# Bibliography

I intend to keep a collection of links at the book's web page, `http://www.ross-anderson.com`. Please check out this page if a link you wish to follow is out of date.


[1] M Abadi, "Explicit Communications Revisited: Two New Attacks on Authentication Protocols," in *IEEE Transactions on Software Engineering*, v 23 no 3 (Mar 1997), pp 185–186.

[2] M Abadi, RM Needham, "Prudent Engineering Practice for Cryptographic Protocols," *IEEE Transactions on Software Engineering*, v 22 no 1 (Jan 1996) 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] 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.

[4] DG Abraham, GM Dolan, GP Double, JV Stevens, "Transaction Security System," in *IBM Systems Journal*, v 30 no 2 (1991), pp 206–229.

[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] N Achs, "VISA Confronts the Con Men," *Cards International* (Oct 20, 1992) pp 8–9.

[7] EN Adams, "Optimizing Preventive Maintenance of Software Products," *IBM Journal of Research & Development*, v 28 no 1 (1984), pp 2–14.

[8] 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.

[9] J Adams, *Risk*, University College London Press (1995), ISBN 1-85728-067-9.

[10] 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 1997), pp 721–732.

[11] C Ajluni, "Two New Imaging Techniques Promise to Improve IC Defect Identification," in *Electronic Design*, v 43 no 14 (July 10, 1995), pp 37–38.

[12] Y Akdeniz, "Regulation of Child Pornography on the Internet" (Dec 1999), at http://www.cyber-rights.org/reports/child.htm.

[13] Alliance to Outfox Phone Fraud, http://www.bell-atl.com/security/fraud/.

[14] American Society for Industrial Security, http://www.asisonline.org.

[15] E Amoroso, *Fundamentals of Computer Security Technology*, Englewood Cliffs, NJ: Prentice Hall (1994), ISBN 0-13-10829-3.

[16] J Anderson, *Computer Security Technology Planning Study*, ESD-TR-73-51, U.S. Air Force Electronic Systems Division (1973), http://csrc.nist.gov/publications/history/index.html.

[17] 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.

[18] RJ Anderson, "Solving a Class of Stream Ciphers," in *Cryptologia*, v XIV no 3 (July 1990), pp 285–288.

[19] RJ Anderson, "Why Cryptosystems Fail," in *Communications of the ACM*, v 37 no 11 (Nov 1994), pp 32–40; earlier version at http://www.cl.cam.ac.uk/users/rja14/wcf.html.

[20] RJ Anderson, "Liability and Computer Security: Nine Principles," in *Computer Security—ESORICS 94*, Springer LNCS, v 875, pp 231–245.

[21] RJ Anderson, "Crypto in Europe—Markets, Law, and Policy," in *Cryptography: Policy and Algorithms*, Springer LNCS, v 1029, pp 75–89.

[22] RJ Anderson, "Clinical System Security—Interim Guidelines," in *British Medical Journal*, v 312 no 7023 (Jan 13, 1996), pp 109–111; http://www.cl.cam.ac.uk/ftp/users/rja14/guidelines.txt.

[23] RJ Anderson, "Security in Clinical Information Systems," British Medical Association (1996), ISBN 0-7279-1048-5.

[24] 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.

[25] RJ Anderson, "An Update on the BMA Security Policy," in [29], pp 233–250; http://www.cl.cam.ac.uk/ftp/users/rja14/bmaupdate.ps.gz.

[26] RJ Anderson, C Manifavas, C Sutherland, "NetCard—A Practical Electronic Cash Scheme," in *Security Protocols* (1996), Springer LNCS, v 1189, pp 49–57.

[27] RJ Anderson, "The Eternity Service," in *Proceedings of Pragocrypt 96* (GC UCMP, ISBN 80-01-01502-5), pp 242–252.

[28] RJ Anderson (ed), *Proceedings of the First International Workshop on Information Hiding* (1996), Springer LNCS, v 1174.

[29] RJ Anderson (ed), *Personal Medical Information—Security, Engineering and Ethics*, Springer-Verlag (1997), ISBN 3-540-63244-1.

[30] RJ Anderson, "GSM hack—Operator Flunks the Challenge," in `comp.risks` v 19.48: `http://catless.ncl.ac.uk/Risks/19.48.html`.

[31] 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`.

[32] RJ Anderson, "Safety and Privacy in Clinical Information Systems," in *Rethinking IT and Health*, J Lenaghan (ed.), IPPR (Nov 1998), (ISBN 1-86030-077-4), pp 140–160.

[33] RJ Anderson, "The DeCODE Proposal for an Icelandic Health Database"; partly published in *Læknabladhidh* (the *Icelandic Medical Journal*), v 84 no 11 (Nov 1998), pp 874–875; full text available from `http://www.cl.cam.ac.uk/users/ rja14/#Med`.

[34] RJ Anderson, "Healthcare Protection Profile—Comments," panel position paper at NISSC 1998; at `http://www.cl.cam.ac.uk/ftp/users/rja14/healthpp.pdf`.

[35] RJ Anderson, "The Formal Verification of a Payment System," chapter in *Industrial Strength Formal Methods: A Practitioner's Handbook*, MG Hinchey and JP Bowen (eds), Springer Verlag (Sept 1999, 1-85233-640-4), pp 43–52.

[36] 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`.

[37] RJ Anderson, "The Millennium Bug—Reasons Not to Panic," at `http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/y2k.html`.

[38] 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`.

[39] RJ Anderson, SJ Bezuidenhoudt, "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/meters.ps.gz`.

[40] 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 [41].

[41] RJ Anderson, E Biham, L Knudsen, "The Serpent Home Page," http://www.cl.cam.ac.uk/~rja14/serpent.html.

[42] 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/.

[43] RJ Anderson, MG Kuhn, "Tamper Resistance—A Cautionary Note," in *Proceedings of the Second Usenix Workshop on Electronic Commerce* (Nov 1996), pp 1–11; http://www.cl.cam.ac.uk/users/rja14/tamper.html.

[44] 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.

[45] 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.

[46] RJ Anderson, JH Lee, "Jikzi: A New Framework for Secure Publishing," in *Security Protocols 99*, Springer LNCS, v 1976, pp 21–36.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] CM Andrew, V Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, New York: Basic Books (1999), ISBN 0-46500310-9.

[52] http://www.anonymizer.com.

[53] JC Anselmo, "U.S. Seen More Vulnerable to Electromagnetic Attack," in *Aviation Week and Space Technology*, v 146 no 4 (July 28, 1997), p 67.

[54] T Appleby, "Chilling Debit-Card Scam Uncovered," in *The Globe & Mail* (Dec 12, 1999), p 1.

[55] U.S. Army, *Electromagnetic Pulse (EMP) and Tempest Protection for Facilities*, Hyattsville, Md: Corps of Engineers Publications Depot (1990).

[56] "ASPECT—Advanced Security for Personal Communications Technologies," at http://www.esat.kuleuven.ac.be/cosic/aspect/index.html.

[57] D Aubrey-Jones, "Internet—Virusnet?" in *Network Security* (Feb 1997), pp 15–19.

[58] D Aucsmith, "Tamper-Resistant Software: An Implementation," in [28], pp 317–333.

[59] D Aucsmith (ed), *Proceedings of the Second International Workshop on Information Hiding* (Portland, Oregon: Apr 1998), Springer LNCS, v 1525.

[60] B Audone, F Bresciani, "Signal Processing in Active Shielding and Direction-Finding Techniques," *IEEE Transactions on Electromagnetic Compatibility*, v 38 no 3 (Aug 1996), pp 334–340.

[61] D Austin, "Barclays Winning Card Fraud War," in *Banking Technology* (Apr 1994), p 5.

[62] D Austin, "Flood warnings," in *Banking Technology* (Jul–Aug 1999), pp 28–31.

[63] "Computer Combat Rules Frustrate the Pentagon," in *Aviation Week and Space Technology*, v 147 no 11 (Sept 9, 1997), pp 67–68.

[64] J Bacon, *Concurrent Systems*, Addison-Wesley (1997), ISBN 0-201-17767-6.

[65] J Bacon, K Moody, J Bates, R Hayton, CY Ma, A McNeil, O Seidel, M Spiteri, "Generic Support for Distributed Applications," in *IEEE Computer* (Mar 2000), pp 68–76.

[66] L Badger, DF Sterne, DL Sherman, KM Walker, SA Haghighat, "Practical Domain and Type Enforcement for UNIX," in *Proceedings of the 1995 IEEE Symposium on Security and Privacy*, pp 66–77.

[67] M Baggott, "The Smart Way to Fight Fraud," *Scottish Banker* (Nov 1995), pp 32–33.

[68] SA Baker, PR Hurst, *The Limits of Trust*, Kluwer Law International (1998), ISBN 9-0411-0639-1.

[69] 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.

[70] J Bamford, *The Puzzle Palace: A Report on NSA, America's Most Secret Agency*, New York: Houghton-Mifflin (1982, 3rd printing, revised edition due out shortly), ISBN 0-395-31286-8.

[71] Bank for International Settlements, *Security and Reliability in Electronic Systems for Payments*, British Computer Society (1982).

[72] Bank for International Settlements, http://www.bis.org/.

[73] "Card Fraud: Banking's Boom Sector," in *Banking Automation Bulletin for Europe* (Mar 1992), pp 1–5.

[74] RL Barnard, *Intrusion Detection Systems*, Butterworths (1988), ISBN 0-409-90030-3.

[75] A Barnett, "Britain's UFO Secrets Revealed," in *The Observer* (June 4, 2000); at

http://www.observer.co.uk/uk_news/story/0,6903,328010,00.html.

[76] J Barr, "The Gates of Hades," in *Linux World* (Apr 2000); at http://www.linuxworld.com/linuxworld/lw-2000-04/lw-04-vcontrol_3.html.

[77] R Baskerville, "Information Systems Security Design Methods: Implications for Information Systems Development," in *ACM Computing Surveys*, v 26 (1994), pp 375–414.

[78] PJ Bass, "Telephone Cards and Technology Development as Experienced by GPT Telephone Systems," in *GEC Review*, v 10 no 1 (1995), pp 14–19.

[79] "Great Microprocessors of the Past and Present," at http://www.cs.uregina.ca/~bayko/cpu.html.

[80] F Beck, *Integrated Circuit Failure Analysis—A Guide to Preparation Techniques*, New York: John Wiley & Sons, Inc. (1998), ISBN 0-471-97401-3.

[81] J Beck, "Sources of Error in Forensic Handwriting Examination," in *Journal of Forensic Sciences*, v 40 (1995), pp 78–87.

[82] HA Beker, C Amery, "Cryptography Policy," at http://www.baltimore.com/library/whitepapers/mn_cryptography.html.

[83] 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.

[84] H Beker, F Piper, *Cipher Systems*, Northwood (1982).

[85] 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.

[86] DE Bell, L LaPadula, "Secure Computer Systems," ESD-TR-73-278, Mitre Corporation; v I and II (Nov 1973), v III (Apr 1974).

[87] 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.

[88] 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.

[89] SM Bellovin, "Packets Found on an Internet," in *Computer Communications Review*, v 23 no 3 (July 1993), pp 26–31.

[90] SM Bellovin, "Defending against Sequence Number Attacks," RFC 1948 (May 1996); at http://sunsite.auc.dk/RFC/rfc/rfc1948.html.

[91] SM Bellovin, "Debit-Card Fraud in Canada," in comp.risks, v 20.69; at http:// catless.ncl.ac.uk/Risks/20.69.html.

[92] SM Bellovin, "Permissive Action Links," at http://www.research.att.com/~smb/nsam-160/pal.html.

[93] SM Bellovin, "ICMP Traceback Messages," Internet draft (Mar 2000), at `http://search.ietf.org/internet-drafts/draft-bellovin-itrace-00.txt`.

[94] SM Bellovin, WR Cheswick, *Firewalls and Internet Security: Repelling the Wily Hacker*, Reading, MA: Addison-Wesley (1994), ISBN 0-201-63357-4.

[95] M Benantar, R Guski, KM Triodle, "Access Control Systems: From Host-Centric to Network-Centric Computing," in *IBM Systems Journal*, v 35 no 1 (1996), pp 94–112.

[96] W Bender, D Gruhl, N Morimoto, A Lu, "Techniques for Data Hiding," in *IBM Systems Journal*, v 35 no 3–4 (1996), pp 313–336.

[97] T Benkart, D Bitzer, "BFE Applicability to LAN Environments," in *Seventeenth National Computer Security Conference* (1994); Proceedings published by NIST, pp 227–236.

[98] 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.

[99] T Berson, G Barksdale, "KSOS: Development Methodology for a Secure Operating System," *AFIPS Conference proceedings* (1979).

[100] K Biba, *Integrity Considerations for Secure Computer Systems*, Mitre Corporation MTR-3153 (1975).

[101] 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.

[102] E Biham, A Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer (1993), ISBN 0-387-97930-1.

[103] E Biham, A Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," in *Advances in Cryptology—Crypto 97*, Springer LNCS, v 1294, pp 513–525.

[104] A Biryukov, A Shamir, D Wagner, "Real-Time Cryptanalysis of A5/1 on a PC," in *Fast Software Encryption* (2000).

[105] Bishop and Bloomfield, "A Conservative Theory for Long-Term Reliability-Growth Prediction," in *IEEE Transactions on Reliability*, v 45 no 4 (Dec 1996), pp 550–560.

