *Mobile Agents and Security*, ISBN 3-540-64792-9, pp 61–91
- [957] RM Needham, "Denial of Service: An Example", in *Communications of the ACM* v 37 no 11 (Nov 94) pp 42–46
- [958] RM Needham, "Naming", in [912], pp 318–127
- [959] RM Needham, "The Hardware Environment", in *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, p 236
- [960] RM Needham, MD Schroeder, "Using Encryption for Authentication in Large Networks of Computers", in *Communications of the ACM* v 21 no 12 (Dec 78) pp 993–999
- [961] A Neewitz, "Defenses lacking at social network sites", *Security Focus* Dec 31 2003, at <http://www.securityfocus.com/news/7739>
- [962] P Neumann, 'Computer Related Risks', Addison-Wesley (1995); ISBN 0-201-55805-X
- [963] P Neumann, *Principled Assuredly Trustworthy Composable Architectures*, CHATS Project final report (2004), at <http://www.csl.sri.com/users/neumann/>
- [964] New South Wales Supreme Court, "RTA v. Michell (New South Wales Supreme Court, 3/24/2006)", reported in <http://www.thenewspaper.com/news/10/1037.asp>
- [965] MEJ Newman, "The structure and function of complex networks", in *SIAM Review* v 45 no 2 (2003) pp 167–256
- [966] MEJ Newman, "Modularity and community structure in networks", in *Proc. Natl. Acad. Sci. USA* v 103 pp 8577–8582 (2006); at <http://arxiv.org/abs/physics/0602124>
- [967] Richard Newman, Sherman Gavette, Larry Yonge, RJ Anderson, "Protecting Domestic Power-line Communications", in *Symposium On Usable Privacy and Security* 2006 pp 122–132

- [968] O Newman, *Defensible Space: People and Design in the Violent City*, MacMillan 1972
- [969] J Newton, "Countering the counterfeiters", in *Cards International* (21/12/94) p 12
- [970] J Newton, *Organised Plastic Counterfeiting*, Her Majesty's Stationery Office (1996), ISBN 0-11-341128-6
- [971] N Nisan, T Roughgarden, E Tardos, VV Vazirani, *Algorithmic Mechanism Design*, CUP 2007
- [972] DA Norman, "Cautious Cars and Cantankerous Kitchens: How Machines Take Control", at <http://www.jnd.org/>; chapter 1 of *The Design of Future Things* (due 2008)
- [973] R Norton-Taylor "Titan Rain—how Chinese hackers targeted Whitehall", in *The Guardian*, Sep 5 2007 p 1; at <http://www.guardian.co.uk/technology/2007/sep/04/news.internet>
- [974] R v Ipswich Crown Court ex parte NTL Ltd, [2002] EWHC 1585 (Admin), at <http://www.cyber-rights.org/documents/ntlcase.htm>
- [975] R v Paul Matthew Stubbs, [2006] EWCA Crim 2312 (12 October 2006), at <http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWCA/Crim/2006/2312.html>
- [976] Nuclear Regulatory Commission, www.nrc.gov
- [977] H Nugent, "Adulterers who call 118 118 for an affair", in *The Times*, May 27 2006; at <http://www.timesonline.co.uk/article/0,,2-2198924.html>
- [978] F Oberholzer, K Strumpf, "The Effect of File Sharing on Record Sales—An Empirical Analysis", June 2004; journal version F Oberholzer-Gee, K Strumpf, "The Effect of File Sharing on Record Sales: An Empirical Analysis", *Journal of Political Economy* v 115 (2007) pp 1–42
- [979] AM Odlyzko, *The history of communications and its implications for the Internet*, at <http://www.dtc.umn.edu/~odlyzko/doc/networks.html>
- [980] AM Odlyzko, "Smart and stupid networks: Why the Internet is like Microsoft", *ACM netWorker*, Dec 1998, pp 38–46, at <http://www.acm.org/networker/issue/9805/ssnet.html>
- [981] AM Odlyzko, "Privacy, economics, and price discrimination on the Internet", in *ICEC '03: Proceedings of the 5th international conference on*

- electronic commerce*, pp 355–366; at <http://www.dtc.umn.edu/~odlyzko/doc/networks.html>
- [982] AM Odlyzko, “Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation”, *TPRC 2004*, at <http://www.dtc.umn.edu/~odlyzko/doc/networks.html>
- [983] N Okuntsev, *Windows NT Security*, R&D Books (1999); ISBN 0-87930-473-1
- [984] Open Net Initiative, *Internet Filtering in China in 2004-2005: A Country Study*, April 14, 2005, at www.opennetinitiative.net
- [985] Open Net Initiative, *China (including Hong Kong)*, Country report 2006, at www.opennetinitiative.net
- [986] Open Net Initiative, *Pulling the Plug*, Oct 2007, at www.opennetinitiative.net
- [987] Open Rights Group, *May 2007 Election Report—Findings of the Open Rights Group Election Observation Mission in Scotland and England*, at <http://www.openrightsgroup.org/e-voting-main>
- [988] R Opplinger, *Internet and Intranet Security*, Artech House (1998) ISBN 0-89006-829-1
- [989] Oracle Inc., *Unbreakable: Oracle’s Commitment to Security*, Oracle White Paper, Feb 2002, at <http://www.oracle.com/technology/ deploy/security/pdf/unbreak3.pdf>
- [990] M Orozco, Y Asfaw, A Adler, S Shirmohammadi, A El Saddik, “Automatic Identification of Participants in Haptic Systems”, in *2005 IEEE Instrumentation and Measurement Technology Conference*, Ottawa, pp 888–892, at <http://www.sce.carleton.ca/faculty/adler/publications/publications.html>
- [991] Organization for Economic Cooperation and Development, *Guidelines for the Protections of Privacy and Transborder Flow of Personal Data*, OECD Doc no C(80)58 (1981), at <http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM>
- [992] J Osen, “The Cream of Other Men’s Wit: Plagiarism and Misappropriation in Cyberspace”, in *Computer Fraud and Security Bulletin* (11/97) pp 13–19
- [993] M Ossman, “WEP: Dead Again”, in *Security Focus: Part 1*, Dec 14 2004, at <http://www.securityfocus.com/infocus/1814>, and part 2, Mar 8 2005, at <http://www.securityfocus.com/infocus/1824>

- [994] DA Osvik, A Shamir, E Tromer, "Cache attacks and countermeasures: the case of AES," in *RSA Conference Cryptographers Track 2006*, LNCS 3860, pp 1–20
- [995] *Out-law News*, "SWIFT broke data protection law, says Working Party", Nov 27 2006, at <http://www.out-law.com/page-7518>
- [996] *Out-law News*, "SWIFT will stop some US processing in 2009", Oct 15 2007, at <http://www.out-law.com/page-8548>;
- [997] A Ozment, S Schechter, "Bootstrapping the Adoption of Internet Security Protocols", at *Fifth Workshop on the Economics of Information Security Security*, 2006; at <http://www.cl.cam.ac.uk/~jo262/>
- [998] A Ozment, S Schechter, "Milk or Wine: Does Software Security Improve with Age?" in *15th Usenix Security Symposium* (2006)
- [999] D Page, 'Theoretical Use of Cache Memory as a Cryptanalytic Side-Channel', Technical Report CSTR-02-003, University of Bristol, June 2002
- [1000] L Page, "Thai insurgents move to keyless-entry bombs", in *The Register* Apr 27 2007, at http://www.theregister.co.uk/2007/04/27/ied_ew_carries_on
- [1001] G Pahl, W Beitz, *Konstruktionslehre*'; translated as 'Engineering Design: A Systematic Approach', Springer 1999
- [1002] S Pancho, "Paradigm shifts in protocol analysis", in *Proceedings of the 1999 New Security Paradigms Workshop*, ACM (2000), pp 70–79
- [1003] A Papadimoulis, "Wish-It-Was Two-Factor", Sep 20 2007, at <http://worsethanfailure.com/Articles/WishItWas-TwoFactor-.aspx>
- [1004] DJ Parker, "DVD Copy Protection: An Agreement At Last?—Protecting Intellectual Property Rights In The Age Of Technology", in *Tape/Disc Magazine* (Oct 96) http://www.kipinet.com/tdb/tdb_oct96/feat_protection.html
- [1005] DJ Parker, 'Fighting Computer crime—A New Framework for Protecting Information', Wiley (1998) ISBN 0-471-16378-3
- [1006] A Pasick, "FBI checks gambling in Second Life virtual world", *Reuters*, Apr 4 2007, at <http://www.reuters.com/article/technologyNews/idUSN0327865820070404?feedType=RSS>
- [1007] J Pastor, "CRYPTOPOST—A cryptographic application to mail processing", in *Journal of Cryptology* v 3 no 2 (Jan 1991) pp 137–146

