Bibliography

[1] M Aamir Ali, B Arief, M Emms, A van Moorsel, “Does the Online Card Payment Landscape Unwittingly Facilitate Fraud?” *IEEE Security & Privacy Magazine* (2017)

[2] M Abadi, RM Needham, “Prudent Engineering Practice for Cryptographic Protocols”, *IEEE Transactions on Software Engineering* v 22 no 1 (Jan 96) pp 6–15; also as DEC SRC Research Report no 125 (June 1 1994)

[3] A Abbasi, HC Chen, “Visualizing Authorship for Identification”, in *ISI 2006*, LNCS 3975 pp 60–71

[4] H Abelson, RJ Anderson, SM Bellovin, J Benaloh, M Blaze, W Diffie, J Gilmore, PG Neumann, RL Rivest, JI Schiller, B Schneier, “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption”, in *World Wide Web Journal* v 2 no 3 (Summer 1997) pp 241–257

[5] H Abelson, RJ Anderson, SM Bellovin, J Benaloh, M Blaze, W Diffie, J Gilmore, M Green, PG Neumann, RL Rivest, JI Schiller, B Schneier, M Specter, D Weizmann, “Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications”, MIT CSAIL Tech Report 2015-026 (July 6, 2015); abridged version in *Communications of the ACM* v 58 no 10 (Oct 2015)

[6] M Abrahms, “What Terrorists Really Want”, *International Security* v 32 no 4 (2008) pp 78–105

[7] M Abrahms, J Weiss, “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia”, *ACSAC 2008*

[8] 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

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

[10] Y Acar, M Backes, S Bugiel, S Fahl, PD McDaniel, M Smith, “SoK: Lessons Learned from Android Security Research for Appified Software Platforms”, *IEEE S&P 2016* pp 433–451

[11] Y Acar, S Fahl, M Mazurek, “You Are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users”, *IEEE SecDev 2016*

[12] N Achs, “VISA confronts the con men”, *Cards International* (20 Oct 1992) pp 8–9

[13] O Acıiçmez, ÇK Koç, JP Seifert, “On the Power of Simple Branch Prediction Analysis” *2nd ACM symposium on Information, computer and communications security* (2007) pp 312–320

[14] S Ackerman, J Ball “Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ” *The Guardian* Feb 28 2014

[15] A Acquisti, A Friedman, R Telang, "Is There a Cost to Privacy Breaches?", *Fifth Workshop on the Economics of Information Security* (2006)

[16] A Acquisti, G Loewenstein, L Brandimarte, "Secrets and Likes: The need for privacy and the difficulty of achieving it in the digital age", *Journal of Consumer Psychology* (2020)

[17] NR Adam, JC Wortmann, "Security-Control Methods for Statistical Databases: A Comparative Study", *ACM Computing Surveys* v 21 no 4 (1989) pp 515–556

[18] EN Adams, "Optimising preventive maintenance of software products", *IBM Journal of Research & Development*, v 28 no 1 (1984) pp 2–14

[19] J Adams, *'Risk'*, University College London Press 1995

[20] J Adams, "Cars, Cholera and Cows: the management of risk and uncertainty", *Policy Analysis* no 335, Cato Institute, Washington, 1999

[21] E Addley "Animal Liberation Front bomber jailed for 12 years", *The Guardian* Dec 6 2006

[22] B Adida, M Bond, J Clulow, A Lin, RJ Anderson, RL Rivest, "A Note on EMV Secure Messaging in the IBM 4758 CCA", at `www.ross-anderson.com`

[23] H Adkins, B Beyer, P Blankiship, P Lewandowski, A Oprea, A Stubblefield, *'Building Secure and Reliable Systems'*, Google 2020

[24] A Adler, "Sample images can be independently restored from face recognition templates", in *Proc. Can. Conf. Elec. Comp. Eng.* (2003) pp 1163–1166

[25] A Adler, "Vulnerabilities in biometric encryption systems", in *NATO RTA Workshop: Enhancing Information Systems Security – Biometrics* (IST-044-RWS-007)

[26] D Adrian, K Bhargavan, Z Durumeric, P Gaudry, M Green, JA Halderman, N Heninger, D Springall, E Thomé, L Valenta, B VanderSloot, E Wustrow, S Zanella-Bǵuelin, P Zimmermann, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice", *ACM CCS 2015*, `weakdh.org`

[27] Y Afina, C Inverarity, B Unal, *'Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems'*, Chatham House, July 2020

[28] S Afroz, M Brennan, R Greenstadt, "Detecting hoaxes, frauds, and deception in writing style online", in *IEEE Symposium on Security and Privacy* (2012) pp 461–475

[29] *'Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QCSD for Server Signing'*, 419241-2, Agence nationale de la sécurité des systèmes d'information, 2018