[106] DM Bishop, "Applying COMPUSEC to the Battlefield," in *17th Annual National Computer Security Conference* (1994), pp 318–326.

[107] M Bishop, M Dilger, "Checking for Race Conditions in File Accesses," in *Computing Systems USENIX*, v 9 no 2 (Spring 1996), pp 131–152.

[108] 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 Patentamt, November 11, 1993.

[109] J Blackledge, "Making Money from Fractals and Chaos: Microbar," in *Mathematics Today*, v 35 no 6 (Dec 1999), pp 170–173.

[110] RD Blackledge, "DNA versus Fingerprints," in *Journal of Forensic Sciences*, v 40 (1995), p 534.

[111] GR Blakley, "Safeguarding Cryptographic Keys," in *Proceedings of NCC AFIPS* (1979), pp 313–317.

[112] B Blakley, R Blakley, RM Soley, *CORBA Security: An Introduction to Safe Computing with Objects*, Reading, MA: Addison-Wesley (1999), ISBN 0-201-32565-9.

[113] M Blaze, "Protocol Failure in the Escrowed Encryption Standard," in *Second ACM Conference on Computer and Communications Security* (Nov 2–4, 1994), Fairfax, VA: Proceedings published by the ACM ISBN 0-89791-732-4, pp 59–67; at `http://www.crypto.com/papers/`.

[114] M 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`.

[115] M Blaze, J Feigenbaum, J Lacy, "Decentralized Trust Management," in *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, pp 164–173.

[116] 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.

[117] 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.

[118] B Blobel, "Clinical Record Systems in Oncology. Experiences and Developments on Cancer Registers in Eastern Germany," in [29], pp 39–56.

[119] 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.

[120] ER Block, *Fingerprinting*, Franklin Wells (1970), SBN 85166-435-0.

[121] 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 1993), pp 138–145.

[122] WE Boebert, RY Kain, "A Practical Alternative to Hierarchical Integrity Policies," in *8th National Computer Security Conference* (1985), Proceedings published by NIST, p 18.

[123] BW Boehm, *Software Engineering Economics*, Englewood Cliffs, NJ: Prentice Hall (1981), ISBN 0-13-822122-7.

[124] N Bohm, I Brown, B Gladman, "Electronic Commerce—Who Carries the Risk of Fraud?" *Journal of Information Law & Technology*, v 3 (2000); `http://elj.warwick.ac.uk/jilt/00-3/bokm.html`.

[125] MK Bond, "Attacks on Cryptoprocessor Transaction Sets," *to be submitted to CHES 2001*.

[126] 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.

[127] 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.

[128] V Bontchev, "Possible Macro Virus Attacks and How to Prevent Them," in *Computers and Security*, v 15 no 7 (1996), pp 595–626.

[129] NS Borenstein, "Perils and Pitfalls of Practical Cybercommerce," in *Communications of the ACM*, v 39 no 6 (June 1996), pp 36–44.

[130] E Bovenlander, talk on smartcard security, Eurocrypt 97, reported in [44].

[131] E Bovenlander, RL van Renesse, "Smartcards and Biometrics: An Overview," in *Computer Fraud and Security Bulletin* (Dec 1995), pp 8–12.

[132] 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.

[133] 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).

[134] S Brands, *Rethinking Public Key Infrastructures and Digital Certificates—Building in Privacy*, MIT Press (2000), ISBN 0-262-02491-8.

[135] 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.

[136] M Brelis, "Patients' Files Allegedly Used for Obscene Calls," in *Boston Globe*, (Apr 11, 1995); also in `comp.risks`, v 17 no 7.

[137] DFC Brewer, MJ Nash, "Chinese Wall Model," in *Proceedings of the 1989 IEEE Computer Society Symposium on Security and Privacy*, pp 215–228.

[138] M Briceno, I Goldberg, D Wagner, "An Implementation of the GSM A3A8 Algorithm," at `http://www.scard.org/gsm/a3a8.txt`.

[139] D Brin, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* Perseus Press (1999), ISBN 0-73820144-8.

[140] F Brooks, *The Mythical Man-Month: Essays on Software Engineering*, Addison-Wesley (1995), ISBN 0-201-83595-9.

[141] D Brown, "Techniques for Privacy and Authentication in Personal Communications Systems," in *IEEE Personal Communications*, v 2 no 4 (Aug 1995), pp 6–10.

[142] R Buderi, *The Invention That Changed the World*, Simon & Schuster, New York, (1996); ISBN 0-684-81021-2.

[143] H Buehler, interview with Swiss Radio International, (July 4, 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.

[144] http://archives.neohapsis.com/archives/bugtraq/.

[145] 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.

[146] 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.

[147] Buro Jansen & Janssen, "Making Up the Rules: Interception versus Privacy," (Aug 8, 2000), at http://www.xs4all.nl/~respub/crypto/english/.

[148] 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.

[149] C Busch, F Graf, S Wolthusen, A Zeidler, "A System for Intellectual Property Protection," Fraunhofer Institute, at http://www.igd.fhg.de/igd-a8.

[150] 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.

[151] "Long Distance Phone Scam Hits Internet Surfers," in businessknowhow.com, at http://www.businessknowhow.com/newlong.htm.

[152] California Secretary of State, "A Report on the Feasibility of Internet Voting" (Jan 2000), at http://www.ss.ca.gov/executive/ivote/.

[153] J Calvert, P Warren, "Secrets of McCartney Bank Cash Are Leaked," in *The Express* (Feb 9, 2000), pp 1–2.

[154] JL Cambier, "Biometric Identification in Large Population," in *Information Security Bulletin*, v 5 no 2 (Mar 2000), pp 17–26.

[155] 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.

[156] LJ Camp, C Wolfram, "Pricing Security," Third Information Survivability Workshop, Boston, (Oct 2000).

[157] D Campbell, "Somebody's Listening," in *The New Statesman* (Aug 12, 1988), pp 1, 10–12; at http://jya.com/echelon-dc.htm.

[158] D Campbell, "Making History: The Original Source for the 1988 First Echelon Report Steps Forward" (Feb 25, 2000); at http://cryptome.org/echelon-mndc.htm.

[159] 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.

[160] D Campbell, P Lashmar, "The New Cold War: How America Spies on Us for Its Oldest Friend—the Dollar," in *The Independent* (July 2, 2000); at `http://www.independent.co.uk/news/World/Americas/2000-07/coldwar020700.shtml`.

[161] JP Campbell, "Speaker Recognition: A Tutorial," in *Proceedings of the IEEE*, v 85 no 9 (Sept 1997), pp 1437–1462.

[162] C Cant, S Wiseman, "Simple Assured Bastion Hosts," in *13th Annual Computer Security Application Conference* (1997); Proceedings published by IEEE Computer Society, ISBN 0-8186-8274-4ACSAC, pp 24–33.

[163] "Dark Horse in Lead for Fingerprint ID Card," *Card World Independent* (May 1994), p 2.

[164] "German A555 Takes Its Toll," in *Card World International* (Dec 1994–Jan 1995), p 6.

[165] "High Tech Helps Card Fraud Decline," in *Cards International*, no 117 (Sept 29, 1994).

[166] "VISA Beefs Up Its Anti-Fraud Technology," in *Cards International*, no 189 (Dec 12, 1997), p 5.

[167] JM Carlin, "UNIX Security Update," at *USENIX Security 93*, pp 119–130.

[168] J Carr, "Doing Nothing Is Just Not an Option," in *The Observer* (June 18, 2000), at `http://www.fipr.org/rip/index.html`.

[169] J Carroll, *Big Blues: The Unmaking of IBM*, New York: Crown Publishers (1993), ISBN 0-517-59197-9.

[170] H Carter, "Car Clock Fixer Jailed for Nine Months," in *The Guardian* (Feb 15, 2000), p 13.

[171] R Carter, "What You Are . . . Not What You Have," in *International Security Review Access Control*, Special Issue (Winter 1993–1994), pp 14–16.

[172] S Castano, M Fugini, G Martella, P Samarati, *Database Security*, Reading, MA: Addison-Wesley (1994), ISBN 0-201-59375-0.

[173] Center for Democracy and Technology, `http://www.cdt.org/`.

[174] 'The CERT Coordination Center Vulnerability Disclosure Policy;' http://www.cert.org/faq/vuldisclosurepolicy.html

[175] 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 (Sep 9, 2000), pp 612–614; at `http://bmj.com/cgi/content/full/321/7261/612`.

[176] L Chapman, *Your Disobedient Servant*, New York: Penguin Books (1979).

[177] D Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," in *Communications of the ACM*, v 24 no 2 (Feb 1981).

[178] D Chaum, "Blind Signatures for Untraceable Payments," in *Crypto 82*, Plenum Press (1983), pp 199–203.

[179] D Chaum, "The Dining Cryptographers' Problem: Unconditional Sender and Recipient Untraceability," in *Journal of Cryptology*, v 1 (1989) pp 65–75.

[180] D Chaum, A Fiat, M Naor, "Untraceable Electronic Cash," in *Advances in Cryptology—CRYPTO '88*, Springer LNCS, v 403, pp 319–327.

[181] R Chellappa, CL Wilcon, S Sirohey, "Human and Machine Recognition of Faces: A Survey," in *Proceedings of the IEEE*, v 83 no 5 (May 1995), pp 705–740.

[182] HJ Choi, private discussion with author.

[183] B Christianson, et al. (ed), "Security Protocols—5th International Workshop," Springer LNCS, v 1360 (1998).

[184] B Christianson, et al. (ed), "Security Protocols—6th International Workshop," Springer LNCS, v 1550 (1999).

[185] F Church (chairman), "Intelligence Activities—Senate Resolution 21," U.S. Senate, 94th Congress, First Session, at `http://cryptome.org/nsa-4th.htm`.

[186] WS Ciciora, "Inside the Set-Top Box," in *IEEE Spectrum*, v 12 no 4 (Apr 1995), pp 70–75.

[187] 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.

[188] R Clark, *The Man Who Broke Purple*, New York, Little Brown (1977), ISBN 0-316-14595-5.

[189] I Clarke, "The Free Network Project Homepage," at `http://freenet.sourceforge.net/`.

[190] 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 (May 18, 1999), at `http://www.linx.net/noncore/bcp/traceability-bcp.html`.

[191] S Clough, "Bombings 'Inspired by Atlanta Attack,'" in *Daily Telegraph* (June 6, 2000); at `http://www.telegraph.co.uk:80/`.

[192] FB Cohen, *A Short Course on Computer Viruses*, New York: John Wiley & Sons, Inc. (1994), ISBN 0-471-00769-2.

[193] JL Colbert, PL Bowen, "A Comparison of Internal Controls: COBIT, SAC, COSO and SAS 55/78," at `http://www.isaca.org/bkr_cbt3.htm`.

[194] A Collins, "Court Decides Software Time-Locks Are Illegal," in *Computer Weekly* (Aug 19, 1993), p 1.

[195] D Comer, "Cryptographic Techniques—Secure Your Wireless Designs," in *EDN* (Jan 18, 1996), pp 57–68.

[196] Committee of Sponsoring Organizations of the Treadway Commission (CSOTC), "Internal Control—Integrated Framework" (COSO Report, 1992); from `http://www.coso.org/`.

[197] "Communicating Britain's Future," at http://www.fipr.org/polarch/labour.html.

[198] "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.

[199] Computer Emergency Response Team Coordination Center, at http://www.cert.org/.

[200] "Telecoms Fraud in the Cellular Market: How Much Is Hype and How Much Is Real?" in *Computer Fraud and Security Bulletin* (June 1997), pp 11–14.

[201] Computer Privacy Digest, v 17 no 7 (Sept 15, 2000).

[202] J B Condat, "Toll Fraud on French PBX Systems," in *Computer Law and Security Report*, v 10 no 2 (Mar/Apr 1994), pp 89–91.

[203] 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.

[204] E Constable, "American Express to Reduce the Risk of Online Fraud".

[205] D Coppersmith, "The Data Encryption Standard (DES) and Its Strength against Attacks," IBM report RC 18613 (81421).

[206] Council of Europe, "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data," European Treaty Series, no. 108 (Jan 28, 1981); at http://www.privacy.org/pi/intl_orgs/coe/dp_convention_108.txt.

[207] 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.

[208] 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/.

[209] L Cranor, "Lorrie Cranor's Electronic Voting Hot List," at http://www.ccrc.wustl.edu/~lorracks/sensus/hotlist.html.

[210] 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.

[211] B Crispo, M Lomas, "A Certification Scheme for Electronic Commerce," in *Security Protocols* (1996), Springer LNCS, v 1189, pp 19–32.

[212] 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 1988), pp 1268–1287.

[213] J Daemen, L Knudsen, V Rijmen, "The Block Cipher SQUARE," in *Fourth*

*International Workshop on Fast Software Encryption*, Springer LNCS, v 1267 (1997), pp 149–165; at http://www.esat.kuleuven.ac.be/~rijmen/square/.

[214] "Beating the Credit Card Telephone Fraudsters," in *Daily Telegraph* (Oct 9, 1999), at http://www.telegraph.co.uk:80/.

[215] T Dalrymple, "The Sinister Ethos of the Baying Mob," in *The Sunday Telegraph* (Aug 13, 2000), at http://www.dailytelegraph.co.uk.

[216] M Darman, E le Roux, "A New Generation of Terrestrial and Satellite Microwave Communication Products for Military Networks," in *Electrical Communication* (Q4 1994), pp 359–364.