- [1008] B Patterson, letter to *Communications of the ACM* v 43 no 4 (Apr 2000) pp 11–12
- [1009] R Paul, “Leaked Media Defender e-mails reveal secret government project”, *Ars Technica* Sep 16 2007, at <http://arstechnica.com/news.ars/post/20070916-leaked-media-defender-e-mails-reveal-secret-government-project.html>
- [1010] LC Paulson, “Inductive analysis of the Internet protocol TLS”, in *ACM Transactions on Computer and System Security* v 2 no 3 (1999) pp 332–351; also at <http://www.cl.cam.ac.uk/users/lcp/papers/protocols.html>
- [1011] V Paxson, “An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks”, in *Computer Communication Review* v 31 no 3, July 2001, at <http://www.icir.org/vern/>
- [1012] B Pease, A Pease, ‘*Why Men Don’t Listen and Women Can’t Read Maps: How We’re Different and What to Do about It*’, Broadway Books 2001
- [1013] TP Pedersen, “Electronic Payments of Small Amounts”, in *Security Protocols* (1996), Springer LNCS v 1189 pp 59–68
- [1014] J Pereira, “Breaking the Code: How Credit-Card Data Went Out Wireless Door”, in *The Wall Street Journal*, May 4 2007, p A1
- [1015] A Perrig, ‘*A Copyright Protection Environment for Digital Images*’, Diploma thesis, École Polytechnique Fédérale de Lausanne (1997)
- [1016] P Pesic, “The Clue to the Labyrinth: Francis Bacon and the Decryption of Nature”, in *Cryptologia* v XXIV no 3 (July 2000) pp 193–211
- [1017] M Peters, “MTN moves to prevent SIM card swap fraud”, *IOL*, Dec 30 2007, at http://www.iol.co.za/index.php?set_id=1&click_id=79&art_id=vn20071230080257431C811594&newslett=1&em=169205a1a20080102ah
- [1018] I Peterson, “From Counting to Writing”, MathLand Archives, <http://www.maa.org/mathland/mathland.2.24.html>
- [1019] FAP Petitcolas, RJ Anderson, MG Kuhn, “Attacks on Copyright Marking Systems”, in *Proceedings of the Second International Workshop on Information Hiding* (1998), Springer LNCS v 1525 pp 219–239
- [1020] FAP Petitcolas, RJ Anderson, MG Kuhn, “Information Hiding—A Survey”, in *Proceedings of the IEEE* v 87 no 7 (July 1999) pp 1062–1078

- [1021] H Petroski, *'To Engineer is Human'*, Barnes and Noble Books (1994)
ISBN 1-56619502-0
- [1022] A Pfitzmann, *Proceedings of the Third International Workshop on Information Hiding* (1999), Springer LNCS v 1768
- [1023] B Pfitzmann, "Information Hiding Terminology", in *Proceedings of the First International Workshop on Information Hiding* (1996), Springer LNCS v 1174 pp 347–350
- [1024] Z Phillips, "Security Theater", in *Government Executive* Aug 1, 2007, at <http://www.govexec.com/features/0807-01/0807-01s3.htm>
- [1025] GE Pickett, "How do you select the 'right' security feature(s) for your company's products?", in *Optical Security and Counterfeit Deterrence Techniques II* (1998), IS&T (The Society for Imaging Science and Technology) and SPIE (The International Society for Optical Engineering) v 3314, ISBN 0-8194-2754-3, pp 52–58
- [1026] RL Pickholtz, DL Schilling, LB Milstein, "Theory of Spread Spectrum Communications—A Tutorial", in *IEEE Transactions on Communications* v TC-30 no 5 (May 1982) pp 855–884
- [1027] RL Pickholtz, DB Newman, YQ Zhang, M Tatebayashi, "Security Analysis of the INTELSAT VI and VII Command Network", in *IEEE Proceedings on Selected Areas in Communications* v 11 no 5 (June 1993) pp 663–672
- [1028] L Pinault, *'Consulting Demons'*, Collins 2000
- [1029] RA Poisel, *'Modern Communications Jamming Principles and Techniques'*, Artech House 2003; ISBN 158053743X
- [1030] D Polak, "GSM mobile network in Switzerland reveals location of its users", in *Privacy Forum Digest* v 6 no 18 (31/12/1997), at <http://www.vortex.com/privacy/priv.06.18>
- [1031] *Politech* mailing list, at <http://www.politechbot.com/>
- [1032] B Pomeroy, S Wiseman, "Private Desktops and Shared Store", in *Computer Security Applications Conference*, Phoenix, Arizona, (1998); proceedings published by the IEEE, ISBN 0-8186-8789-4, pp190–200
- [1033] GJ Popek, RP Goldberg, "Formal Requirements for Virtualizable Third Generation Architectures", in *Communications of the ACM* v 17 no 7 (July 1974) pp 412–421

- [1034] B Poser, "The Provenzano Code", in *Language Log*, Apr 21, 2006; at <http://itre.cis.upenn.edu/~myl/language-log/archives/003049.html>
- [1035] Richard Posner, "An Economic Theory of Privacy", in *Regulation* (1978) pp 19–26
- [1036] Richard Posner, "Privacy, Secrecy and Reputation" in *Buffalo Law Review* v 28 no 1 (1979)
- [1037] K Poulsen, "ATM Reprogramming Caper Hits Pennsylvania", in *Wired*, July 12 2007, at <http://blog.wired.com/27bstroke6/2007/07/atm-reprogrammi.html>
- [1038] S Poulter, "Phone firm's whistleblower says his life has been made a misery", in *The Daily Mail* Jun 21 2007; at http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=463593&in_page_id=1770
- [1039] J Preece, H Sharp, Y Rogers, *Interaction design: beyond human-computer interaction*, Wiley (2002)
- [1040] B Preneel, PC van Oorschot, "MDx-MAC and Building Fast MACs from Hash Functions", in *Advances in Cryptology—Crypto 95*, Springer LNCS v 963 pp 1–14
- [1041] RS Pressman, *Software Engineering: A Practitioner's Approach*, McGraw-Hill (5th edition, 2000) ISBN 0-073-65578-3
- [1042] V Prevelakis, D Spinellis, "The Athens Affair", *IEEE Spectrum*, July 2007, at <http://www.spectrum.ieee.org/print/5280>
- [1043] G Price, *The Interaction Between Fault Tolerance and Security*, Technical Report no 214, Cambridge University Computer Laboratory
- [1044] WR Price, "Issues to Consider When Using Evaluated Products to Implement Secure Mission Systems", in *Proceedings of the 15th National Computer Security Conference*, National Institute of Standards and Technology (1992) pp 292–299
- [1045] H Pringle, "The Cradle of Cash", in *Discover* v 19 no 10 (Oct 1998); http://www.discover.com/oct_issue/cradle.html
- [1046] C Prins, "Biometric Technology Law", in *The Computer Law and Security Report* v 14 no 3 (May/Jun 98) pp 159–165
- [1047] Privacy Commissioner of Canada, "Inadequate security safeguards led to TJX breach, Commissioners say", Sep 25 2007, at <http://www.privcom.gc.ca/media/nr-c/2007/nr-c-070925.e.asp>

- [1048] The Privacy Exchange, <http://www.privacyexchange.org/>
- [1049] A Pruneda, "Windows Media Technologies: Using Windows Media Rights Manager to Protect and Distribute Digital Media", *MSDN Magazine*, Dec 2001, at <http://msdn.microsoft.com/msdnmag/issues/01/12/DRM/>
- [1050] *Public Lending Right (PLR)*, at <http://www.writers.org.uk/guild/Crafts/Books/PLRBody.html>
- [1051] Public Record Office, '*Functional Requirements for Electronic Record Management Systems*', November 1999, <http://www.pro.gov.uk/recordsmanagement/eros/invest/reference.pdf>
- [1052] RD Putnam, '*Bowling Alone: the Collapse and Revival of American Community*', Simon & Schuster, 2000
- [1053] T Pyszczynski, S Solomon, J Greenberg, '*In the Wake of 9/11—the Psychology of Terror*', American Psychological Association 2003
- [1054] JJ Quisquater, D Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards" in *International Conference on Research in Smart Cards*, Springer LNCS v 2140 pp 200–210
- [1055] Rain Forest Puppy, "Issue disclosure policy v1.1", at <http://www.wiretrip.net/rfp/policy.html>
- [1056] W Rankl, W Effing, '*Smartcard Handbook*', Wiley (1997), ISBN 0-471-96720-3; translated from the German '*Handbuch der Chpkarten*', Carl Hanser Verlag (1995), ISBN 3-446-17993-3
- [1057] ES Raymond, "The Case of the Quake Cheats", 27/12/1999, at <http://www.tuxedo.org/~esr/writings/quake-cheats.html>
- [1058] ES Raymond, '*The Cathedral and the Bazaar*', at <http://www.tuxedo.org/~esr/writings/cathedral-bazaar/>
- [1059] ES Raymond, '*The Magic Cauldron*', June 1999, at <http://www.tuxedo.org/~esr/writings/magic-cauldron/magic-cauldron.html>
- [1060] J Reason, '*Human Error*', Cambridge University Press 1990
- [1061] SM Redl, MK Weber, MW Oliphant, '*GSM and Personal Communications Handbook*', Artech House (1998) ISBN 0-89006-957-3
- [1062] MG Reed, PF Syverson, DM Goldschlag, "Anonymous Connections and Onion Routing", in *IEEE Journal on Special Areas in Communications* v 16 no 4 (May 98) pp 482–494