[217] Data Protection Commissioners of EU and EES countries and Switzerland, two statements, *20th International Conference on Data Protection*, Santiago de Compostela, (Sept 16–18, 1998); at http://www.dataprotection.gov.uk/20dpcom.html.

[218] 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 1993), pp 1148–1161.

[219] J Daugman, "Biometric Decision Landscapes," Technical Report No. TR482, University of Cambridge Computer Laboratory.

[220] C Davies, R Ganesan, "BApasswd: A New Proactive Password Checker," in *16th National Computer Security Conference* (1993); proceedings published by NIST, pp 1–15.

[221] DW Davies, WL Price, *Security for Computer Networks*, New York: John Wiley & Sons, Inc. (1984).

[222] 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.

[223] H Davies, "Physiognomic Access Control," in *Information Security Monitor*, v 10 no 3 (Feb 1995), pp 5–8.

[224] D Davis, "Compliance Defects in Public-Key Cryptography," in *Sixth USENIX Security Symposium Proceedings* (July 1996), pp 171–178.

[225] 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.

[226] 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.

[227] C Deavours, D Kahn, L Kruh, G Mellen, B Winkel, *Cryptology—Yesterday, Today, and Tomorrow*, Artech House (1987), ISBN 0-89006-253-6.

[228] 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.

[229] C Deavours, L Kruh, *Machine Cryptography and Modern Cryptanalysis*, Artech House (1985), ISBN 0-89006-161-0.

[230] B Demoulin, L Kone, C Poudroux, P Degauque, "Electromagnetic Radiation of Shielded Data Transmission Lines," in [301], pp 163–173.

[231] 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.

[232] I Denley, S Weston-Smith, "Privacy in Clinical Information Systems in Secondary Care," in *British Medical Journal*, v 318 (May 15, 1999), pp 1328–1331.

[233] DE Denning, "The Lattice Model of Secure Information Flow," in *Communications of the ACM*, v 19 no 5, pp 236–243.

[234] DE Denning, *Cryptography and Data Security*, Addison-Wesley (1982), ISBN 0-201-10150-5.

[235] DE Denning, *Information Warfare and Security*, Addison-Wesley (1999), ISBN 0-201-43303-6.

[236] 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`.

[237] DE Denning, PH MacDoran, "Location-Based Authentication: Grounding Cyberspace for Better Security," in *Computer Fraud and Security Bulletin* (Feb 1996), pp 12–16.

[238] DE Denning, J Schlorer, "Inference Controls for Statistical Databases," in *IEEE Computer*, v 16 no 7 (July 1983), pp 69–82.

[239] DE Denning, *Information Warfare and Security*, Readings, MA: Addison Wesley (1998), ISBN 0-201-43303-6.

[240] Department of Defense, "Department of Defense Trusted Computer System Evaluation Criteria," DoD 5200.28-STD (Dec 1985).

[241] Department of Defense, "A Guide to Understanding Covert Channel Analysis of Trusted Systems," NCSC-TG-030 (Nov 1993).

[242] Department of Defense, "Password Management Guideline," CSC-STD-002-85 (1985).

[243] Department of Defense, "A Guide to Understanding Data Remanence in Automated Information Systems," NCSC-TG-025 (1991).

[244] Department of Defense, "Technical Rationale behind CSC-STD-003-85: Computer Security Requirements," CSC-STD-004-85 (1985).

[245] Department of Justice, "Guidelines for Searching and Seizing Computers" (1994); at `http://www.epic.org/security/computer_search_guidelines.txt`.

[246] Y Desmedt, Y Frankel, "Threshold Cryptosystems," in *Advances in Cryptology—Proceedings of Crypto 89*, Springer LNCS, v 435, pp 307–315.

[247] J Dethloff, "Special Report: Intellectual Property Rights and Smart Card Patents: The Past, the Present, the Future," in *Smart Card News* (Feb 1996), pp 36–38.

[248] W Diffie, ME Hellman, "New Directions in Cryptography," in *IEEE Transactions on Information Theory*, v 22 no 6 (Nov 1976), pp 644–654.

[249] W Diffie, ME Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," in *Computer*, v 10 no 6 (June 1977), pp 74–84.

[250] W Diffie, S Landau, *Privacy on the Line—The Politics of Wiretapping and Encryption*, MIT Press (1998), ISBN 0-262-04167-7.

[251] E Dijkstra, "Solution of a Problem in Concurrent Programming Control," in *Communications of the ACM*, v 8 no 9 (1965), p 569.

[252] The Discount Long Distance Digest, at `http://www.thedigest.com/shame/`.

[253] D Dittrich, "Distributed Denial of Service (DDoS) Attacks/Tools," at `http://staff.washington.edu/dittrich/misc/ddos/`; see also `http://www.washington.edu/People/dad/`.

[254] RC Dixon, *Spread Spectrum Systems with Commercial Applications*, New York: John Wiley & Sons, Inc. (1994), ISBN 0-471-59342-7.

[255] H Dobbertin, "Cryptanalysis of MD4," *Journal of Cryptology*, v 11 no 4 (1998), pp 253–270.

[256] 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.

[257] "Dotcom Executives 'More Likely to Have Dark Pasts'," C Daniel, *Financial Times*, (Oct 23, 2000); `http://www.ft.com`.

[258] I Drury, "Pointing the Finger," in *Security Surveyor*, v 27 no 5 (Jan 1997), pp 15–17.

[259] Wim van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" in *Computers & Security*, v 4 (1985), pp 269–286.

[260] *The Economist*, "Digital Rights and Wrongs" (July 17, 1999); see `www.economist.com`.

[261] *The Economist*, "Living in the Global Goldfish Bowl," (Dec 18–24, 1999), Christmas special; see `www.economist.com`.

[262] A Edwards, "BOLERO, a TTP project for the Shipping Industry," in *Information Security Technical Report*, v 1 no 1 (1996), pp 40–45.

[263] 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.

[264] Electronic Frontier Foundation, `http://www.eff.org`.

[265] Electronic Frontier Foundation, *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design* EFF (1998); ISBN 1-56592-520-3; at `http://cryptome.org/cracking-des.htm`.

[266] Electronic Privacy Information Center, http://www.epic.org.

[267] JH Ellis, *The History of Non-Secret Encryption*, at http://www.cesg.gov.uk/about/nsecret/ellis.htm.

[268] 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.

[269] *Enfopol Papiere*, Telepolis archiv special (1998/1999), at http://www.heise.de/tp/deutsch/special/enfo/default.html.

[270] 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 1996), pp 1063–1088.

[271] EPIC, "Approvals for Federal Pen Registers and Trap and Trace Devices 1987–1998," at http://www.epic.org/privacy/wiretap/stats/penreg.html.

[272] 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.

[273] 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.

[274] J Epstein, R Pascale, "User Interface for a High-Assurance Windowing System," in *9th Annual Computer Security Applications Conference* (1993); proceedings published by the IEEE, ISBN 0-8186-4330-7, pp 256–264.

[275] T Escamilla, *Intrusion Detection—Network Security beyond the Firewall*, New York: John Wiley & Sons, Inc. (1998), ISBN 0-471-29000-9.

[276] J Essinger, *ATM Networks—Their Organization, Security, and Future*, Elsevier (1987).

[277] A Etzioni, *The Limits of Privacy*, New York: Basic Books (1999), ISBN 0-465-04089-6.

[278] European Parliament, "Development of Surveillance Technology and Risk of Abuse of Economic Information," Luxembourg (Apr 1999), PE 166.184/Part3/4, at http://www.gn.apc.org/duncan/stoa.htm.

[279] 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/intl_orgs/ec/eudp.html.

[280] European Union, "Draft Council Resolution on the Lawful Interception of Telecommunications in Relation to New Technologies" 6715/99 (Mar 15, 1999), at http://www.fipr.org/polarch/enfopol19.html/; for background, see http://www.fipr.org/polarch/.

[281] G Faden, "Reconciling CMW Requirements with Those of X11 Applications," in *Proceedings of the 14th Annual National Computer Security Conference* (1991).

[282] M Fairhurst, "The Hedge End Experiment," in *International Security Review*, no 85 (Summer 1994), p 20.

[283] M Fairhurst, "Signature Verification Revisited: Promoting Practical Exploitation of Biometric Technology," in *Electronics and Communication Engineering Journal*, v 9 no 6 (Dec 1997), pp 273–280.

[284] *Federal Trade Commission v Audiotex Connection, Inc.*, and others, at `http://www.ftc.gov/os/1997/9711/Adtxamdfcmp.htm`.

[285] Federal Trade Commission, "ID Theft: When Bad Things Happen to Your Good Name," at `http://www.consumer.gov/idtheft/`.

[286] Federation of American Scientists, `http://www.fas.org`.

[287] H Federrath, J Thees, "Schutz der Vertraulichkeit des Aufenthaltsorts von Mobilfunkteilnehmern," in *Datenschutz und Datensicherheit* (June 1995), pp 338–348.

[288] P Fellwock (using pseudonym Winslow Peck), "U.S. Electronic Espionage: A Memoir," in *Ramparts*, v 11 no 2 (Aug 1972), pp 35–50; at `http://jya.com/nsa-elint.htm`.

[289] JS Fenton, "Information Protection Systems," PhD thesis, Cambridge University, 1973.

[290] N Ferguson, B Schneier, "A Cryptographic Evaluation of IPSEC," at `http://www.counterpane.com/ipsec.html`.

[291] D Ferraiolo, R Kuhn, "Role-Based Access Controls," in *15th National Computer Security Conference* (1992); proceedings published by NIST, pp 554–563.

[292] PFJ Fillery, AN Chandler, "Is Lack of Quality Software a Password to Information Security Problems?" in *IFIP SEC 94*, paper C8.

[293] "Psychologists and Banks Clash over Merits of Photographs on Cards," in *Financial Technology International Bulletin*, v 13 no 5 (Jan 1996), pp 2–3.

[294] D Fine, "Why Is Kevin Lee Poulsen Really in Jail?" at `http://www.well.com/user/fine/journalism/jail.html`.

[295] B Fischer, talk given at Cryptologic History Symposium, NSA (Oct 1999); reported in *Cryptologia*, v 24 no 2 (Apr 2000), pp 160–167.

[296] S Fischer-Hubner, "Towards a Privacy-Friendly Design and Use of IT-Security Mechanisms," in *17th National Computer Security Conference* (1994); proceedings published by NIST, pp 142–152.

[297] RA Fisher, *The Genetical Theory of Natural Selection*, Oxford: Clarendon Press (1930); 2nd ed., New York: Dover Publications (1958).

[298] 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`.

[299] M Fleet, "Five Face Sentence over Notes That Passed Ultraviolet Tests," in *The Daily Telegraph* (Dec 23, 1999), at `http://www.telegraph.co.uk:80/`.

[300] SN Foley, "Aggregation and Separation as Noninterference Properties," in *Journal of Computer Security*, v 1 no 2 (1992), pp 158–188.

[301] Fondazione Ugo Bordoni, Symposium on Electromagnetic Security for Information Protection, Rome, Italy (Nov 21–22, 1991).

[302] S Forrest, SA Hofmeyr, A Somayaji, "Computer Immunology," in *Communications of the ACM*, v 40 no 10 (Oct 1997), pp 88–96.

[303] DS Fortney, JJ Lim, "A Technical Approach for Determining the Importance of Information in Computerized Alarm Systems," in *17th National Computer Security Conference* (1994); proceedings published by NIST, pp 348–357.

[304] The Foundation for Information Policy Research, `http://www.fipr.org`.

[305] B Fox, "How to Keep Thieves Guessing," in *New Scientist* (June 3, 1995), p 18.

[306] B Fox, "Do Not Adjust Your set . . . We Have Assumed Radio Control," in *New Scientist* (Jan 8, 2000), at `http://www.newscientist.com/ns/20000108/newsstory6.html`.

[307] B Fox, "The Pirate's Tale," in *New Scientist* (Dec 18, 1999), at `http://www.newscientist.com/ns/19991218/thepirates.html`.

[308] D Fox, "IMSI-Catcher," in *Datenschutz und Datensicherheit*, v 21 no 9 (Sept 1997), p 539.

[309] D Foxwell, "Off-the-Shelf, on to Sea," in *International Defense Review*, v 30 (Jan 1997), pp 33–38.

[310] D Foxwell, M Hewish, "GPS: Is It Lulling the Military into a False Sense of Security?" in *Jane's International Defense Review* (Sept 1998), pp 32–41.

[311] LJ Fraim, "SCOMP: A Solution to the Multilevel Security Problem," in *IEEE Computer*, v 16 no 7 (July 1983), pp 26–34.

[312] E Franz, A Jerichow, "A Mix-Mediated Anonymity Service and Its Payment," in *ESORICS 98*, Springer LNCS, v 1485, pp 313–327.

[313] 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.

[314] "Banks Fingerprint Customers to Cut Cheque Fraud," in *Fraud Watch*, no 1 (1997), p 9.

[315] "Chip Cards Reduce Fraud in France," in *Fraud Watch*, no 1 (1996), p 8.

[316] "Counterfeit and Cross-Border Fraud on Increase Warning," in *Fraud Watch*, no 1 (1996), pp 6–7.

[317] "Finger Minutiae System Leaps the 1:100,000 False Refusal Barrier," in *Fraud Watch*, no 2 (1996), pp 6–9.

[318] "Widespread Card Skimming Causes European Concern," in *Fraud Watch*, no 3 (1997), pp 1–2.