- [1063] T Reid, "China's cyber army is preparing to march on America, says Pentagon", in *The Times* Sep 7 2007; at http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2409865.ece
- [1064] "Mystery of Levy tax phone calls", C Reiss, *Evening Standard* July 5 2000 p 1; also at <http://www.thisislondon.com/>
- [1065] MK Reiter, "A Secure Group Membership Protocol", *IEEE Transactions on Software Engineering* v 22 no 1 (Jan 96) pp 31–42
- [1066] MK Reiter, MK Franklin, JB Lacy, RA Wright, "The Omega Key Management Service", *3rd ACM Conference on Computer and Communications Security* (1996) pp 38–47
- [1067] M Reiter, AD Rubin, "Anonymous web transactions with Crowds", in *Communications of the ACM* v 42 no 2 (Feb 99) pp 32–38
- [1068] J Reno, <http://www.cnn.com/2000/US/05/25/security.breaches.01/index.html>
- [1069] Reporters without Borders, *Handbook for Bloggers and Cyber-dissidents*, 2005, at http://www.rsf.org/rubrique.php3?id_rubrique=542
- [1070] E Rescorla, *SSL and TLS—Designing and Building Secure Systems*, Addison-Wesley 2000
- [1071] E Rescorla, "Is Finding Security Holes a Good Idea?", *Third Workshop on the Economics of Information Security* (2004)
- [1072] *Reuters*, "No Surveillance Tech for Tampa", in *Wired* Aug 21 2003, at <http://www.wired.com/politics/law/news/2003/08/60140>
- [1073] *Reuters*, "Nissan warns U.S. cellphones can disable car keys", May 24 2007, at <http://www.reuters.com/article/technologyNews/idUSN2424455020070524?feedType=RSS&rpc=22>
- [1074] D Richardson, *Techniques and Equipment of Electronic Warfare*, Salamander Books, ISBN 0-8601-265-8
- [1075] LW Ricketts, JE Bridges, J Miletta, *EMP Radiation and Protection Techniques*, Wiley 1975
- [1076] M Ridley, *The Red Queen: Sex and the Evolution of Human Nature*, Viking Books (1993); ISBN 0-1402-4548-0
- [1077] RL Rivest, A Shamir, "PayWord and MicroMint: Two Simple Micro-payment Schemes", in *Security Protocols* (1996), Springer LNCS v 1189 pp 69–87

- [1078] RL Rivest, A Shamir, L Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", in *Communications of the ACM* v 21 no 2 (Feb 1978) pp 120–126
- [1079] MB Robinson, "The Theoretical Development of 'CPTED': 25 years of Responses to C. Ray Jeffery", in *Advances in Criminological Theory* v 8; at <http://www.acs.appstate.edu/dept/ps-cj/vitacpted2.html>
- [1080] AR Roddy, JD Stosz, "Fingerprint Features — Statistical Analysis and System Performance Estimates", in *Proceedings of the IEEE* v 85 no 9 (Sep 97) pp 1390–1421
- [1081] R Rohozinski, M Mambetalieva, "Election Monitoring in Kyrgyzstan", 2005, *Open Net Initiative*, at <http://opennet.net/special/kg/>
- [1082] SJ Root, 'Beyond COSO—Internal Control to Enhance Corporate Governance', Wiley 1998
- [1083] N Rosasco, D Larochelle, "How and Why More Secure Technologies Succeed in Legacy Markets: Lessons from the Success of SSH", in *WEIS 2003*; at <http://www.cl.cam.ac.uk/~rja14/econsec.html>
- [1084] J Rosen, "A Watchful State", in *New York Times*, Oct 7 2001 p 38
- [1085] B Ross, C Jackson, N Miyake, D Boneh, JC Mitchell, "Stronger Password Authentication Using Browser Extensions", in *Proceedings of the 14th Usenix Security Symposium, 2005*; at <http://crypto.stanford.edu/PwdHash/>
- [1086] DE Ross, "Two Signatures", in *comp.risks* v 20.81: <http://catless.ncl.ac.uk/Risks/20.81.html>
- [1087] "Card fraud plummets in France", M Rowe, *Banking Technology* (May 94) p 10
- [1088] T Rowland, "Ringling up the wrong numbers", in *The Guardian* May 18 2006; at <http://www.guardian.co.uk/media/2006/may/18/newmedia.technology>
- [1089] The Royal Society, 'Strategy options for the UK's separated plutonium', Sep 27 2007, at <http://royalsociety.org/document.asp?latest=1&id=7080>
- [1090] WW Royce, "Managing the development of Large Software Systems: Concepts and Techniques", in *Proceedings IEEE WESCON* (1970) pp 1–9

- [1091] A Rubin, "Bugs in Anonymity Services", *BugTraq*, 13 Apr 1999; at <http://www.securityportal.com/list-archive/bugtraq/1999/Apr/0126.html>
- [1092] HH Rubinovitz, "Issues Associated with Porting Applications to the Compartmented Mode Workstation", in *ACM SIGSAC v 12 no 4* (Oct 94) pp 2–5
- [1093] RA Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag (1986) ISBN 0-387-16870-2
- [1094] RA Rueppel, "Criticism of ISO CD 11166 Banking: Key Management by Means of Asymmetric Algorithms", in *Proceedings of 3rd Symposium of State and Progress of Research in Cryptography*, Fondazione Ugo Bordoni, Rome 1993, pp 191–198
- [1095] R Ruffin, "Following the Flow of Funds" in *Security Management* (July 1994) pp 46–52
- [1096] J Rushby, B Randell, "A Distributed Secure System", in *IEEE Computer v 16 no 7* (July 83) pp 55–67
- [1097] B Russell, Answer to parliamentary question, *Hansard* 10 Jun 2003 column 762W, at <http://www.publications.parliament.uk/pa/cm200203/cmhansrd/vo030610/text/30610w13.htm>
- [1098] D Russell, GT Gangemi, *Computer Security Basics*, Chapter 10: TEMPEST, O'Reilly & Associates (1991), ISBN 0-937175-71-4
- [1099] J Rutkowska, "Running Vista Every Day!", *Invisible Things Blog*, Feb 2007; at <http://theinvisiblethings.blogspot.com/2007/02/running-vista-every-day.html>
- [1100] DR Safford, DL Schales, DK Hess, "The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment", in *Usenix Security 93*, pp 91–118
- [1101] *Salon*, "The computer virus turns 25", Jul 12 2007; at http://machinist.salon.com/blog/2007/07/12/virus_birthday/index.html
- [1102] JD Saltzer, MD Schroeder, "The Protection of Information in Computer Systems", in *Proceedings of the IEEE v 63 no 9* (Mar 1975) pp 1278–1308
- [1103] RG Saltzman, "Assuring Accuracy, Integrity and Security in National Elections: The Role of the U.S. Congress", in *Computers, Freedom and Privacy* (1993); at <http://www.cpsr.org/conferences/cfp93/saltman.html>

- [1104] J Saltzman, M Daniel, "Man freed in 1997 shooting of officer—Judge gives ruling after fingerprint revelation", in *The Boston Globe* Jan 24 2004, at <http://www.truthinjustice.org/cowans2.htm>
- [1105] T Sammes, B Jenkinson, *Forensic Computing—A Practitioner's Guide*, Springer (2000); ISBN 1-85233-299-9
- [1106] R Samuels, S Stich, L Faucher, "Reason and Rationality", in *Handbook of Epistemology* (Kluwer, 1999); at <http://ruccs.rutgers.edu/Archive-Folder/Research%20Group/Publications/Reason/ReasonRationality.htm>
- [1107] P Samuelson, "Copyright and digital libraries", in *Communications of the ACM* v 38 no 4, April 1995
- [1108] P Samuelson, "Intellectual Property Rights and the Global Information Economy", in *Communications of the ACM* v 39 no 1 (Jan 96) pp 23–28
- [1109] P Samuelson, "The Copyright Grab", at http://uainfo.arizona.edu/~weisband/411_511/copyright.html
- [1110] Pam Samuelson and Suzanne Scotchmer, "The Law and Economics of Reverse Engineering", *Yale Law Journal* (2002)
- [1111] D Samyde, SP Skorobogatov, RJ Anderson, JJ Quisquater, "On a New Way to Read Data from Memory", in *IEEE Security in Storage Workshop* (2002) pp 65–69
- [1112] RS Sandhu, S Jajodia, "Polyinstantiation for Cover Stories", in *Computer Security — ESORICS 92*, LNCS v 648 pp 307–328
- [1113] SANS Institute, "Consensus List of The Top Ten Internet Security Threats", at <http://www.sans.org/>, Version 1.22 June 19, 2000
- [1114] G Sandoval, "Glitches let Net shoppers get free goods", in *CNET News.com*, July 5 2000; at <http://news.cnet.com/news/0-1007-200-2208733.html>
- [1115] PF Sass, L Gorr, "Communications for the Digitized Battlefield of the 21st Century", in *IEEE Communications* v 33 no 10 (Oct 95) pp 86–95
- [1116] W Schachtman, "How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social—Not Electronic", in *Wired*, Dec 15 2007, at <http://www.wired.com/politics/security/magazine/15-12/ff-futurewar?currentPage=all>
- [1117] M Schaefer, "Symbol Security Condition Considered Harmful", in *Proceedings of the 1989 IEEE Symposium on Security and Privacy*, pp 20–46

- [1118] RR Schell, "Computer Security: The Achilles' Heel of the Electronic Air Force?", in *Air University Review*, v 30 no 2 (Jan–Feb 1979) pp 16–33
- [1119] RR Schell, PJ Downey, GJ Popek, 'Preliminary notes on the design of secure military computer systems', Electronic Systems Division, Air Force Systems Command (1/1/1973) MCI-73-1; at <http://seclab.cs.ucdavis.edu/projects/history/papers/sche73.pdf>
- [1120] DL Schilling, 'Meteor Burst Communications: Theory and Practice', Wiley (1993) ISBN 0-471-52212-0
- [1121] DC Schleher, 'Electronic Warfare in the Information Age', Artech House (1999) ISBN 0-89006-526-8
- [1122] D Schmandt-Besserat, 'How Writing Came About', University of Texas Press (1996): ISBN: 0-29277-704-3, <http://www.dla.utexas.edu/depts/lrc/numerals/dsb1.html>
- [1123] ZE Schnabel, "The estimation of the total fish population in a lake", in *American Mathematical Monthly* v 45 (1938) pp 348–352
- [1124] PM Schneider, "Datenbanken mit genetischen Merkmalen von Straftätern", in *Datenschutz und Datensicherheit* v 22 (6/1998) pp 330–333
- [1125] B Schneier, 'Applied Cryptography', Wiley (1996); ISBN 0-471-12845-7
- [1126] B Schneier, "Why Computers are Insecure", in *comp.risks* v 20.67: <http://catless.ncl.ac.uk/Risks/20.67.html>
- [1127] B Schneier, 'Secrets and Lies : Digital Security in a Networked World', Wiley (2000); ISBN 0-471-25311-1
- [1128] B Schneier, "Semantic Attacks: The Third Wave of Network Attacks", in *Crypto-Gram Newsletter* October 15, 2000 at <http://www.schneier.com/crypto-gram-0010.html>
- [1129] B Schneier, 'Beyond Fear: Thinking Sensibly about Security in an Uncertain World', Copernicus Books (2003)
- [1130] B Schneier, "Real-World Passwords", in *Crypto-Gram Newsletter* Dec 14, 2006; at http://www.schneier.com/blog/archives/2006/12/realworld_passw.html
- [1131] B Schneier, "Choosing Secure Passwords", Aug 7 2007; at http://www.schneier.com/blog/archives/2007/08/asking_for_pass.html
- [1132] B Schneier, "Secure Passwords Keep You Safer, in *Crypto-Gram Newsletter* Jan 11, 2007; at http://www.schneier.com/blog/archives/2007/01/choosing_secure.html

- [1133] B Schneier, "The Psychology of Security", *RSA Conference* (2007), at <http://www.schneier.com/essay-155.html>
- [1134] B Schneier, "The Nugache Worm/Botnet", Dec 31 2007, at http://www.schneier.com/blog/archives/2007/12/the_nugache_wor.html
- [1135] B Schneier, D Banisar, *The Electronic Privacy Papers—Documents on the Battle for Privacy in the Age of Surveillance*, Wiley (1997) ISBN 0-471-12297-1
- [1136] B Schneier, A Shostack, "Breaking up is Hard to Do: Modeling Security Threats for Smart Cards," in *USENIX Workshop on Smart Card Technology* 1999, pp 175–185, at <http://www.schneier.com/paper-smart-card-threats.html>
- [1137] M Schnyder, "Datenfluesse im Gesundheitswesen", in *Symposium für Datenschutz und Informationssicherheit*, Zuerich, Oct 98
- [1138] RA Scholtz, "Origins of Spread-Spectrum Communications", in *IEEE Transactions on Communications* v TC-30 no 5 (May 1982) pp 822–854
- [1139] MD Schroeder, 'Cooperation of Mutually Suspicious Subsystems in a Computer Utility', MIT PhD Thesis, September 1972, also available as Project MAC Technical Report MAC TR-104, available on the web as http://hdl.handle.net/ncstr1.mit_lcs/MIT/LCS/TR-104
- [1140] M Scorgie, "Untapped sources for accountants" in *Genizah Fragments* (The Newsletter of Cambridge University's Taylor-Schechter Genizah Research Unit) no 29 (April 1995), at <http://www.lib.cam.ac.uk/Taylor-Schechter/GF/GF29.html>
- [1141] Beale Screamer, "Microsoft DRM - Technical description" and supporting documents, on *Cryptome.org*, Oct 23 2001; at <http://cryptome.org/beale-sci-crypt.htm>
- [1142] W Seltzer, M Anderson, "Census Confidentiality under the Second War Powers Act (1942-1947)," Annual Meeting of the Population Association of America, Mar 30 2007, New York; at *Official Statistics and Statistical Confidentiality: Recent Writings and Essential Documents*, at <http://www.uwm.edu/%7Emargo/govstat/integrity.htm>
- [1143] R Senderek, 'Key-Experiments—How PGP Deals With Manipulated Keys', at <http://senderek.de/security/key-experiments.html>
- [1144] D Senie, "Changing the Default for Directed Broadcasts in Routers", RFC 2644, at <http://www.ietf.org/rfc/rfc2644.txt>
- [1145] Chandak Sengoopta, *Imprint of the Raj*, Pan Macmillan 2004

- [1146] A Shamir, "How to share a secret", in *Communications of the ACM* v 22 no 11 (Nov 1979) pp 612–613
- [1147] A Shamir, "Identity-based cryptosystems and signature schemes", in *Proceedings of Crypto 1984*, Springer LNCS v 196, pp 47–53
- [1148] A Shamir, "Research Announcement: Microprocessor Bugs Can Be Security Disasters", Nov 2007, at <http://cryptome.org/bug-attack.htm>
- [1149] MI Shamos, "Electronic Voting - Evaluating the Threat", in *Computers, Freedom and Privacy* (1993); at <http://www.cpsr.org/conferences/cfp93/shamos.html>
- [1150] MI Shamos, "Paper v. Electronic Voting Records—An Assessment", in *Computers, Freedom & Privacy* (Apr 2004), at <http://euro.econ.cmu.edu/people/faculty/mshamos/paper.htm>
- [1151] M Sherr, E Cronin, S Clark, M Blaze, "Signaling vulnerabilities in wiretapping systems", *IEEE Security and Privacy* v 3 no 6 (Nov/Dec 2005) pp 13–25
- [1152] O Sibert, PA Porras, R Lindell, "An Analysis of the Intel 80x86 Security Architecture and Implementations" in *IEEE Transactions on Software Engineering* v 22 no 5 (May 96) pp 283–293
- [1153] H Simon, *The Sciences of the Artificial*, 3rd ed, MIT Press, 1996
- [1154] Y Shachmurove, G Fishman, S Hakim, "The burglar as a rational economic agent," Technical Report CARESS Working Paper 97-07, U Penn University of Pennsylvania Center for Analytic Research in Economics and the Social Sciences, June 1997
- [1155] G Shah, A Molina, M Blaze, "Keyboards and Covert Channels", in *15th USENIX Security Symposium 2006*, at <http://www.crypto.com/papers/>
- [1156] Y Shaked, A Wool, "Cracking the Bluetooth PIN", 2005, at <http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/index.html>
- [1157] CE Shannon, "A Mathematical Theory of Communication", in *Bell Systems Technical Journal* v 27 (1948) pp 379–423, 623–656
- [1158] CE Shannon, "Communication theory of secrecy systems", in *Bell Systems Technical Journal* v 28 (1949) pp 656–715
- [1159] C Shapiro, H Varian, *Information Rules*, Harvard Business School Press (1998), ISBN 0-87584-863-X
- [1160] P Shekelle, SC Morton, EB Keeler, JK Wang, BI Chaudhry, SY Wu, WA Majica, M Maglione, EA Roth, C Rolon, D Valentine, R Shanman, SJ

- Newberry, *Costs and Benefits of Health Information Technology*, DHHS June 2006; at <http://aspe.hhs.gov/daltcp/reports/2006/HITcb.htm>
- [1161] M Sherr, E Cronin, S Clark, MA Blaze, "Signaling vulnerabilities in wiretapping systems", *IEEE Security and Privacy*, Nov/Dec 2005, at <http://www.cryptocom.com/papers/wiretapping/>
- [1162] D Sherwin, "Fraud—the Unmanaged Risk", in *Financial Crime Review* v 1 no 1 (Fall 2000) pp 67–69
- [1163] S Sheye, "SSL Client Certificates—Not Securing the Web", in *Cryptomathic NewsOnInk Quarterly Newsletter* (Nov 2006), at http://www.cryptomathic.com/Admin/Public/DWSDownload.aspx?File=%2fFiles%2fFiler%2fNewsletters%2fNewsOnInk_Nov_2006.pdf
- [1164] JF Shoch, JA Hupp, "The 'Worm' Programs—Early Experience with a Distributed Computation", *Comm ACM* v 25 no 3 (1982) pp 172–180
- [1165] PW Shor, "Algorithms for Quantum Computers", in *35th Annual Symposium on the Foundations of Computer Science* (1994), proceedings published by the IEEE, ISBN 0-8186-6580-7, pp 124–134
- [1166] A Shostack, P Syverson, "What Price Privacy? (and why identity theft is about neither identity nor theft)", in *Economics of Information Security*, Kluwer Academic Publishers, 2004, Chapter 11
- [1167] V Shoup, "OAEP Reconsidered", IBM Zürich, Switzerland, September 18, 2001; at <http://www.shoup.net/papers/oaep.pdf>
- [1168] *Luther Simjian—Inventor of the Week*, at <http://web.mit.edu/invent/iow/simjian.html>
- [1169] GJ Simmons, "The Prisoners' Problem and the Subliminal Channel", in *Proceedings of CRYPTO '83*, Plenum Press (1984) pp 51–67
- [1170] GJ Simmons, "How to Insure that Data Acquired to Verify Treaty Compliance are Trustworthy", GJ Simmons, *Proceedings of the IEEE* v 76 no 5 (1988; reprinted as a chapter in [1171])
- [1171] GJ Simmons (ed), *Contemporary Cryptology—The Science of Information Integrity*, IEEE Press (1992) ISBN 0-87942-277-7
- [1172] GJ Simmons, "A Survey of Information Authentication", in [1171] pp 379–439
- [1173] GJ Simmons, "An Introduction to Shared Secret and/or Shared Control Schemes and Their Application", in [1171] pp 441–497