[319] P Freiberger, M Swaine, *Fire in the Valley—The Making of the Personal Computer*, New York: McGraw-Hill (1999), ISBN 0-07-135892-7.

[320] M Freiss, *Protecting Networks with Satan*, O'Reilly & Associates (1997), ISBN 1-56592-425-8.

[321] J Frizell, T Phillips, T Groover, "The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document," in *17th National Computer Security Conference* (1994); proceedings published by NIST, pp 378–399.

[322] M Frost, "Spyworld: Inside the Canadian & American Intelligence Establishments," Diane Publishing Co (1994), ISBN 0-78815791-4.

[323] 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`.

[324] DA Fulghum, "Communications Intercepts Pace EP-3s," in *Aviation Week and Space Technology*, v 146 no 19 (May 5, 1997), pp 53–54.

[325] S Furber, *ARM System Architecture*, Addison-Wesley (1996), ISBN 0-210-40352-8.

[326] HF Gaines, *Cryptanalysis—A Study of Ciphers and Their Solution*, Dover, ISBN 486-20097-3 (1939, 1956).

[327] M Galecotti, "Russia's Eavesdroppers Come Out of the Shadows," in *Jane's Intelligence Review*, v 9 no 12 (Dec 1997), pp 531–535.

[328] F Galton, "Personal Identification and Description," in *Nature* (June 21, 1888), pp 173–177.

[329] T Gandy, "Brainwaves in Fraud Busting," *Banking Technology* (Dec 1995/Jan 1996), pp 20–24.

[330] S Garfinkel, *Database Nation*, O'Reilly & Associates (2000), ISBN 1-56592-653-6.

[331] S Garfinkel, G Spafford, *Practical UNIX and Internet Security*, O'Reilly & Associates (1996), ISBN 1-56592-148-8.

[332] W Gates, W Buffett, "The Bill & Warren Show," in *Fortune* (July 20, 1998).

[333] General Accounting Office, U.S., "Medicare—Improvements Needed to Enhance Protection of Confidential Health Information," GAO/HEHS-99-140; at `http://www.gao.gov/AIndexFY99/abstracts/he99140.htm`.

[334] E German, "Problem Idents," at http://onin.com/fp/problemidents.html.

[335] A Gidari, JP Morgan, "Survey of State Electronic & Digital Signature Legislative Initiatives," at `http://www.ilpf.org/digsig/digrep.htm`.

[336] D Gifford, A Spector, "The CIRRUS Banking Network," in *Communications of the ACM*, v 28 no 8 (Aug 1985), pp 797–807.

[337] 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.

[338] WN Goetzmann, "Financing Civilization," at `http://viking.som.yale.edu/will/finciv/chapter1.htm`.

[339] 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.

[340] I Goldberg, D Wagner, "Randomness and the Netscape Browser," in *Dr. Dobbs Journal*, no 243 (Jan 1996), pp 66–70.

[341] L Goldberg, "Recycled Cold-War Electronics Battle Cellular Telephone Thieves," in *Electronic Design*, v 44 no 18 (Sept 3, 1996), pp 41–42.

[342] O Goldreich, *"Foundations of Cryptography" (fragments of a book)*, at `http://www.toc.lcs.mit.edu/~oded/homepage.html`.

[343] O Goldreich, "Modern Cryptography, Probabilistic Proofs, and Pseudorandomness," in Springer (1999), ISBN 3-540-64766-X.

[344] D Gollmann, *Computer Security*, New York: John Wiley & Sons, Inc. (1999), ISBN 0-471-97884-2.

[345] D Gollmann, "What Is Authentication?" in *Security Protocols*, Springer LNCS, v 1796 (2000), pp 65–72.

[346] L Gong, *Inside Java 2 Platform Security: Architecture, API Design, and Implementation*, Addison-Wesley (1999), ISBN 0-201-31000-7.

[347] KE Gordon, RJ Wong, "Conducting Filament of the Programmed Metal Electrode Amorphous Silicon Antifuse," in *Proceedings of International Electron Devices Meeting* (Dec 1993); reprinted as pp 6–3 to 6–10, *QuickLogic Data Book* (1994).

[348] J Gough, *Watching the Skies—A History of Ground Radar for the Air Defence of the United Kingdom by the Royal Air Force from 1946 to 1975*, London: Her Majesty's Stationery Office (1993), ISBN 0-11-772723-7.

[349] RM Graham, "Protection in an Information Processing Utility," in *Communications of the ACM*, v 11 no 5 (May 1968), pp 365–369.

[350] FT Grampp, RH Morris, "UNIX Operating System Security," in *AT&T Bell Laboratories Technical Journal*, v 63 no 8 (Oct 1984), pp 1649–1672.

[351] 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.

[352] 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.

[353] J Gray, P Syverson, "A Logical Approach to Multilevel Security of Probabilistic Systems," in *Distributed Computing*, v 11 no 2 (1988), pp 73–90.

[354] T Greening, "Ask and Ye Shall Receive: A Study in Social Engineering," in *SIGSAC Review*, v 14 no 2 (Apr 1996), pp 9–14.

[355] A Griew, R Currell, *A Strategy for Security of the Electronic Patient Record*, Aberystwyth: Institute for Health Informatics, University of Wales (Mar 1995).

[356] D Grover, *The Protection of Computer Software—Its Technology and Applications*, Cambridge: British Computer Society/Cambridge University Press (1992), ISBN 0-521-42462-3.

[357] D Gruhl, W Bender, "Information Hiding to Foil the Casual Counterfeiter," in

*Proceedings of the Second International Workshop on Information Hiding* (Portland, Oregon, Apr 1998), Springer LNCS, v 1525, pp 1–15.

[358] LC Guillou, M Ugon, JJ Quisquater, "The Smart Card—A Standardized Security Device Dedicated to Public Cryptology," in [702], pp 561–613.

[359] C Gülcü, G Tsudik, "Mixing E-mail with Babel," in *Proceedings of the Internet Society Symposium on Network and Distributed System Security* (1996); proceedings published by the IEEE, ISBN 0-8186-7222-6, pp 2–16.

[360] R Gupta, SA Smolka, S Bhaskar, "On Randomization in Sequential and Distributed Algorithms," in *ACM Computing Surveys*, v 26 no 1 (Mar 1994), pp 7–86.

[361] J Gurnsey, *Copyright Theft*, Aslib (1997), ISBN 0-566-07631-4.

[362] P Gutman, "Secure Deletion of Data from Magnetic and Solid-State Memory," in *Sixth USENIX Security Symposium Proceedings* (July 1996), pp 77–89.

[363] P Gutman, "Software Generation of Practically Strong Random Numbers," in *Seventh USENIX Security Symposium Proceedings* (Jan 1998), pp 243–257.

[364] S Haber, WS Stornetta, "How to Time-Stamp a Digital Document," in *Journal of Cryptology*, v 3 no 2 (1991), pp 99–111.

[365] S Haber, WS Stornetta, "Secure Names for Bit-Strings," in *4th ACM Conference on Computer and Communications Security*; proceedings published by the ACM, ISBN 0-89791-912-2CCS 97, pp 28–35.

[366] W Hackmann, "Asdics at War," in *IEE Review*, v 46 no 3 (May 2000), pp 15–19.

[367] "Chris Carey Arrested in New Zealand," in *Hack Watch News* (Jan 1, 1999), at `http://www.iol.ie/~kooltek/legal.html`.

[368] N Hager, *Secret Power—New Zealand's Role in the International Spy Network*, Craig Potton Publishing (1996), ISBN 0-908802-35-8.

[369] 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.

[370] 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.

[371] R Hanley, "Millions in Thefts Plague New Jersey Area," in *The New York Times* (Feb 9, 1981), p A1.

[372] R Hanson, "Can Wiretaps Remain Cost-Effective?" in *Communications of the ACM*, v 37 no 12 (Dec 1994), pp 13–15.

[373] MA Harrison, ML Ruzzo, JD Ullman, "Protection in Operating Systems," in *Communications of the ACM*, v 19 no 8 (Aug 1976), pp 461–471.

[374] A Hassey, M Wells, "Clinical Systems Security—Implementing the BMA Policy and Guidelines," in [29], pp 79–94.

[375] 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.

[376] N Heintze, "Scalable Document Fingerprinting," in *Second USENIX Workshop on Electronic Commerce* (1996), ISBN 1-880446-83-9, pp 191–200.

[377] Herodotus, *Histories*, Book 1, 123.4, Book 5 35.3, and Book 7 239.3.

[378] "Interview with David Herson—SOGIS," (Sept 25, 1996), in *Ingeniørennet*, at http://www.ing.dk/redaktion/herson.htm.

[379] A Herzberg, M Jokabsson, S Jarecki, H Krawczyk, M Yung, "Proactive Public Key and Signature Systems," *4th ACM Conference on Computer and Communications Security* (1997), pp 100–110.

[380] RA Hettinga, "Credit Card Fraud Higher, Credit Card Fraud Lower," in nettime (Mar 22, 2000), at http://www.nettime.org/nettime.w3archive/200003/msg00184.html.

[381] M Hewish, "Combat ID Advances on All Fronts," in *International Defense Review*, v 29 (Dec 1996), pp 18–19.

[382] Hewlett-Packard, "IA-64 Instruction Set Architecture Guide," at http://devresource.hp.com/devresource/Docs/Refs/IA64ISA/index.html.

[383] HJ Highland, "Electromagnetic Radiation Revisited," in *Computers & Security*, v 5 (1986), pp 85–93, 181–184.

[384] 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.

[385] TF Himdi, RS Sandhu, "Lattice-Based Models for Controlled Sharing of Confidential Information in the Saudi Hąjj System," in *13th Annual Computer Security Applications Conference*, San Diego, CA (Dec 8–12, 1997); proceedings published by the IEEE Computer Society, ISBN 0-8186-8274-4; pp 164–174.

[386] J Hoffman, "Implementing RBAC on a Type-Enforced System," in *13th Annual Computer Security Applications Conference*, San Diego, CA (Dec 8–12, 1997); proceedings published by the IEEE Computer Society, ISBN 0-8186-8274-4; pp 158–163.

[387] P Hollinger, "Single Language for Barcode Babel," in *Financial Times* (July 25, 2000), p 15.

[388] C Holloway, "Controlling the Use of Cryptographic Keys," in *Computers and Security*, v 14 no 7 (1995), pp 587–598.

[389] DI Hopper, "Authorities Sue Adult Web Sites," in *The Washington Post* (Aug 23, 2000); at http://www.washingtonpost.com/.

[390] 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.

[391] 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 (1993), pp 279–290.

[392] 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.

[393] D Howell, "Counterfeit Technology Forges Ahead," in *The Daily Telegraph* (Mar 22, 1999), at http://www.telegraph.co.uk:80/.

[394] N Htoo-Mosher, R Nasser, N Zunic, J Straw, "E4 ITSEC Evaluation of PR/SM on ES/9000 Processors," in *19th National Information Systems Security Conference* (1996), proceedings published by MST, pp 1–11.

[395] Q Hu, JY Yang, Q Zhang, K Liu, XJ Shen, "An Automatic Seal Imprint Verification Approach," in *Pattern Recognition*, v 28 no 8 (Aug 1995), pp 251–266.

[396] G Huber, "CMW Introduction," in *ACM SIGSAC*, v 12 no 4 (Oct 1994), pp 6–10.

[397] 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/.

[398] "Role of Communications in Operation Desert Storm," *IEEE Communications Magazine*, Special Issue, v 30 no 1 (Jan 1992).

[399] *IEEE Carnahan Conference*, at http://www.carnahanconference.com/.

[400] *IEEE Electronics and Communications Engineering Journal*, v 12 no 3 (June 2000), special issue on UMTS.

[401] *IEEE Spectrum*, special issue on nuclear safekeeping, v 37 no 3 (Mar 2000).

[402] IFCI, "Real Cases," at http://risk.ifci.ch/Realcases.htm.

[403] "Ex-Radio Chief 'Masterminded' TV Cards Scam," in *The Independent* (Feb 17, 1998); see also, "The Sinking of a Pirate," *Sunday Independent* (Mar 1, 1998).

[404] Intel Corporation, *Intel Architecture Software Developer's Manual, Volume 1: Basic Architecture*, Order number 243190 (1997).

[405] "New England Shopping Mall ATM Scam Copied in UK," in *Information Security Monitor*, v 9 no 7 (June 1994), pp 1–2.

[406] "Pink Death Strikes at US West Cellular," in *Information Security Monitor*, v 9 no 2 (Jan 1994), pp 1–2.

[407] Information Systems Audit and Control Association, "Control Objectives for Information and related Technology," at http://www.isaca.org/cobit.htm.

[408] Information Systems Audit and Control Association, "Exam Preparation Materials," available from ISACA, at http://www.isaca.org/cert1.htm.

[409] International Atomic Energy Authority (IAEA), "The Physical Protection of Nuclear Material and Nuclear Facilities," INFCIRC/225/Rev. 4, at http://www.iaea.org/worldatom/program/protection/index.shtml.

[410] International Electrotechnical Commission, *Digital Audio Interface*, IEC 60958, Geneva (Feb 1989).

[411] I Jackson, personal communication with the author.

[412] L Jackson, "BT Forced to Pay Out Refunds after Free Calls Fraud," in *The Sunday Telegraph* (Feb 9, 1997); at `http://www.telegraph.co.uk:80/`.

[413] G Jagpal, "Steganography in Digital Images," undergraduate thesis, Selwyn College, Cambridge University (1995).

[414] AK Jain, R Bolle, S Pankanti, *Biometrics—Personal Identification in Networked Society*, Kluwer (1991), ISBN 0-7923-8346-1.

[415] AK Jain, L Hong, S Pankanti, R Bolle, "An Identity-Authentication System Using Fingerprints," in *Proceedings of the IEEE*, v 85 no 9 (Sept 1997), pp 1365–1388.

[416] S Jajodia, W List, G McGregor, L Strous (eds), *Integrity and Internal Control in Information Systems*, *Volume 1: Increasing the Confidence in Information Systems*, Chapman & Hall (1997), ISBN 0-412-82600-3.

[417] M Jay, "ACPO's Intruder Policy—Underwritten?" in *Security Surveyor*, v 26 no 3 (Sept 1995), pp 10–15.

[418] 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; also appeared at the Public Key Infrastructure Invitational Workshop at MITRE, VA (Sept 1995) and PKS '96 in Zürich (Oct 1, 1996).

[419] 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 1998), pp 495–509.

[420] John Young Architect, `http://www.jya.com`.

[421] K Johnson, "One Less Thing to Believe In: Fraud at Fake Cash Machine," in *The New York Times* (May 13, 1993), p 1.

[422] RG Johnson, ARE Garcia, "Vulnerability Assessment of Security Seals," in *Journal of Security Administration*, v 20 no 1 (June 1997), pp 15–27; `http://lib-www.lanl.gov/la-pubs/00418796.pdf`; more at `http://pearl1.lanl.gov/seals/`.

[423] P Jones, "Protection Money," in *Computer Business Review*, v 4 no 12 (Dec 1996), pp 31–36.

[424] RV Jones, *Most Secret War*, Wordsworth Editions (1978, 1998), ISBN 1-85326-699-X.

[425] RV Jones, "*Reflections on Intelligence*," Octopus (1989), ISBN 0-7493-0474-X.

[426] 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.

[427] *Dorothy Judd v Citibank*, 435 NYS, 2d series, pp 210–212, 107 Misc.2d 526.

[428] D Kahn, *The Codebreakers*, New York: Macmillan (1967).

[429] D Kahn, *Seizing the Enigma*, New York: Houghton Mifflin (1991), ISBN 0-395-42739-8.

[430] D Kahn, "Soviet Comint in the Cold War," in *Cryptologia*, v XXII no 1 (Jan 1998), pp 1–24.

[431] M Kam, G Fielding, R Conn, "Writer Identification by Professional Document Examiners," in *Journal of Forensic Sciences*, v 42 (1997), pp 778–786.

[432] 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.

[433] 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.

[434] MH Kang, IS Moskowitz, "A Pump for Rapid, Reliable, Secure Communications," in *1st ACM Conference on Computer and Communications Security* (Nov 3–5, 1993), Fairfax, VA; proceedings published by the ACM, ISBN 0-89791-629-8, pp 118–129.

[435] 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.

[436] MH Kang, IS Moskowitz, DC Lee, "A Network Pump," in *IEEE Transactions on Software Engineering*, v 22 no 5 (May 1996), pp 329–338.

[437] 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, (Dec 9–13, 1996); proceedings published by the IEEE, ISBN 0-8186-7606-X, pp 32–43.

[438] MH Kang, JN Froscher, IS Moskowitz, "An Architecture for Multilevel Secure Interoperability," in *13th Annual Computer Security Applications Conference*, San Diego, CA, (Dec 8–12, 1997); proceedings published by the IEEE Computer Society, ISBN 0-8186-8274-4; pp 194–204.

[439] CS Kaplan, "Privacy Plan Likely to Kick Off Debate," in *The New York Times* (July 28, 2000), at `http://www.nytimes.com/`.

[440] PA Karger, VA Austell, DC Toll, "*A New Mandatory Security Policy Combining Secrecy and Integrity*," IBM Research Report RC 21717 (97406) (Mar 15, 2000).

[441] F Kasiski, *Die Geheimschriften und die Dechiffrier-Kunst*, Berlin: Mittler & Sohn (1863).

[442] KASUMI Specification, ETSI/SAGE, v 1 (Dec 23, 1999), at `http://www.etsi.org/dvbandca/`.

[443] S Katzenbeisser, FAP Petitcolas, *Information Hiding—Techniques for Steganography and Digital Watermarking*, Artech House (2000), ISBN 1-58053-035-4.

[444] C Kaufman, R Perlman, M Speciner, *Network Security—Private Communication in a Public World*, Prentice Hall 1995, ISBN 0-13-061466-1.

[445] DT Keitkemper, SF Platek, KA Wolnik, "DNA versus Fingerprints," in *Journal of Forensic Sciences*, v 40 (1995), p 534.

[446] 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.

[447] 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.

[448] 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.

[449] R Kemmerer, C Meadows, J Millen, "Three Systems for Cryptographic Protocol Analysis," in *Journal of Cryptology*, v 7 no 2 (Spring 1994), pp 79–130.

[450] 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.

[451] 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.

[452] JO Kephardt, SR White, "Measuring and Modeling Computer Virus Prevalence," in *Proceedings of the 1993 IEEE Symposium on Security and Privacy*, pp 2–15.

[453] JO Kephardt, SR White, DM Chess, "Epidemiology of Computer Viruses," in *IEEE Spectrum*, v 30 no 5 (May 1993), pp 27–29.

[454] A Kerckhoffs, "La Cryptographie Militaire," in *Journal des Sciences Militaires* (Jan 9, 1883), pp 5–38; at `http://www.cl.cam.ac.uk/users/fapp2/kerckhoffs/`.

[455] PJ Kerry, "EMC in the New Millennium," in *Electronics & Communication Engineering Journal*, v 12 no 2, pp 43–48.

[456] 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.

[457] 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.

[458] J King, "Bolero—A Practical Application of Trusted Third-Party Services," in *Computer Fraud and Security Bulletin* (July 1995), pp 12–15.

[459] Kingpin, "iKey 1000 Administrator Access and Data Compromise," in *bugtraq* (July 20, 2000), at `http://www.L0pht.com/advisories.html`.

[460] DV Klein, "Foiling the Cracker: A Survey of, and Improvements to, UNIX

Password Security," *Proceedings of the USENIX Security Workshop*, Portland, OR: USENIX Association (Summer 1990); http://www.deter.com/unix/.

[461] RL Klevans, RD Rodman, *Voice Recognition*, Artech House (1997), ISBN 0-89006-927-1.

[462] 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 (Sept 1994), pp 82–89.

[463] N Koblitz, *A Course in Number Theory and Cryptography*, Springer Graduate Texts in Mathematics, no 114 (1987), ISBN 0-387-96576-9.

[464] ER Koch, J Sperber, *Die Datenmafia*, Rohwolt Verlag (1995), ISBN 3-499-60247-4.

[465] M Kochanski, "A Survey of Data Insecurity Devices," in *Cryptologia*, v IX no 1, pp 1–15.

[466] 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.

[467] 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.

[468] 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.

[469] 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.

[470] 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.

[471] A Kondi, R Davis, "Software Encryption in the DoD," in *20th National Information Systems Security Conference* (1997); proceedings published by NIST, pp 543–554.

[472] BJ Koops, "Crypto Law Survey," at http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm; see also his thesis "The Crypto Controversy: A Key Conflict in the Information Society," The Hague: Kluwer Law International (1999), ISBN 90-411-1143-3.

[473] DP Kormann, AD Rubin, "Risks of the Passport Single Signon Protocol," in *Computer Networks* (July 2000); at http://avirubin.com/vita.html .

[474] H Krawczyk, M Bellare, R Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104 (Feb 1997); at http://www.faqs.org/rfcs/rfc2104.html.

[475] HM Kriz, "Phreaking recognized by Directorate General of France Telecom," in *Chaos Digest* 1.03 (Jan 1993).

[476] I Krsul, EH Spafford, "Authorship Analysis: Identifying the Author of a Program," in *Computers and Security*, v 16 no 3 (1996), pp 233–257.

[477] 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.

[478] MG Kuhn, RJ Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," in *Proceedings of the Second International Workshop on Information Hiding* (Portland, Apr 1998), Springer LNCS, v 1525, pp 126–143.

[479] MG Kuhn, private communication with the author.

[480] R Kuhn, P Edfors, V Howard, C Caputo, TS Philips, "Improving Public Switched Network Security in an Open Environment," in *Computer* (Aug 1993), pp 32–35.

[481] "L0phtCrack 2.52 for Win95/NT," at `http://www.l0pht.com/l0phtcrack/`.

[482] RJ Lackey, DW Upmal, "Speakeasy: The Military Software Radio," in *IEEE Communications Magazine*, v 33 no 5 (May 1995), pp 56–61.

[483] 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, OR: Apr 1998), Springer LNCS, v 1525, pp 158–168.

[484] Lamarr/Antheil Patent Story Home Page, `http://www.ncafe.com/chris/pat2/index.html`; contains U.S. patent no 2,292,387 (HK Markey et al., Aug 11, 1942).

[485] G Lambourne, *The Fingerprint Story*, Harrap (1984), ISBN 0-245-53963-8.

[486] L Lamport, "Time, Clocks and the Ordering of Events in a Distributed System," in *Communications of the ACM*, v 21 no 7 (July 1978), pp 558–565.

[487] L Lamport, R Shostack, M Peace, "The Byzantine Generals' Problem," in *ACM Transactions on Programming Languages and Systems*, v 4 no 3 (1982), pp 382–401.

[488] B Lampson, "A Note on the Confinement Problem," in *Communications of the ACM*, v 16 no 10 (Oct 1973), pp 613–615.

[489] 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.

[490] 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 U.S. Crypto Policy," *Report of the ACM U.S. Public Policy Committee* (June 1994).

[491] R Landley, "Son of DIVX: DVD Copy Control," Motley Fool, `http://www.fool.com/portfolios/rulemaker/2000/rulemaker000127.htm`.

[492] 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.

[493] CE Landwehr, AR Bull, JP McDermott, WS Choi, "A Taxonomy of Computer Program Security Flaws, with Examples," U.S. Navy Report NRL/FR/5542–93-9591 (Nov 19, 1993).

[494] D Lane, "Where Cash is King," in *Banking Technology* (Oct 1992), pp 38–41.

[495] J Leake, "Workers Used Forged Passes at Sellafield," in *Sunday Times* (Apr 2, 2000), p 6.

[496] HC Lee, RE Guesslen (eds), *Advances in Fingerprint Technology*, Elsevier (1991), ISBN 0-444-01579-5.

[497] AK Lenstra, HW Lenstra, "The Development of the Number Field Sieve," in *Springer Lecture Notes in Mathematics*, v 1554 (1993), ISBN 0-387-57013-6.

[498] NG Leveson, *Safeware—System Safety and Computers*, Addison-Wesley (1994), ISBN 0-201-11972-2.

[499] A Lewcock, "Bodily Power," in *Computer Business Review*, v 6 no 2 (Feb 1998), pp 24–27.

[500] O Lewis, "Re: News: London Mailbomber Used the Net," post to `ukcrypto` mailing list (June 5, 2000), archived at `http://www.cs.ucl.ac.uk/staff/I.Brown/archives/ukcrypto/` and `http://www.chiark.greenend.org.uk/mailman/listinfo/ukcrypto`.

[501] "Minister Backs Phone Crime Initiative," *Lewisham Community News*, at `http://www.lewisham.gov.uk/templates/community/commdetails.cfm?file=2000071200.txt`.

[502] CC Lin, WC Lin, "Extracting Facial Features by an Inhibiting Mechanism Based on Gradient Distributions," in *Pattern Recognition*, v 29 no 12 (Dec 1996), pp 2079–2101.

[503] R Linde, "Operating Systems Penetration," *National Computer Conference*, AFIPS (1975), pp 361–368.

[504] JPMG Linnartz, "The 'Ticket' Concept for Copy Control Based on Embedded Signalling," *Fifth European Symposium on Research in Computer Security* (ESORICS 1998), Springer LNCS, v 1485, pp 257–274.

[505] JPMG Linnartz, M van Dijk, "Analysis of the Sensitivity attack against Electronic Watermarks in Images," in [59], pp 258–272.

[506] B Littlewood, "Predicting Software Reliability," in *Philosophical Transactions of the Royal Society of London*, A327 (1989), pp 513–527.

[507] WF Lloyd, *Two Lectures on the Checks to Population*, Oxford University Press (1833).

[508] Lockheed Martin, "Covert Surveillance Using Commercial Radio and Television Signals," at `http://silentsentry.external.lmco.com`.

[509] L Loeb, *Secure Electronic Transactions—Introduction and Technical Reference*, Artech House (1998), ISBN 0-89006-992-1.

[510] 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.

[511] WW Lowrance, "Privacy and Health Research," Report to the U.S. Secretary of Health and Human Services (May 1997).

[512] M Ludwig, *The Giant Black Book of Computer Viruses*, American Eagle Publishers (1995), ISBN 0-929408-10-1.

[513] AP Lutzker, "Primer on the Digital Millennium—What the Digital Millennium Copyright Act and the Copyright Term Extension Act Mean for the Library Community," Association of Research Libraries, at `http://www.arl.org/info/frn/copy/primer.html`.

[514] M Lyu, *Software Reliability Engineering*, IEEE Computer Society Press (1995), ISBN 0-07-039400-8.