- [1174] GJ Simmons, invited talk at the 1993 ACM Conference on Computer and Communications Security, Fairfax, Virginia, Nov 3–5, 1993
- [1175] GJ Simmons, ‘Subliminal Channels; Past and Present’, *European Transactions on Telecommunications* v 5 no 4 (Jul/Aug 94) pp 459–473
- [1176] GJ Simmons, “The History of Subliminal Channels”, in *IEEE Journal on Selected Areas in Communications* v 16 no 4 (April 1998) pp 452–462
- [1177] R Singel, “Encrypted E-Mail Company Hushmail Spills to Feds”, in *Wired* Nov 7 2007 at <http://blog.wired.com/27bstroke6/2007/11/encrypted-e-mai.html>
- [1178] R Singel, “Point, Click ... Eavesdrop: How the FBI Wiretap Net Operates”, in *Wired* Aug 29 2007 at <http://www.wired.com/politics/security/news/2007/08/wiretap>
- [1179] A Sipress, “Tracking Traffic by Cell Phone; Md., Va. to Use Transmissions to Pinpoint Congestion”, in *Washington Post* (22/12/1999) p A01, at <http://www.washingtonpost.com/>
- [1180] KS Siyan, J Casad, J Millecan, D Yarashus, P Tso, J Shoults, ‘*Windows NT Server 4–Professional Reference*’, New Riders Publishing (1996)
- [1181] SP Skorobogatov, “Copy Protection in Modern Microcontrollers”, at http://www.cl.cam.ac.uk/~sps32/mcu_lock.html
- [1182] SP Skorobogatov, ‘*Low temperature data remanence in static RAM*’, Cambridge University Technical Report UCAM-CL-TR-536 (June 2002), at <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-536.html>
- [1183] SP Skorobogatov, ‘*Semi-invasive attacks–A new approach to hardware security analysis*’, PhD Thesis, 2004; University of Cambridge Technical Report 630, 2005; at <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.html>
- [1184] SP Skorobogatov, “Data Remanence in Flash Memory Devices”, in *Cryptographic Hardware and Embedded Systems Workshop (CHES-2005)*, Springer LNCS 3659 pp 339–353
- [1185] SP Skorobogatov, “Optically Enhanced Position-Locked Power Analysis”, in *CHES 2006* pp 61–75
- [1186] SP Skorobogatov, “Tamper resistance and physical attacks”, at *Summer School on Cryptographic Hardware, Side-Channel and Fault Attacks*, June 12–15, 2006, Louvain-la-Neuve, Belgium; slides at <http://www.cl.cam.ac.uk/~sps32>

- [1187] SP Skorobogatov, RJ Anderson, "Optical Fault Induction Attacks", in *Cryptographic Hardware and Embedded Systems Workshop (CHES 2002)*, Springer LNCS v 2523 pp 2–12; at <http://www.cl.cam.ac.uk/~sps32>
- [1188] B Skyrms, *'Evolution of the Social Contract'* Cambridge University Press (1996)
- [1189] P Slovic, ML Finucane, E Peters, DG MacGregor, "Rational Actors or Rational Fools? Implications of the Affect Heuristic for Behavioral Economics", at <http://www.decisionresearch.org/pdf/dr498v2.pdf>; revised version of "The Affect Heuristic" in *Heuristics and Biases: The Psychology of Intuitive Judgment*, Cambridge University Press (2002) pp 397–420
- [1190] Smartcard Standards, http://www.cardwerk.com/smartcards/smartcard_standards.aspx
- [1191] "Plastic Card Fraud Rises in the UK", in *Smart Card News* v 6 no 3 (Mar 97) p 45
- [1192] A Smith, *'An Inquiry into the Nature and Causes of the Wealth of Nations'*, 1776; at <http://www.econlib.org/LIBRARY/Smith/smWN.html>
- [1193] RE Smith, "Constructing a high assurance mail guard", in *Seventeenth National Computer Security Conference*, 11–14 October, Baltimore, Maryland; proceedings published by NIST (1994) pp 247–253
- [1194] RM Smith, "Problems with Web Anonymizing Services" (15/4/1999), at <http://www.tiac.net/users/smiths/anon/anonprob.htm>
- [1195] S Smith, S Weingart, *'Building a High-Performance, Programmable Secure Coprocessor'*, IBM Technical report RC 21102, available through <http://www.ibm.com/security/cryptocards/>
- [1196] P Smulders, "The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables", in *Computers & Security* v 9 (1990) pp 53–58
- [1197] C Soghoian, "Go Fish: Is Facebook Violating European Data Protection Rules?", on *Slight Paranoia* June 26 2007, at <http://paranoia.dubfire.net/2007/06/go-fish-is-facebook-violating-european.html>
- [1198] A Solomon, "A brief history of PC viruses", in *Computer Fraud and Security Bulletin* (Dec 93) pp 9–19
- [1199] A Solomon, Seminar given at Cambridge University Computer Laboratory, 30th May 2000

- [1200] D Solove, "A Taxonomy of Privacy", in *University of Pennsylvania Law Review* v 154 no 3 (2006) pp 477–560; at http://papers.ssrn.com/abstract_id=667622
- [1201] D Solove, *The future of reputation—gossip, rumor and privacy in the Internet*, Caravan, 2007
- [1202] P Sommer, "Intrusion Detection and Legal Proceedings", at *Recent Advances in Intrusion Detection (RAID) 1998*, at http://www.zurich.ibm.com/~dac/Prog_RAID98/Full_Papers/Sommer_text.pdf
- [1203] DX Song, D Wagner, XQ Tian, "Timing analysis of keystrokes and SSH timing attacks," in *Proceedings of 10th USENIX Security Symposium* (2001)
- [1204] R v Department of Health, ex parte Source Informatics: [2000] 2 WLR 940
- [1205] South West Thames Regional Health Authority, *'Report of the Inquiry into the London Ambulance Service'* (1993), at <http://www.cs.ucl.ac.uk/staff/A.Finkelstein/las.html>
- [1206] E Spafford, "The Internet worm program: an analysis", in *Computer Communications Review* v 19 no 1 (Jan 89) pp 17–57
- [1207] EH Spafford, "OPUS: Preventing Weak Password Choices", in *Computers and Security* v 11 no 3 (1992) pp 273–278
- [1208] M Specter, "Do fingerprints lie? The gold standard of forensic evidence is now being challenged", *New York Times*, May 27, 2002; at http://www.michaelspecter.com/ny/2002/2002_05_27_fingerprint.html
- [1209] R Spencer, S Smalley, P Loscocco, M Hibler, D Andersen, J Lepreau, "The Flask Security Architecture: System Support for Diverse Security Policies," in *Proceedings of the 8th USENIX Security Symposium* (1999) pp 123–139
- [1210] "Tip von Urmel", in *Spiegel Magazine* no 38 (11/9/95)
- [1211] J Spolsky, "Does Issuing Passports Make Microsoft a Country?" at [http://joel.edittthispage.com/stories/storyReader\\$139](http://joel.edittthispage.com/stories/storyReader$139)
- [1212] "Your car radio may be revealing your tastes", in *St Petersburg Times* (31/1/2000), at http://www.sptimes.com/News/013100/Technology/Your_car_radio_may_be.shtml
- [1213] S Stamm, Z Ramzan, M Jakobsson, "Drive-By Pharming", Indiana University Department of Computer Science Technical Report TR641, 2006

- [1214] M Stamp, RM Low, *'Applied Cryptanalysis'*, Wiley 2007
- [1215] T Standage, *'The Victorian Internet'*, Phoenix Press (1999), ISBN 0-75380-703-3
- [1216] D Standeford, "Case Could Signal Weakening Of Digital Rights Management in Europe", in *Intellectual Property Watch*, June 4 2007, at http://www.ip-watch.org/weblog/index.php?p=639&res=1600_ff&print=0
- [1217] F Stajano, personal communication
- [1218] F Stajano, RJ Anderson, "The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks", in *'Security Protocols-7th International Workshop'*, Springer LNCS 1796 pp 172-182
- [1219] F Stajano, RJ Anderson, "The Cocaine Auction Protocol-On the Power of Anonymous Broadcast", in [1022] pp 434-447
- [1220] S Staniford, D Moore, V Paxson, N Weaver, "The Top Speed of Flash Worms", in *WORM04*, at www.icir.org/vern/papers/topspeed-worm04.pdf
- [1221] "Computer Chip Usage in Toner Cartridges and Impact on the Aftermarket: Past, Current and Future", Static Control, Inc., formerly at <http://www.scc-inc.com/special/oemwarfare/whitepaper/default.htm>, retrieved via www.archive.org
- [1222] WA Steer, "VideoDeCrypt", at <http://www.ucl.ac.uk/~ucapwas/vdc/>
- [1223] P Stein, P Feaver, "Assuring Control of Nuclear Weapons", CSIA occasional paper number 2, Harvard University 1987
- [1224] J Steiner, BC Neuman, JI Schiller, "Kerberos: An Authentication Service for Open Network Systems", in *USENIX* (Winter 1988); version 5 in *'RFC 1510: The Kerberos Network Authentication Service (V5)'*; at <http://sunsite.utk.edu/net/security/kerberos/>
- [1225] N Stephenson, *'Snow Crash'*, Bantam Doubleday Dell (1992), ISBN 0-553-38095-8
- [1226] DR Stinson, *'Cryptography-Theory and Practice'*, CRC Press (1995); ISBN 0-8493-8521-0
- [1227] *'Watching Them, Watching Us - UK CCTV Surveillance Regulation Campaign'*, at <http://www.spy.org.uk/>
- [1228] R Strehle, *'Verschlüsselt-Der Fall Hans Bühler'*, Werd Verlag (1994) ISBN 3-85932-141-2