[515] B Macq, "Special Issue: Identification and Protection of Multimedia Information," *Proceedings of the IEEE*, v 87 no 7 (July 1999).

[516] W Madsen, "Airline Passengers to Be Subject to Database Monitoring," in *Computer Fraud and Security Bulletin* (Mar 1997), pp 7–8.

[517] W Madsen, "Crypto AG: The NSA's Trojan Whore?" in *Covert Action Quarterly* (Winter 1998), at `http://www.mediafilter.org/caq/cryptogate/`.

[518] W Madsen, "Government-Sponsored Computer Warfare and Sabotage," in *Computers and Security*, v 11 (1991), pp 233–236.

[519] 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.

[520] K Maguire, "Muckraker Who Feeds Off Bins of the Famous," in *The Guardian* (July 27, 2000), at `http://www.guardianunlimited.co.uk/Labour/Story/0,2763,347535,00.html`.

[521] S Maguire, *Debugging the Development Process*, Redmond, WA: Microsoft Press, ISBN 1-55615-650-2 (1994), p 50.

[522] 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 1997), pp 27–40.

[523] L Marks, *Between Silk and Cyanide—A Codemaker's War 1941–1945*, New York: HarperCollins (1998), ISBN 0-68486780-X.

[524] D Martin, "Internet Anonymizing Techniques," in `;login:` Magazine, (May 1998); at `http://www.usenix.org/publications/login/1998-5/martin.html`.

[525] B Masuda, "Reducing the Price of Convenience," *International Security Review*, no 82 (Autumn 1993), pp 45–48.

[526] M Matsui, "Linear Cryptanalysis Method for DES Cipher," in *Advances in Cryptology—Eurocrypt 93*, Springer LNCS, v 765, pp 386–397.

[527] M Matsui, "New Block Encryption Algorithm MISTY," in *Fourth International*

*Workshop on Fast Software Encryption* (1997), Springer LNCS, v 1267, pp 54–68.

[528] Gospel according to St. Matthew, Chapter 7, verse 3.

[529] R Matthews, "The Power of One," in *New Scientist* (Oct 7, 1999), pp 26–30; at http://www.newscientist.com/ns/19990710/thepowerof.html.

[530] 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.

[531] 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.

[532] J McCormac, "*European Scrambling Systems—The Black Book*," version 5, Waterford University Press, Ireland (1996), ISBN 1-873556-22-5.

[533] D McCullagh, "U.S. to Track Crypto Trails," in *Wired* (May 4, 2000), at http://www.wired.com/news/politics/0,1283,36067,00.html; statistics at http://www.uscourts.gov/wiretap99/contents.html.

[534] 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.

[535] K McCurley, Remarks at IACR General Meeting, *Crypto 98*, Santa Barbara, CA: (Aug 1998).

[536] AD McDonald, MG Kuhn, "StegFS: A Steganographic File System for Linux," in [613], pp 463–477.

[537] G McGraw, EW Felten, *Java Security*, New York: John Wiley & Sons, Inc. (1997), ISBN 0-471-17842-X.

[538] I McKie, "Total Vindication for Shirley McKie!" (June 23, 2000), at http://onin.com/fp/mckievindication.html.

[539] J McLean, "The Specification and Modeling of Computer Security," in *Computer*, v 23 no 1 (Jan 1990), pp 9–16.

[540] J McLean, "Security Models," in *Encyclopedia of Software Engineering*, New York: John Wiley & Sons, Inc. (1994).

[541] 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.

[542] J McNamara, "The Complete, Unofficial TEMPEST Information Page," at http://www.eskimo.com/~joelm/tempest.html.

[543] B McWilliams, "Sex Sites Accused of Gouging Visitors with Phone Scam," in InternetNews.com (Apr 7, 2000), at http://www.internetnews.com/bus-news/print/0,,3_337101,00.html.

[544] 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/.

[545] 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.

[546] 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.

[547] TS Messergues, EA Dabish, RH Sloan, "Investigations of Power Analysis Attacks on Smartcards," in *USENIX Workshop on Smartcard Technology;* proceedings published by USENIX (1999), ISBN 1-880446-34-0, pp 151–161.

[548] CH Meyer and SM Matyas, *Cryptography: A New Dimension in Computer Data Security*, New York: John Wiley & Sons, Inc. (1982).

[549] 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, ISBN 3-540-41455-X, pp 78–92.

[550] J Micklethwait, A Wooldridge, *The Witch Doctors—What the Management Gurus Are Saying, Why It Matters and How to Make Sense of It*, New York: Random House (1997), ISBN 0-7493-2645-X.

[551] A Midgley, "R.I.P. and NHSNet," post to `ukcrypto` mailing list (July 1, 2000), archived at `http://www.cs.ucl.ac.uk/staff/I.Brown/archives/ukcrypto/`.

[552] J Millen, "A Resource Allocation Model for Denial of Service Protection," in *Journal of Computer Security*, v 2 nos 2–3 (1993), pp 89–106.

[553] B Miller, "Vital Signs of Security," in *IEEE Spectrum* (Feb 1994), pp 22–30.

[554] 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.

[555] K Mitnick, Congressional testimony, as reported by Associated Press (Mar 3, 2000); 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`.

[556] B Moghaddam, A Pentland, "Probabilistic Visual learning for Object Representation," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, v 19 no 7 (July 1997), pp 696–710.

[557] F Mollet, "Card Fraud Nets Esc6 billion," in *Cards International* (Sept 22, 1995), p 3.

[558] 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`.

[559] R Morris, "A Weakness in the 4.2BSD UNIX TCP/IP Software," Bell Labs

Computer Science Technical Report no. 117 (Feb 25, 1985); at http://www.cs.berkeley.edu/~daw/security/seq-attack.html.

[560] R Morris, Invited talk, *Crypto 95*.

[561] R Morris, K Thompson, "Password Security: A Case History," in *Communications of the ACM*, v 22 no 11 (Nov 1979), pp 594–597.

[562] DP Moynihan, *Secrecy—The American Experience*, New Haven, CT: Yale University Press (1999), ISBN 0-300-08079-4.

[563] 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.

[564] 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.

[565] S Mullender (ed), *Distributed Systems*, Addison-Wesley (1993), ISBN 0-201-62427-3.

[566] 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.

[567] E Murray, "SSL Server Security Survey," at http://www.meer.net/~ericm/papers/ssl_servers.html.

[568] K Murray, "Protection of Computer Programs in Ireland," in *Computer Law and Security Report*, v 12 no 3 (May/June 1996), pp 57–59.

[569] RFH Nalder, *History of the Royal Corps of Signals*, Royal Signals Institution (1958).

[570] Napster, http://www.napster.com.

[571] M Nash, R Kennett, "Implementing Security Policy in a Large Defense Procurement," in *12th Annual Computer Security Applications Conference*, San Diego, CA (Dec 9–13, 1996); proceedings published by the IEEE, ISBN 0-8186-7606-X; pp 15–23.

[572] National Information Infrastructure Task Force, "Options for Promoting Privacy on the National Information Infrastructure" (Apr 1997), at http://www.iitf.nist.gov/ipc/privacy.htm.

[573] National Institute of Standards and Technology, archive of publications on computer security, http://csrc.nist.gov/publications/history/index.html.

[574] National Institute of Standards and Technology, "Common Criteria for Information Technology Security," Version 2.0/ISO IS 15408 (May 1998), http://www.commoncriteria.org.

[575] National Institute of Standards and Technology, "Data Encryption Standard (DES)," FIPS 46; Draft FIPS 46-3, incorporating upgrade to triple DES, at http://csrc.nist.gov/encryption/.

[576] National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules" (Jan 11, 1994), at http://www.itl.nist.gov/fipspubs/0-toc.htm#cs.

[577] National Institute of Standards and Technology, "SKIPJACK and KEA Algorithms," (June 23, 1998), at http://csrc.nist.gov/encryption/skipjack-kea.htm.

[578] National Institute of Standards and Technology, "Escrowed Encryption Standard," FIPS 185 (Feb 1994).

[579] National Institute of Standards and Technology, "SCSUG Smart Card Protection Profile" (draft, v 2.0, May 2000), at http://csrc.nist.gov/cc/sc/sclist.htm.

[580] National Research Council, *Cryptography's Role in Securing the Information Society*, National Academy Press (1996), ISBN 0-309-05475-3.

[581] National Research Council, *For the Record: Protecting Electronic Health Information*, National Academy Press (1997), ISBN 0-309-05697-7.

[582] National Security Agency, "The NSA Security Manual," at http://www.cl.cam.ac.uk/ftp/users/rja14/nsaman.tex.gz.

[583] P Naur, B Randell, "Software Engineering—Report on a Conference," NATO Scientific Affairs Division, Garmisch (1968).

[584] R Neame, "Managing Health Data Privacy and Security," in [29], pp 225–232.

[585] GC Necula, P Lee, "Safe, Untrusted Agents Using Proof-Carrying Code," in *Mobile Agents and Security*, ISBN 3-540-64792-9, pp 61–91.

[586] RM Needham, "Denial of Service: An Example," in *Communications of the ACM*, v 37 no 11 (Nov 1994), pp 42–46.

[587] RM Needham, "Naming," in [565], pp 318–327.

[588] RM Needham, "The Hardware Environment," in *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, p 236.

[589] RM Needham, MD Schroeder, "Using Encryption for Authentication in Large Networks of Computers," in *Communications of the ACM*, v 21 no 12 (Dec 1978), pp 993–999.

[590] P Neumann, *Computer-Related Risks*, Addison-Wesley (1995), ISBN 0-201-55805-X.

[591] J Newton, "Countering the Counterfeiters," in *Cards International* (Dec 12, 1994), p 12.

[592] J Newton, "Organised Plastic Counterfeiting," Her Majesty's Stationery Office (1996), ISBN 0-11-341128-6.

[593] Nuclear Regulatory Commission, www.nrc.gov.

[594] AM Odlyzko, "The History of Communications and Its Implications for the Internet," at http://www.research.att.com/~amo/doc/networks.html.

[595] 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.

[596] N Okuntsev, *Windows NT Security*, R&D Books (1999), ISBN 0-87930-473-1.

[597] R Oppliger, *Internet and Intranet Security*, Artech House (1998), ISBN 0-89006-829-1.

[598] Organization for Economic Cooperation & 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.

[599] J Osen, "The Cream of Other Men's Wit: Plagiarism and Misappropriation in Cyberspace," in *Computer Fraud and Security Bulletin* (Nov 1997), pp 13–19.

[600] S Pancho, "Paradigm Shifts in Protocol Analysis," in *Proceedings of the 1999 New Security Paradigms Workshop*, ACM (2000), pp 70–79.

[601] DJ Parker, "DVD Copy Protection: An Agreement At Last? Protecting Intellectual Property Rights in the Age of Technology," in *Tape/Disc Magazine* (Oct 1996), http://www.kipinet.com/tdb/tdb_oct96/feat_protection.html.

[602] DJ Parker, *Fighting Computer Crime—A New Framework for Protecting Information*, New York: John Wiley & Sons, Inc. (1998), ISBN 0-471-16378-3.

[603] B Patterson, letter to *Communications of the ACM*, v 43 no 4 (Apr 2000), pp 11–12.

[604] 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.

[605] TP Pedersen, "Electronic Payments of Small Amounts," in *Security Protocols* (1996), Springer LNCS, v 1189, pp 59–68.

[606] A Perrig, "A Copyright Protection Environment for Digital Images," Diploma thesis, École Polytechnique Fédérale de Lausanne (1997).

[607] 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.

[608] R Petersen, "UCITA Update," at http://www.arl.org/info/frn/copy/petersen.html.

[609] I Peterson, "From Counting to Writing," MathLand Archives, http://www.maa.org/mathland/mathland_2_24.html.

[610] 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.

[611] FAP Petitcolas, RJ Anderson, MG Kuhn, "Information Hiding—A Survey," in *Proceedings of the IEEE*, v 87 no 7 (July 1999), pp 1062–1078.

[612] H Petroski, *To Engineer Is Human*, New York: Barnes and Noble Books (1994), ISBN 1-56619502-0.

[613] A Pfitzmann, *Proceedings of the Third International Workshop on Information Hiding* (1999), Springer LNCS, v 1768.

[614] B Pfitzmann, "Information Hiding Terminology," in *Proceedings of the First International Workshop on Information Hiding* (1996), Springer LNCS, v 1174, pp 347–350.

[615] 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.

[616] 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.

[617] RL Pickholtz, DB Newman, YQ Zhang, M Tatebayashi, "Security Analysis of the INTEL-SAT VI and VII Command Network," in *IEEE Proceedings on Selected Areas in Communications*, v 11 no 5 (June 1993), pp 663–672.

[618] D Polak, "GSM Mobile Network in Switzerland Reveals Location of Its Users," in *Privacy Forum Digest*, v 6 no 18 (Dec 31, 1997), at `http://www.vortex.com/privacy/priv.06.18`.

[619] Politech mailing list, at `http://www.politechbot.com/`.

[620] B Pomeroy, S Wiseman, "Private Desktops and Shared Store," in *Computer Security Applications Conference*, Phoenix, AZ (1998); proceedings published by the IEEE, ISBN 0-8186-8789-4, pp 190–200.

[621] 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.

[622] RS Pressman, *Software Engineering: A Practitioner's Approach*, New York: McGraw-Hill (5th ed, 2000), ISBN 0-073-65578-3.

[623] G Price, "The Interaction between Fault Tolerance and Security," Technical Report no 214, Cambridge University Computer Laboratory.

[624] 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.

[625] H Pringle, "The Cradle of Cash," in *Discover*, v 19 no 10 (Oct 1998); at `http://www.discover.com/oct_issue/cradle.html`.

[626] C Prins, "Biometric Technology Law," in *The Computer Law and Security Report*, v 14 no 3 (May/Jun 1998), pp 159–165.

[627] D Pritchard, *The Radar War—Germany's Pioneering Achievement 1904–1945*, Wellingborough (1989), ISBN 1-85260-246-5.

[628] The Privacy Exchange, `http://www.privacyexchange.org/`.

[629] Public Lending Right (PLR), at http://www.writers.org.uk/guild/Crafts/Books/PLRBody.html.

[630] Public Record Office, "Functional Requirements for Electronic Record Management Systems," (Nov 1999), at http://www.pro.gov.uk/recordsmanagement/eros/invest/reference.pdf.

[631] Rain Forest Puppy, "Issue Disclosure Policy V1.1," at http://www.wiretrip.net/rfp/policy.html.

[632] W Rankl, W Effing, *Smartcard Handbook*, New York: John Wiley & Sons, Inc. (1997), ISBN 0-471-96720-3; translated from the German *Handbuch der Chpkarten*, Carl Hanser Verlag (1995), ISBN 3-446-17993-3.

[633] ES Raymond, "The Case of the Quake Cheats," (Dec 27, 1999), at http://www.tuxedo. org/~esr/writings/quake-cheats.html.

[634] ES Raymond, "The Cathedral and the Bazaar," at http://www.tuxedo.org/~esr/writings/cathedral-bazaar/.

[635] ES Raymond, "The Magic Cauldron," (June 1999), at http://www.tuxedo.org/~esr/writings/magic-cauldron/magic-cauldron.html.

[636] SM Redl, MK Weber, MW Oliphant, *GSM and Personal Communications Handbook*, Artech House (1998), ISBN 0-89006-957-3.

[637] MG Reed, PF Syverson, DM Goldschlag, "Anonymous Connections and Onion Routing," in *IEEE Journal on Special Areas in Communications*, v 16 no 4 (May 1998), pp 482–494.

[638] C Reiss, "Mystery of Levy Tax Phone Calls," *The Evening Standard* (July 5, 2000), p 1; also at http://www.thisislondon.com/.

[639] MK Reiter, "A Secure Group Membership Protocol," in *IEEE Transactions on Software Engineering*, v 22 no 1 (Jan 1996), pp 31–42.

[640] MK Reiter, MK Franklin, JB Lacy, RA Wright, "The Omega Key Management Service," in *3rd ACM Conference on Computer and Communications Security* (1996), pp 38–47.

[641] M Reiter, AD Rubin, "Anonymous Web Transactions with Crowds," in *Communications of the ACM*, v 42 no 2 (Feb 1999), pp 32–38.

[642] J Reno, http://www.cnn.com/2000/US/05/25/security.breaches.01/index.html.

[643] MA Rice, AJ Sammes, *Command and Control: Support Systems in the Gulf War*, Brassey's (1994), ISBN 1-8575 3-015-2.

[644] D Richardson, *Techniques and Equipment of Electronic Warfare*, Salamander Books, ISBN 0-8601-265-8.

[645] LW Ricketts, JE Bridges, J Miletta, *EMP Radiation and Protective Techniques*, John Wiley & Sons, Inc. New York (1975), ISBN 0-471-010403-6.

[646] M Ridley, "The Red Queen: Sex and the Evolution of Human Nature," New York: Viking Books (1993), ISBN 0-1402-4548-0.

[647] V Rijmen, *The block cipher Rijndael*, at `http://www.esat.kuleuven.ac.be/~rijmen/rijndael/`.

[648] RL Rivest, A Shamir, "PayWord and MicroMint: Two Simple Micropayment Schemes," in *Security Protocols* (1996), Springer LNCS, v 1189, pp 69–87.

[649] 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.

[650] AR Roddy, JD Stosz, "Fingerprint Features—Statistical Analysis and System Performance Estimates," in *Proceedings of the IEEE*, v 85 no 9 (Sept 1997), pp 1390–1421.

[651] DE Ross, "Two Signatures," in `comp.risks`, v 20.81: `http://catless.ncl.ac.uk/Risks/20.81.html`.

[652] M Rowe, "Card Fraud Plummets in France," *Banking Technology* (May 1994), p 10.

[653] WW Royce, "Managing the Development of Large Software Systems: Concepts and Techniques," in *Proceedings IEEE WESCON* (1970), pp 1–9.

[654] A Rubin, "Bugs in Anonymity Services," bugtraq (Apr 13, 1999); at `http://www.securityportal.com/list-archive/bugtraq/1999/Apr/0126.html`.

[655] HH Rubinovitz, "Issues Associated with Porting Applications to the Compartmented Mode Workstation," in *ACM SIGSAC*, v 12 no 4 (Oct 1994), pp 2–5.

[656] RA Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag (1986), ISBN 0-387-16870-2.

[657] 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*, Rome: Fondazione Ugo Bordoni (1993), pp 191–198.

[658] R Ruffin, "Following the Flow of Funds," in *Security Management* (July 1994), pp 46–52.

[659] J Rushby, B Randell, "A Distributed Secure System," in *IEEE Computer*, v 16 no 7 (July 1983), pp 55–67.

[660] D Russell, GT Gangemi, "Computer Security Basics," Chapter 10: *TEMPEST*, O'Reilly & Associates (1991), ISBN 0-937175-71-4.

[661] 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.

[662] 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.

[663] RG Saltman, "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`.

[664] T Sammes, B Jenkinson, *Forensic Computing—A Practitioner's Guide*, Springer (2000), ISBN 1-85233-299-9.

[665] P Samuelson, "Copyright and Digital Libraries," in *Communications of the ACM*, v 38 no 4 (April 1995).

[666] P Samuelson, "Intellectual Property Rights and the Global Information Economy," in *Communications of the ACM*, v 39 no 1 (Jan 1996), pp 23–28.

[667] P Samuelson, "The Copyright Grab," at `http://uainfo.arizona.edu/~weisband/411_511/copyright.html`.

[668] D Samyde, JJ Quisquater, "S.E.M.A. Electromagnetic Analysis," *presented at the rump session of Eurocrypt 2000*.

[669] RS Sandhu, S Jajodia, "Polyinstantiation for Cover Stories," in *Computer Security—ESORICS 92*, LNCS, v 648, pp 307–328.

[670] SANS Institute, "Consensus List of the Top Ten Internet Security Threats," v 1.22 (June 19, 2000); at `http://www.sans.org/`.

[671] 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`.

[672] PF Sass, L Gorr, "Communications for the Digitized Battlefield of the 21st Century," in *IEEE Communications*, v 33 no 10 (Oct 1995), pp 86–95.

[673] M Schaefer, "Symbol Security Condition Considered Harmful," in *Proceedings of the 1989 IEEE Symposium on Security and Privacy*, pp 20–46.

[674] 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.

[675] RR Schell, PJ Downey, GJ Popek, "Preliminary Notes on the Design of Secure Military Computer Systems," Electronic Systems Division, Air Force Systems Command (Jan 1, 1973), MCI-73-1; at `http://seclab.cs.ucdavis.edu/projects/history/papers/sche73.pdf`.

[676] DL Schilling, *Meteor Burst Communications: Theory and Practice*, New York: John Wiley & Sons, Inc. (1993), ISBN 0-471-52212-0.

[677] DC Schleher, *Electronic Warfare in the Information Age*, Artech House (1999), ISBN 0-89006-526-8.

[678] 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`.

[679] ZE Schnabel, "The Estimation of the Total Fish Population in a Lake," in *American Mathematical Monthly*, v 45 (1938), pp 348–352.

[680] PM Schneider, "Datenbanken mit genetischen Merkmalen von Straftätern," in *Datenschutz und Datensicherheit*, v 22 (June 1998), pp 330–333.

[681] B Schneier, *Applied Cryptography*, New York: John Wiley & Sons, Inc. (1996); ISBN 0-471-12845-7.

[682] B Schneier, "Why Computers Are Insecure," in `comp.risks` v 20.67; at `http://catless.ncl.ac.uk/Risks/20.67.html`.

[683] B Schneier, *Secrets and Lies: Digital Security in a Networked World*, New York: John Wiley & Sons, Inc. (2000); ISBN 0-471-25311-1.

[684] B Schneier, D Banisar, *The Electronic Privacy Papers—Documents on the Battle for Privacy in the Age of Surveillance*, New York: John Wiley & Sons, Inc. (1997); ISBN 0-471-12297-1.

[685] M Schnyder, "Datenfluesse im Gesundheitswesen," in *Symposium für Datenschutz und Informationssicherheit*, Zuerich (Oct 1998).

[686] RA Scholtz, "Origins of Spread-Spectrum Communications," in *IEEE Transactions on Communications*, v TC-30 no 5 (May 1982), pp 822–854.

[687] MD Schroeder, "Cooperation of Mutually Suspicious Subsystems in a Computer Utility," MIT PhD Thesis (Sept 1972); also available as Project MAC Technical Report MAC TR-104, `http://hdl.handle.net/ncstrl.mit_lcs/MIT/LCS/TR-104`.

[688] CJ Seiferth, "Opening the Military to Open Source," in *COTS Magazine* (Nov-Dec 1999), at `http://www.rtcgroup.com/cotsjournal/cotsj111200/cots111200.html`.

[689] CJ Seiferth, "Adoption of Open Licensing," in *COTS Magazine* (Nov-Dec 1999), at `http://www.rtcgroup.com/cotsjournal/cotsj111200/cots111200.html`.

[690] R Senderek, "Key-Experiments—How PGP Deals with Manipulated Keys," at `http://senderek.de/security/key-experiments.html`.

[691] D Senie, "Changing the Default for Directed Broadcasts in Routers," RFC 2644, at `http://www.ietf.org/rfc/rfc2644.txt`.

[692] A Shamir, "How to Share a Secret," in *Communications of the ACM*, v 22 no 11 (Nov 1979), pp 612–613.

[693] MI Shamos, "Electronic Voting—Evaluating the Threat," in *Computers, Freedom, and Privacy* (1993); at `http://www.cpsr.org/conferences/cfp93/shamos.html`.

[694] CE Shannon, "A Mathematical Theory of Communication," in *Bell Systems Technical Journal*, v 27 (1948), pp 379–423, 623–656.

[695] CE Shannon, "Communication Theory of Secrecy Systems," in *Bell Systems Technical Journal*, v 28 (1949), pp 656–715.

[696] C Shapiro, H Varian, *Information Rules*, Boston: Harvard Business School Press (1998), ISBN 0-87584-863-X; see `http://www.inforules.com`.

[697] D Sherwin, "Fraud—The Unmanaged Risk," in *Financial Crime Review*, v 1 no 1 (Fall 2000), pp 67–69.

[698] 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.

[699] 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 1996), pp 283–293.

[700] GJ Simmons, "The Prisoners' Problem and the Subliminal Channel," in *Proceedings of CRYPTO '83*, Plenum Press (1984), pp 51–67.

[701] GJ Simmons, "How to Insure That Data Acquired to Verify Treaty Compliance Are Trustworthy," in *Proceedings of the IEEE*, v 76 no 5 (1988); reprinted as a chapter in [702]).

[702] GJ Simmons (ed), *Contemporary Cryptology—The Science of Information Integrity*, IEEE Press (1992), ISBN 0-87942-277-7.

[703] GJ Simmons, "A Survey of Information Authentication," in [702], pp 379–439.

[704] GJ Simmons, "An Introduction to Shared Secret and/or Shared Control Schemes and Their Application," in [702], pp 441–497.

[705] GJ Simmons, invited talk at the *1993 ACM Conference on Computer and Communications Security*, Fairfax, VA (Nov 3–5, 1993).

[706] GJ Simmons, "Subliminal Channels: Past and Present," in *European Transactions on Telecommunications*, v 5 no 4 (July/Aug 1994), pp 459–473.

[707] GJ Simmons, "The History of Subliminal Channels," in *IEEE Journal on Selected Areas in Communications*, v 16 no 4 (April 1998), pp 452–462.

[708] DR Simon, "Anonymous Communication and Anonymous Cash," in *Advances in Cryptology—Crypto 96*, Springer LNCS, v 1109, pp 61–73.

[709] WA Simpson, "Electronic Signatures Yield Unpleasant Surprises," (June 23, 2000), at `http://cryptome.org/esigs-suck.htm`.

[710] A Sipress, "Tracking Traffic by Cell Phone Maryland, Virginia to Use Transmissions to Pinpoint Congestion," in *The Washington Post* (Dec 22, 1999), p A1, at `http://www.washingtonpost.com/`.

[711] KS Siyan, J Casad, J Millecan, D Yarashus, P Tso, J Shoults, *Windows NT Server 4—Professional Reference*, New Riders Publishing (1996).

[712] SP Skorobogatov, "Low Temperature Remanence in Static RAM" (*to appear*).

[713] Smartcard Developer Association, `http://www.scard.org/gsm/`.

[714] "Plastic Card Fraud Rises in the UK," in *Smart Card News*, v 6 no 3 (Mar 1997), p 45.