- [1229] R Stross, "How to Lose Your Job on Your Own Time", in *New York Times* Dec 30 2007; at <http://www.nytimes.com/2007/12/30/business/30digi.html?ex=1356670800&en=bafd771bdcae2594&ei=5124&partner=permalink&exprod=permalink>
- [1230] A Stubblefield, J Ioannidis, A Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", in *ISOC 2002*
- [1231] K Stumper, "DNA-Analysen und ein Recht auf Nichtwissen", in *Datenschutz und Datensicherheit* v 19 no 9 (Sep 95) pp 511–517
- [1232] Suetonius (Gaius Suetonius Tranquillus), '*Vitae XII Caesarum*', translated into English as '*History of twelve Caesars*' by Philemon Holland, 1606; Nutt (1899)
- [1233] D Sutherland, "A Model of Information", in *9th National Computer Security Conference* (1986)
- [1234] M Sutton, "How Prevalent Are SQL Injection Vulnerabilities?" *Michael Sutton's Blog*, Sep 26 2006, at <http://portal.spidynamics.com/blogs/msutton/archive/2006/09/26/How-Prevalent-Are-SQL-Injection-Vulnerabilities.3F00.aspx>
- [1235] L Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality", in *Journal of Law, Medicine and Ethics* v 25 no 2–3 (1997) pp 98–110
- [1236] F Swiderski, W Snyder, '*Threat Modeling*', Microsoft Press 2004
- [1237] P Swire, "Efficient Confidentiality for Privacy, Security, and Confidential Business Information", *Brookings-Wharton Papers on Financial Services* (2003), at <http://ssrn.com/abstract=383180>
- [1238] P Swire, "A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Agencies", in *Houston Law Review* v 42 no 5 (Jan 2006) pp 101–148; at http://ssrn.com/abstract_id=842228
- [1239] Symantec, '*Symantec Internet Security Threat Report—Trends for January–June 07*' v 12, Sep 2007, at www.symantec.com/threatreport/
- [1240] *Symposium On Usable Privacy and Security*, <http://cups.cs.cmu.edu/soups/2007/>
- [1241] C Tavris, E Aronson, '*Mistakes were made—but not by me*', Harcourt 2007
- [1242] J Taylor, MR Johnson, CG Crawford, '*DVD Demystified*', Third edition, McGraw-Hill 2006

- [1243] J Tehranian, "An Unhurried View of Copyright Reform: Bridging the Law/Norm Gap", 2007 *Utah Law Review*, at www.turnergreen.com/publications/Tehranian.Infringement.Nation.pdf
- [1244] S Tendler, N Nuttall, "Hackers run up £1m bill on Yard's phones", in *The Times*, 5 Aug 1996; at <http://www.the-times.co.uk/>
- [1245] E Tews, RP Weinmann, A Pyshkin, "Breaking 104 bit WEP in less than 60 seconds", *Cryptology ePrint archive*, Apr 2007; at <http://eprint.iacr.org/2007/120.pdf>
- [1246] L Thalheim, J Krissler, PM Ziegler, "Body Check—Biometric Access Protection Devices and their Programs Put to the Test", *c't magazine*, Nov 2002 p 114, at <http://www.heise.de/ct/english/02/11/114/>
- [1247] K Thompson, "Reflections on Trusting Trust", in *Communications of the ACM* v 27 no 8 (Aug 84) pp 761–763; at <http://www.acm.org/classics/sep95/>
- [1248] R Thompson, "Google Sponsored Links Not Safe", Exploit Prevention Labs Apr 24 2007, at <http://explabs.blogspot.com/2007/04/google-sponsored-links-not-safe.html>; see also J Richards, "Hackers hijack Google AdWords", *The Times*, Apr 27 2007, http://technology.timesonline.co.uk/tol/news/tech_and_web/article1714656.ece
- [1249] J Ticehurst, "Barclays online bank suffers another blow" (11/8/2000), at <http://www.vnunet.com/News/1108767>
- [1250] TimeWarner, "Carmine Caridi, Motion Picture Academy Member Who Handed Over His Awards Screeners for Illegal Duplication, Ordered to Pay \$300,000 to Warner Bros. Entertainment Inc.", Nov 23 2004, at <http://www.timewarner.com/corp/newsroom/pr/0,20812,832500,00.html>
- [1251] AZ Tirkel, GA Rankin, RM van Schyndel, WJ Ho, NRA Mee, CF Osborne, "Electronic Watermark", in *Digital Image Computing, Technology and Applications* (DICTA 93) McQuarie University (1993) pp 666–673
- [1252] The TJX Companies, Inc., 'Form 10-k', filed with SEC, at <http://www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm>
- [1253] MW Tobias, *Locks, Safes and Security—An International Police Reference* (second edition, 2000) ISBN 978-0-398-07079-3
- [1254] MW Tobias, "Opening locks by bumping in five seconds or less: is it really a threat to physical security?", 2006, at www.security.org

- [1255] MW Tobias, "Bumping of locks—legal issues in the United States", at www.security.org
- [1256] MW Tobias, "The Medeco M3 Meets the Paper Clip: Is the security of this lock at risk?" (2007), at www.security.org
- [1257] C Tomlinson, 'Rudimentary Treatise on the Construction of Locks', 1853 (excerpt), at http://www.deter.com/unix/papers/treatise_locks.html
- [1258] TT Tool, 'The MIT Lock Picking Manual', 1991; at <http://people.csail.mit.edu/custo/MITLockGuide.pdf>
- [1259] Transactional Records Access Clearinghouse, 'TRACFBI', at <http://trac.syr.edu/tracfbi/index.html>
- [1260] A Travis, "Voice ID device to track failed asylum seekers", in *The Guardian* Mar 10 2006; at http://www.guardian.co.uk/uk_news/story/0,,1727834,00.html
- [1261] I Traynor, "DNA database agreed for police across EU", in *The Guardian*, June 13 2007; at <http://www.guardian.co.uk/international/story/0,,2101496,00.html>
- [1262] M Trombly, "Visa issues 10 'commandments' for online merchants", in *Computerworld* (11/8/2000), at http://www.computerworld.com/cwi/story/0,1199,NAV47_STO48487,00.html
- [1263] E Tromer, 'Hardware-Based Cryptanalysis', PhD Thesis, Weizmann Institute of Science (2007), at <http://www.wisdom.weizmann.ac.il/~tromer/papers/tromer-phd-dissertation.pdf>
- [1264] C Troncoso, G Danezis, E Kosta, B Preneel, "PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance", in *Workshop on Privacy in the Electronic Society* (2007), at <https://www.cosic.esat.kuleuven.be/publications/article-944.pdf>
- [1265] JD Tygar, BS Yee, N Heintze, "Cryptographic Postage Indicia", in *ASIAN 96* (Springer-Verlag LNCS v 1179) pp 378–391, at www.cs.berkeley.edu/~tygar/papers/Cryptographic_Postage_Indicia/CMU-CS-96-113.pdf
- [1266] R Uhlig, "BT admits staff could have fiddled system to win Concorde trip", in *The Daily Telegraph* (23/7/1997), at <http://www.telegraph.co.uk:80/>
- [1267] *ukcrypto* mailing list, at <http://www.chiark.greenend.org.uk/mailman/listinfo/ukcrypto>
- [1268] Underwriters' Laboratories, <http://www.ul.com>