[715] RE Smith, "Constructing a High-Assurance Mail Guard," in *17th National Computer Security Conference* (Oct 11–14, 1994), Baltimore, MD; proceedings published by NIST, pp 247–253.

[716] RM Smith, "Problems with Web Anonymizing Services," (Apr 15, 1999), at `http://www.tiac.net/users/smiths/anon/anonprob.htm`.

[717] SP Smith, H Perrit, H Krent, S Mencik, JA Crider, MF Shyong, LL Reynolds, *Independent Technical Committee Review of the Carnivore System—Draft report*, U.S. Department of Justice Contract No. 00-C-0238 IITRI, CR-022-216 (Nov 17, 2000), at `http://cryptome.org/carnivore.rev.htm`.

[718] S Smith, S Weingart, "Building a High-Performance, Programmable Secure Coprocessor," IBM Technical report RC 21102, available at `http://www.ibm.com/security/cryptocards/`.

[719] Peter Smulders, "The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables," in *Computers & Security*, v 9 (1990), pp 53–58.

[720] A Solomon, "A Brief History of PC Viruses," in *Computer Fraud and Security Bulletin* (Dec 1993), pp 9–19.

[721] A Solomon, Seminar given at Cambridge University Computer Laboratory (May 30, 2000).

[722] P Sommer, "Intrusion Detection and Legal Proceedings," in *Recent Advances in Intrustion Detection* (RAID) (1998), at `http://www.zurich.ibm.com/~dac/Prog_RAID98/Full_Papers/Sommer_text.pdf`.

[723] 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`.

[724] E Spafford, "The Internet Worm Program: An Analysis," in *Computer Communications Review*, v 19 no 1 (Jan 1989), pp 17–57.

[725] EH Spafford, "OPUS: Preventing Weak Password Choices," in *Computers and Security*, v 11 no 3 (1992), pp 273–278.

[726] "Tip von Urmel," in *Spiegel Magazine*, no 38 (Sept 11, 1995).

[727] J Spolsky, "Does Issuing Passports Make Microsoft a Country?" at `http://joel.editthispage.com/stories/storyReader$139`.

[728] "Your Car Radio May Be Revealing Your Tastes," in *St. Petersburg Times* (Jan 31, 2000), at `http://www.sptimes.com/News/013100/Technology/Your_car_radio_may_be.shtml`.

[729] T Standage, *The Victorian Internet*, Phoenix Press (1999), ISBN 0-75380-703-3.

[730] F Stajano, personal communication with the author.

[731] F Stajano, RJ Anderson, "The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks," in *Security Protocols—7th International Workshop*, Springer LNCS, v 1796, pp 172–182.

[732] F Stajano, RJ Anderson, "The Cocaine Auction Protocol—On the Power of Anonymous Broadcast," in [613], pp 434–447.

[733] WA Steer, "VideoDeCrypt," at `http://www.ucl.ac.uk/~ucapwas/vdc/`.

[734] P Stein, P Feaver, *Assuring Control of Nuclear Weapons*, University Press (1987) quoted in [92].

[735] 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/`.

[736] N Stephenson, *Snow Crash*, New York: Bantam Doubleday Dell (1992), ISBN 0-553-38095-8.

[737] FA Stevenson, "Cryptanalysis of Contents Scrambling System," at `http://www.derfrosch.de/decss/`.

[738] DR Stinson, *Cryptography—Theory and Practice*, CRC Press (1995); ISBN 0-8493-8521-0.

[739] "Watching Them, Watching Us—UK CCTV Surveillance Regulation Campaign," at http://www.spy.org.uk/.

[740] R Strehle, *Verschlüsselt—Der Fall Hans Bühler*, Werd Verlag (1994), ISBN 3-85932-141-2.

[741] K Stumper, "DNA-Analysen und ein Recht auf Nichtwissen," in *Datenschutz und Datensicherheit*, v 19 no 9 (Sept 1995), pp 511–517.

[742] Suetonius (Gaius Suetonius Tranquillus), *Vitae XII Caesarum*, *translated into English as History of Twelve Caesars*, by Philemon Holland, 1606; Nutt (1899).

[743] D Sutherland, "A Model of Information," in *9th National Computer Security Conference (1986)*, pp 175–183.

[744] L Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality," in *Journal of Law*, *Medicine*, *and Ethics*, v 25 nos 2–3 (1997), pp 98–110.

[745] S Tendler, N Nuttall, "Hackers Run Up £1m Bill on Yard's Phones," in *The London Times* (Aug 5, 1996); at http://www.the-times.co.uk/.

[746] K Thompson, "Reflections on Trusting Trust," in *Communications of the ACM*, v 27 no 8 (Aug 1984), pp 761–763; at http://www.acm.org/classics/sep95/.

[747] J Ticehurst, "Barclays Online Bank Suffers Another Blow" (Aug 11, 2000), at http://www.vnunet.com/News/1108767.

[748] 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.

[749] JW Toigo, *Disaster Recovery Planning for Computers and Communication Resources*, New York: John Wiley & Sons, Inc. (1996), ISBN 0-471-12175-4.

[750] C Tomlinson, "*Rudimentary Treatise on the Construction of Locks*," (1853) excerpt at http://www.deter.com/unix/papers/treatise_locks.html.

[751] Transactional Records Access Clearinghouse, "TRACFBI," at http://trac.syr.edu/tracfbi/index.html.

[752] M Trombly, "VISA Issues 10 'Commandments' for Online Merchants," in *Computerworld* (Aug 11, 2000), at http://www.computerworld.com/cwi/story/0,1199,NAV47_STO48487,00.html.

[753] JD Tygar, BS Yee, N Heintze, "Cryptographic Postage Indicia," in *Concurrency and Parallelism*, *Programming*, *Networking*, *and Security*, Springer-Verlag, (Dec 1996), pp 378–391, at http://buffy.eecs.berkeley.edu/~tygar/recommend.html.

[754] R Uhlig, "BT Admits Staff Could Have Fiddled System to Win Concorde Trip," in *The Daily Telegraph* (July 23, 1997), at http://www.telegraph.co.uk:80/.

[755] ukcrypto mailing list, at http://www.chiark.greenend.org.uk/mailman/listinfo/ukcrypto.

[756] Underwriters' Laboratories, http://www.ul.com.

[757] J Ungoed-Thomas, A Lorenz, "French Play Dirty for £1bn Tank Deal," in *The Sunday Times* (Aug 6, 2000), p 5.

[758] United Kingdon Government, "e-commerce@its.best.uk," at http://www.e-envoy.gov.uk/2000/strategy/strategy.htm.

[759] United States Code—U.S. Federal Law, online for example at http://www4.law.cornell.edu/uscode/.

[760] 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 (Aug 15, 2000), at http://pacer.cadc.uscourts.gov/common/opinions/200008/99-1442a.txt.

[761] United States Senate Select Committee on Intelligence, *CIA Office of Inspector General Investigations Staff Report on the Improper Handling of Classified Information by John M. Deutch*, 106th Congress, at http://intelligence.senate.gov/igreport.pdf.

[762] UPI newswire item, Oklahoma distribution (Nov 26, 1983), Tulsa, OK.

[763] 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/.

[764] 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.

[765] R van Renesse, *Optical Document Security* (2nd ed), Artech House (1997), ISBN 0-89006-982-4.

[766] 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.

[767] H van Vliet, *Software Engineering—Principles and Practice*, 2nd ed, New York: John Wiley & Sons, Inc. (2000), ISBN 0-471-97508-7.

[768] R van Voris, "Black Box Car Idea Opens Can of Worms," in *Law News Network* (June 4, 1999), at http://www.lawnewsnetwork.com/stories/A2024-1999Jun4.html.

[769] G Vanneste, J Degraeve, "Initial Report on Security Requirements," in [56].

[770] HR Varian, *Intermediate Microeconomics—A Modern Approach*, 5 ed, New York: W. W. Norton (1999), ISBN 0-393-97370-0.

[771] HR Varian, "Managing Online Security Risks," in *The New York Times* (June 1, 2000); at http://www.nytimes.com/library/financial/columns/060100econ-scene.html.

[772] 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.

[773] S Vaudenay, "FFT-Hash-II Is Not Yet Collision-Free," in *Laboratoire d'Informatique de l'Ecole Normale Supérieure report LIENS-92-17*.

[774] W Venema, "Murphy's Law and Computer Security," in *USENIX Security 96*, pp 187–193.

[775] 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`.

[776] 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`.

[777] VISA International, "Integrated Circuit Chip Card—Security Guidelines Summary," version 2 draft 1 (Nov 1997).

[778] A Viterbi, "Spread-Spectrum Communications—Myths and Realities," in *IEEE Communications Magazine*, v 17 no 3 (May 1979), pp 11–18.

[779] PR Vizcaya, LA Gerhardt, "A Nonlinear Orientation Model for Global Description of Fingerprints," in *Pattern Recognition*, v 29 no 7 (July 1996), pp 1221–1231.

[780] 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.

[781] 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.

[782] DA Wagner, SM Bellovin, "A 'Bump in the Stack' Encryptor for MS-DOS Systems," in *Proceedings of the Internet Society Symposium on Network and Distributed System Security* (1996); proceedings published by the IEEE, ISBN 0-8186-7222-6, pp 155–160.

[783] 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/`.

[784] 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`.

[785] 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.

[786] 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`.

[787] G Walsh, "Review of Policy Relating to Encryption Technologies" (1996), at http://www.efa.org.au/Issues/Crypto/Walsh/.

[788] KG Walter, WF Ogden, WC Rounds, FT Bradshaw, SR Ames, DG Shumway, "Models for Secure Computer Systems," Case Western Reserve University, Report No. 1137 (July 31, 1973, revised Nov 21, 1973).

[789] 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 (Jan 23, 1974); at http://www.dtic.mil.

[790] E Waltz, *Information Warfare—Principles and Operations*, Artech House (1998), ISBN 0-89006-511-X.

[791] 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); at http://csrc.nist.gov/publications/history/index.html.

[792] SD Warren, LD Brandeis, "The Right to Privacy," *Harvard Law Review*, series 4 (1890), pp 193–195.

[793] M Weaver, "Developer Tortured by Raiders with Crowbars," *Daily Telegraph* (Oct 31, 1997).

[794] W Webb, "High-Tech Security: The Eyes Have It," in *EDN* (Dec 18, 1997), pp 75–78.

[795] SH Weingart, "Physical Security for the $\mu$ABYSS System," in *Proceedings of the 1987 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, pp 52–58.

[796] 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* (Dec 3–7, 1990), Tucson, AZ; proceedings published by the IEEE (1990), pp 232–243.

[797] L Weinstein, "IDs in Color Copies—A PRIVACY Forum Special Report," in *Privacy Forum Digest*, v 8 no 18 (Dec 6, 1999), at http://www.vortex.com/privacy/priv.08.18.

[798] C Weissman, "Security Controls in the ADEPT–50 Time-Sharing System," in *AFIPS Conference Proceedings*, v 35, 1969 Fall Joint Computer Conference, pp 119–133.

[799] 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.

[800] G Welchman, *The Hut Six Story*, New York: McGraw-Hill (1982), ISBN 0-07-069180-0.

[801] 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.

[802] AF Westin, "Data Protection in the Global Society" (1996 conference report), at http://www.privacyexchange.org/iss/confpro/aicgsberlin.html.

[803] A Whitten, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *Eighth USENIX Security Symposium*, proceedings ISBN 1-880446-28-6, pp 169–183.

[804] MV Wilkes, RM Needham, *The Cambridge CAP Computer and Its Operating System*, Elsevier North Holland (1979).

[805] 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).

[806] FW Winterbotham, *The Ultra Secret*, New York: Harper & Row (1974).

[807] K Wong, "Mobile Phone Fraud—Are GSM Networks Secure?" in *Computer Fraud and Security Bulletin* (Nov 1996), pp 11–18.

[808] CC Wood, "Identity Token Usage at American Commercial Banks," in *Computer Fraud and Security Bulletin* (Mar 1995), pp 14–16.

[809] 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.

[810] B Wright, "The Verdict on Plaintext Signatures: They're Legal," in *Computer Law and Security Report*, v 14 no 6 (Nov/Dec 1994), pp 311–312.

[811] B Wright, *The Law of Electronic Commerce: EDI, Fax and Email*, New York: Little Brown (1991); 4th ed, (with supplement) 1994.

[812] 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, U.S. Department of Energy Office of Scientific and Technical Information (1997), http://www.osti.gov/opennet/app-f.html.

[813] MA Wright, "Security Controls in ATM Systems," in *Computer Fraud and Security Bulletin* (Nov 1991), pp 11–14.

[814] P Wright, *Spycatcher—The Candid Autobiography of a Senior Intelligence Officer*, Australia: William Heinemann (1987), ISBN 0-85561-098-0.

[815] 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.

[816] JX Yan, S Early, R Anderson, "The XenoService—A Distributed Defeat for Distributed Denial of Service," Third Information Survivability Workshop (Oct 2000), at http://www.cl.cam.ac.uk/users/rja14/.

[817] T Ylönen, "SSH—Secure Login Connections over the Internet," in *USENIX Security 96*, pp 37–42.

[818] 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 (1998), pp 283–293.

[819] 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.

[820] 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.

[821] Zero Knowledge Systems Inc., `http://www.zeroknowledge.com/`.

[822] MW Zior, "A Community Response to CMM-Based Security Engineering Process Improvement," in *18th National Information Systems Security Conference* (1995), pp 404–413.

[823] 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.