- [1269] J Ungoed-Thomas, A Lorenz, "French play dirty for £1bn tank deal", in *Sunday Times* (6/8/2000) p 5
- [1270] United Kingdom Government, 'e-commerce@its.best.uk', at <http://www.e-envoy.gov.uk/2000/strategy/strategy.htm>
- [1271] US Army, 'TM 31-210 *Improvised Munitions Handbook*', 1969, at <http://cryptome.org/tm-31-210.htm>
- [1272] 'United States Code'—US Federal Law, online for example at <http://www4.law.cornell.edu/uscode/>
- [1273] United States Court of Appeals, District of Columbia Circuit, *United States Telecom Association v. Federal Communications Commission and United States of America*, no 99-1442, 15/8/2000, at <http://pacer.cadc.uscourts.gov/common/opinions/200008/99-1442a.txt>
- [1274] UK Passport Service, 'Biometrics Enrolment Trial Report', May 2005; at www.passport.gov.uk/downloads/UKPSBiometricsEnrolment_TrialReport.pdf
- [1275] UPI newswire item, Oklahoma distribution, November 26, 1983, Tulsa, Oklahoma
- [1276] NA Van House, "Flickr and Public Image-Sharing: Distant Closeness and Photo Exhibition", at *CHI 2007* pp 2717–2722
- [1277] L van Hove, "Electronic Purses: (Which) Way to Go?", in *First Monday* v 5 no 7 (June 2000) at <http://firstmonday.org/issues/issue5-7/hove/>
- [1278] P Van Oorschot, M Wiener, "Parallel Collision Search with Application to Hash Functions and Discrete Logarithms", *Second ACM Conference on Computer and Communications Security*; proceedings published by the ACM, ISBN 0-89791-732-4, pp 210–218
- [1279] R van Renesse, 'Optical Document Security' (second edition), Artech House (1997) ISBN 0-89006-982-4
- [1280] R van Renesse, "Verifying versus falsifying banknotes", in *Optical Security and Counterfeit Deterrence Techniques II* (1998), IS&T (The Society for Imaging Science and Technology) and SPIE (The International Society for Optical Engineering) v 3314 ISBN 0-8194-2754-3, pp 71–85
- [1281] H van Vliet, 'Software Engineering—Principles and Practice', Wiley (second edition, 2000) ISBN 0-471-97508-7

- [1282] R van Voris, "Black Box Car Idea Opens Can of Worms", in *Law news Network* (4/6/99), at <http://www.lawnewsnetwork.com/stories/A2024-1999Jun4.html>
- [1283] G Vanneste, J Degraeve, "Initial report on security requirements", in [92]
- [1284] HR Varian, *'Intermediate Microeconomics—A Modern Approach'* (fifth edition), Norton (1999), ISBN 0-393-97370-0
- [1285] HR Varian, "Managing Online Security Risks", in *The New York Times*, 1 June 2000; at <http://www.nytimes.com/library/financial/columns/060100econ-scene.html>
- [1286] HR Varian, "New Chips Can Keep a Tight Rein on Customers", *New York Times* July 4 2002, at <http://www.nytimes.com/2002/07/04/business/04SCEN.html>
- [1287] S Vaudenay, "FFT-Hash-II is not yet Collision-Free", *Laboratoire d'Informatique de l'Ecole Normale Supérieure report LIENS-92-17*
- [1288] V Varadharajan, N Kumar, Y Mu, "Security Agent Based Distributed Authorization: An Approach", in *20th National Information Systems Security Conference*, proceedings published by NIST (1998) pp 315–328
- [1289] H Varian, "Economic Aspects of Personal Privacy", in *Privacy and Self-Regulation in the Information Age*, National Telecommunications and Information Administration report, 1996
- [1290] H Varian, "Managing Online Security Risks", Economic Science Column, *The New York Times*, June 1, 2000
- [1291] H Varian, "New chips and keep a tight rein on consumers, even after they buy a product", *New York Times*, July 4 2002
- [1292] H Varian, "System Reliability and Free Riding", in *Economics of Information Security*, Kluwer 2004 pp 1–15
- [1293] H Varian, Keynote address to the Third Digital Rights Management Conference, Berlin, Germany, January 13, 2005
- [1294] W Venema, "Murphy's Law and Computer Security", in *Usenix Security 96* pp 187–193
- [1295] J Vijayan, "HIPAA audit at hospital riles health care IT", *Computerworld*, June 15 2007; at <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9024921>

- [1296] J Vijayan, "Retail group takes a swipe at PCI, puts card companies 'on notice' ", *Computerworld* Oct 4 2007; at http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9040958&intsrc=hm_list
- [1297] N Villeneuve, "DNS tampering in China", Jul 10 2007, at <http://www.nartv.org/2007/07/10/dns-tampering-in-china/>
- [1298] B Vinck, "Security Architecture" (3G TS 33.102 v 3.2.0), from *Third Generation Partnership Project*, at http://www.3gpp.org/TSG/Oct_status_list.htm
- [1299] B Vinck, "Lawful Interception Requirements" (3G TS 33.106 v 3.0.0), from *Third Generation Partnership Project*, at http://www.3gpp.org/TSG/Oct_status_list.htm
- [1300] VISA International, *Integrated Circuit Chip Card–Security Guidelines Summary*, version 2 draft 1, November 1997
- [1301] A Viterbi, "Spread spectrum communications–myths and realities", in *IEEE Communications Magazine* v 17 no 3 (May 1979) pp 11–18
- [1302] PR Vizcaya, LA Gerhardt, "A Nonlinear Orientation Model for Global Description of Fingerprints", in *Pattern Recognition* v 29 no 7 (July 96) pp 1221–1231
- [1303] L von Ahn, personal communication, 2006
- [1304] L von Ahn, M Blum, NJ Hopper, J Langford, "CAPTCHA: Using Hard AI Problems For Security", *Advances in Cryptology–Eurocrypt 2003*, Springer LNCS v 2656 pp 294–311
- [1305] D Wagner, B Schneier, J Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm", in *Advances in Cryptology–Crypto 95*, Springer LNCS v 1294 pp 527–537
- [1306] D Wagner, "Cryptanalysis of Some Recently-Proposed Multiple Modes of Operation", in *Fifth International Workshop on Fast Software Encryption* (1998), Springer LNCS v 1372 pp 254–269
- [1307] D Wagner, I Goldberg, M Briceno, "GSM Cloning", at <http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html>; see also <http://www.scard.org/gsm/>
- [1308] D Wagner, B Schneier, "Analysis of the SSL 3.0 Protocol", in *Second USENIX Workshop on Electronic Commerce* (1996), pp 29–40; at <http://www.counterpane.com>

- [1309] M Waldman, AD Rubin, LF Cranor, "Publius: A robust, tamper-evident, censorship-resistant, web publishing system", in *9th USENIX Security Symposium* (2000) pp 59–72
- [1310] M Walker, "On the Security of 3GPP Networks", Invited talk at Eurocrypt 2000, at <http://www.ieee-security.org/Cipher/ConfReports/2000/CR2000-Eurocrypt.html>
- [1311] G Walsh, 'Review of Policy relating to Encryption Technologies' (1996), at <http://www.efa.org.au/Issues/Crypto/Walsh/>
- [1312] KG Walter, WF Ogden, WC Rounds, FT Bradshaw, SR Ames, DG Shumway, 'Models for Secure Computer Systems', Case Western Reserve University, Report no 1137 (31/7/1973, revised 21/11/1973)
- [1313] KG Walter, WF Ogden, WC Rounds, FT Bradshaw, SR Ames, DG Shumway, 'Primitive Models for Computer Security', Case Western Reserve University, Report no ESD-TR-74-117 (23/1/1974); at <http://www.dtic.mil>
- [1314] E Waltz, 'Information Warfare-Principles and Operations', Artech House (1998) ISBN 0-89006-511-X
- [1315] XY Wang, DG Feng, XJ Lai, HB Yu, "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD", IACR Cryptology ePrint Archive Report 2004/199, at <http://eprint.iacr.org/2004/199>
- [1316] XY Wang, YQL Yin, HB Yu, "Collision Search Attacks on SHA1", Feb 13 2005, at <http://www.infosec.sdu.edu.cn/sha-1/shanote.pdf>
- [1317] XY Wang, HB Yu, "How to Break MD5 and Other Hash Functions", in *Advances in Cryptology-Eurocrypt 2005*, at <http://www.infosec.sdu.edu.cn/paper/md5-attack.pdf>
- [1318] R Want, A Hopper, V Falcao, J Gibbons, "The Active Badge Location System", in *ACM Transactions on Information Systems* v 10 no 1 (Jan 92) pp 91–102; at <http://www.cl.cam.ac.uk/research/dtg/attarchive/ab.html>
- [1319] W Ware, 'Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security', Rand Report R609-1, The RAND Corporation, Santa Monica, CA (Feb 1970), available from <http://csrc.nist.gov/publications/history/index.html>
- [1320] M Warner, "Machine Politics In the Digital Age", in *The New York Times* November 9, 2003; at <http://query.nytimes.com/gst/fullpage.html?res=9804E3DC1339F93AA35752C1A9659C8B63>

- [1321] SD Warren, LD Brandeis, "The Right To Privacy" *Harvard Law Review* series 4 (1890) pp 193–195
- [1322] J Warrick, "Leak Severed a Link to Al-Qaeda's Secrets", in the *Washington Post* Oct 9 2007 p A01, "U.S. Intelligence Officials Will Probe Leak of Bin Laden Video", *ibid.*, Oct 10 2007 p A13
- [1323] Waste electrical and electronic equipment (WEEE) regulations 2007, at http://www.netregs.gov.uk/netregs/275207/1631119/?version=1&lang=_e
- [1324] M Watson, "Sat-nav 'jammer' threatens to sink road pricing scheme", in *Auto Express* Aug 8th 2007; at http://www.autoexpress.co.uk/news/autoexpressnews/209801/sat_nav_jammer.html
- [1325] RNM Watson, "Exploiting Concurrency Vulnerabilities in Kernel System Call Wrappers", in *First USENIX Workshop on Offensive Technologies (WOOT 07)*, at <http://www.watson.org/~robert/2007woot/>
- [1326] "Developer tortured by raiders with crowbars", M Weaver, *Daily Telegraph*, 31 October 97
- [1327] W Webb, "High-tech Security: The Eyes Have It", in *EDN* (18/12/97) pp 75–78
- [1328] SH Weingart, "Physical Security for the μ ABYSS System", in *Proceedings of the 1987 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, pp 52–58
- [1329] SH Weingart, "Mind the Gap: Updating FIPS 140", at *FIPS Physical Security Workshop*, Hawaii 2005; at <http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper18.pdf>
- [1330] SH Weingart, SR White, WC Arnold, GP Double, "An Evaluation System for the Physical Security of Computing Systems", in *Sixth Annual Computer Security Applications Conference*, 3–7/12/90, Tucson, Arizona; proceedings published by the IEEE (1990) pp 232–243
- [1331] L Weinstein, "IDs in Color Copies—A PRIVACY Forum Special Report" in *Privacy Forum Digest*, v 8 no 18 (6 Dec 1999), at <http://www.vortex.com/privacy/priv.08.18>
- [1332] L Weinstein, "The Online Medical Records Trap", Oct 4 2007, at <http://lauren.vortex.com/archive/000306.html>
- [1333] L Weinstein, "Not on Track with 'Do Not Track' ", Oct 31 2007, at <http://lauren.vortex.com/archive/000326.html>

- [1334] C Weissman, "Security Controls in the ADEPT-50 Time Sharing System", in *AFIPS Conference Proceedings, Volume 35, 1969 Fall Joint Computer Conference* pp 119–133
- [1335] C Weissman, "BLACKER: Security for the DDN, Examples of A1 Security Engineering Trades", in *Proceedings of the 1992 IEEE Symposium on Security and Privacy* pp 286–292
- [1336] G Welchman, *The Hut Six Story*, McGraw Hill (1982) ISBN 0-07-069180-0
- [1337] B Wels, R Gonggrijp, "Bumping locks", 2006, at <http://www.toool.nl/bumping.pdf>
- [1338] A Westfeld, A Pfitzmann, "Attacks on Steganographic Systems", in *Proceedings of the Third International Workshop on Information Hiding* (1999), Springer LNCS v 1768 pp 61–76
- [1339] AF Westin, *Data Protection in the Global Society* (1996 conference report), at <http://www.privacyexchange.org/iss/confpro/aicgsberlin.html>
- [1340] E Whitaker, "At SBC, It's All About 'Scale and Scope'", in *Business Week* Nov 7 2005, at http://www.businessweek.com/@n34h*IUQu7KtOwgA/magazine/content/05_45/b3958092.htm
- [1341] O Whitehouse, "Bluetooth: Red fang, blue fang," in *CanSecWest/core04*, linked from "Bluetooth PIN Cracker: Be Afraid" at http://www.symantec.com/enterprise/security_response/weblog/2006/11/bluetooth_pin_cracker_be_afrai.html
- [1342] A Whitten, JD Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0", in *Eighth USENIX Security Symposium* (1999) pp 169–183
- [1343] J Wildermuth, "Secretary of state casts doubt on future of electronic voting", *San Francisco Chronicle* Dec 2 2007, at <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/12/02/BASRTMOPE.DTL>
- [1344] MV Wilkes, RM Needham, *The Cambridge CAP computer and its Operating System*, Elsevier North Holland (1979)
- [1345] J Wilkins, *Mercury; or the Secret and Swift Messenger: Shewing, How a Man May with Privacy and Speed Communicate his Thoughts to a Friend at Any Distance*, London, Rich Baldwin (1694)
- [1346] C Williams, "Surge in encrypted torrents blindsides record biz", in *The Register* Nov 8 2007, at http://www.theregister.co.uk/2007/11/08/bittorrent_encryption_explosion/

- [1347] CL Wilson, MD Garris and CI Watson, "Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints", NIST IR 7110 (May 2004), at ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir.7110.pdf
- [1348] R Wilson, "Panel unscrambles intellectual property encryption issues", *EDN* Jan 31 2007, at <http://www.edn.com/index.asp?layout=article&articleid=CA6412249>
- [1349] T Wilson, "Visa Gave TJX a Pass on PCI in 2005", in *Dark Reading* Nov 12 2007, at http://www.darkreading.com/document.asp?doc_id=138838
- [1350] FW Winterbotham, *The Ultra Secret*, Harper & Row (1974)
- [1351] A Wolfson, 'A hoax most cruel', in *The Courier-Journal* Oct 9, 2005; at <http://www.courier-journal.com/apps/pbcs.dll/article?AID=/20051009/NEWS01/510090392>
- [1352] K Wong, "Mobile Phone Fraud - Are GSM Networks Secure?", in *Computer Fraud and Security Bulletin* (Nov 96) pp 11–18
- [1353] N Wong, "Judge tells DoJ 'No' on search queries", Google blog Mar 17 2006
- [1354] CC Wood, "Identity token usage at American commercial banks", in *Computer Fraud and Security Bulletin* (Mar 95) pp 14–16
- [1355] E Wood, *Housing Design, A Social Theory*, Citizens' Housing and Planning Council of New York, 1961
- [1356] L Wood, "Security Feed", in *CSO*, Apr 20 2007; at http://www2.csoonline.com/blog_view.html?CID=32865
- [1357] JPL Woodward, *Security Requirements for System High and Compartmented Mode Workstations* Mitre MTR 9992, Revision 1, 1987 (also published by the Defense Intelligence Agency as document DDS-2600-5502-87)
- [1358] B Wright, "The Verdict on Plaintext Signatures: They're Legal", in *Computer Law and Security Report* v 14 no 6 (Nov/Dec 94) pp 311–312
- [1359] B Wright, *The Law of Electronic Commerce: EDI, Fax and Email*, Little, Brown 1991; fourth edition (with supplement) 1994
- [1360] DB Wright, AT McDaid, "Comparing system and estimator variables using data from real line-ups", in *Applied Cognitive Psychology* v 10 no 1 pp 75–84
- [1361] JB Wright, *Report of the Weaponization and Weapons Production and Military Use Working Group—Appendix F to the Report of the*

- Fundamental Classification Policy Review Group*, US Department of Energy Office of Scientific and Technical Information (1997), <http://www.osti.gov/opennet/app-f.html>
- [1362] MA Wright, "Security Controls in ATM Systems", in *Computer Fraud and Security Bulletin*, November 1991, pp 11–14
- [1363] P Wright, *Spycatcher—The Candid Autobiography of a Senior Intelligence Officer*, William Heinemann Australia, 1987, ISBN 0-85561-098-0
- [1364] JX Yan, *Security for Online Games*, PhD thesis, University of Cambridge 2003
- [1365] JX Yan, A Blackwell, RJ Anderson, A Grant, "The Memorability and Security of Passwords—Some Empirical Results", University of Cambridge Computer Laboratory Technical Report no 500; at <http://www.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf>; also in *IEEE Security & Privacy*, Sep–Oct 2004 pp 25–29
- [1366] JX Yan, S Early, RJ Anderson, "The XenoService—A Distributed Defeat for Distributed Denial of Service", at Information Survivability Workshop, Oct 2000
- [1367] JX Yan, B Randell, *Security in Computer Games: from Pong to Online Poker*, University of Newcastle Tech Report CS-TR-889 (2005)
- [1368] JX Yan, B Randell, "A systematic classification of cheating in online games", at *Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games* (2005), at <http://portal.acm.org/citation.cfm?id=1103606>
- [1369] T Ylönen, 'SSH—Secure Login Connections over the Internet', in *Usenix Security 96* pp 37–42
- [1370] KS Yoon, YK Ham, RH Park, "Hybrid Approaches to Fractal Face Recognition Using the Hidden Markov Model and Neural Network", in *Pattern Recognition* v 31 no 3 (98) pp 283–293
- [1371] G Yuval, "Reinventing the Travois: Encryption/MAC in 30 ROM Bytes", in *Fourth International Workshop on Fast Software Encryption* (1997), Springer LNCS v 1267 pp 205–209
- [1372] MC Zari, AF Zwilling, DA Hess, KW Snow, CJ Anderson, D Chiang, "Personal Identification System Utilizing Low probability of Intercept (LPI) Techniques for Covert Ops", in *30th Annual IEEE Carnahan Conference on Security Technology* (1996) pp 1–6
- [1373] ZDnet, "Software blocks images of money", Jan 12 2004, at <http://news.zdnet.co.uk/software/0,1000000121,39119018,00.htm>

- [1374] K Zetter, "Scan This Guy's E-Passport and Watch Your System Crash", in *Wired*, Aug 1 2007, at <http://www.wired.com/politics/security/news/2007/08/epassport>
- [1375] RS Zhang, XY Wang, XH Yan, XX Jiang, "Billing Attacks on SIP-Based VOIP Systems", in *WOOT 2007*
- [1376] L Zhuang, F Zhou, JD Tygar, "Keyboard Acoustic Emanations Revisited" in *12th ACM Conference on Computer and Communications Security* (2005)
- [1377] P Zimbardo, *The Lucifer Effect*, Random House (2007)
- [1378] MW Zior, "A community response to CMM-based security engineering process improvement", in *18th National Information Systems Security Conference* (1995) pp 404–413
- [1379] M Zviran, WJ Haga, "A Comparison of Password Techniques for Multilevel Authentication Mechanisms", in *The Computer Journal* v 36 no 3 (1993) pp 227–237