[30] H Agnew, "Jim Chanos pockets $100m from Wirecard short", *Financial Times* Jul 24 2020

[31] E Ahmed-Rengers, M Ahmed-Rengers, "Democracy on the Margins of the Market: A Critical Look into the Privatisation of Cyber Norm Formation", *Hague Conference on Cyber Norms* 2020, at `https://ahmed-rengers.com/cybernorms/`

[32] M Ahmed-Rengers, R Anderson, D Halatova, I Shumailov, "Snitches Get Stitches: On The Difficulty of Whistleblowing", *Security Protocols Workshop* (2019); online as *arXiv:2006.14407* (2010)

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

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

[35] G Akerlof, "The Market for 'Lemons: Quality Uncertainty and the Market Mechanism", in *The Quarterly Journal of Economics* v 84 no 3 (1970) pp 488–500

[36] M Alagappan, JV Rajendran, M Doroslovački, G Venkataramani, "DFS Covert Channels on Multi-Core Platforms", *Visisoc 2017*

[37] R Albert, HW Jeong, AL Barabási, "Error and attack tolerance of complex networks", in *Nature* v 406 no 1 (2000) pp 387–482

[38] J Alfke, "Facebook and Decentralized Identifiers", in *Thought Palace* Dec 2 2007

[39] AM Algarni, YK Malaiya, "Software Vulnerability Markets: Discoverers and Buyers", *International Journal of Computer, Information Science and Engineering* v 8 no 3 (2014)

[40] M Ali, P Sapiezinski, M Bogen, A Korolova, A Mislove, A Rieke, "Discrimination through Optimization:How Facebook's Ad Delivery Can Lead to Biased Outcomes", *Proceedings of the ACM on Human-Computer Interaction* v 3 (2019)

[41] M Ali, P Sapiezinski, A Korolova, A Mislove, A Rieke, "Ad Delivery Algorithms:The Hidden Arbiters of Political Messaging", *arXiv:1912.04255*, Dev 17 2019

[42] E Allman, "Managing Technical Debt", *Communications of the ACM* v 55 no 5 (May 2012) pp 50–55

[43] M Allman, V Paxson, "Etiquette Concerning Use of Shared Measurement Data", in *Internet Measurement Conference* (IMC 2007), at `http://www.imconf.net/imc-2007/papers/imc80.pdf`

[44] F Almgren, G Andersson, T Granlund, L Ivansson, S Ulfberg, "How We Cracked the Code Book Ciphers", at `http://codebook.org`

[45] T Alves, D Felton, "TrustZone: Integrated Hardware and Software Security", *Information Quarterly* (2004)

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

[47] *Amnesty International*, "Evolving Phishing Attacks Targeting Journalists and Human Rights Defenders from the Middle-East and North Africa", Aug 16 2019

[48] E Amoroso, *'Fundamentals of Computer Security Technology'*, Prentice Hall 1994

[49] R Andersen, "The Panopticon Is Already Here", *The Atlantic*, Sep 2020

[50] C Anderson, K Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge", *Carnegie Endowment* Jan 4 2018

[51] B Andersen, M Frenz, "The Impact of Music Downloads and P2P File-Sharing on the Purchase of Music: A Study for Industry Canada", 2007, at `http://strategis.ic.gc.ca/epic/site/ippd-dppi.nsf/en/h_ip01456e.html`

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

[53] M Anderson, W Seltzer, *Official Statistics and Statistical Confidentiality: Recent Writings and Essential Documents*, at `http://www.uwm.edu/%7Emargo/govstat/integrity.htm`

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

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

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

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

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

[59] RJ Anderson, *'Security in Clinical Information Systems'*, British Medical Association 1996

[60] RJ Anderson, "A Security Policy Model for Clinical Information Systems", in *1996 IEEE Symposium on Security and Privacy* pp 30–43; at `http://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html`

[61] RJ Anderson, "An Update on the BMA Security Policy", in [64] pp 233–250

[62] RJ Anderson, “The Eternity Service”, in *Proceedings of Pragocrypt 96* pp 242–252

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

[64] RJ Anderson (ed), ‘*Personal Medical Information – Security, Engineering and Ethics*’, Springer-Verlag 1997

[65] RJ Anderson, “On the Security of Digital Tachographs”, in *ESORICS 98*, Springer LNCS v 1485 pp 111–125

[66] RJ Anderson, “Safety and Privacy in Clinical Information Systems”, in ‘*Rethinking IT and Health*’, J Lenaghan (ed), IPPR (Nov 98) pp 140–160

[67] RJ Anderson, “The DeCODE Proposal for an Icelandic Health Database”; *Læknabladhidh* (The Icelandic Medical Journal) v 84 no 11 (Nov 98) pp 874–5, `http://www.cl.cam.ac.uk/users/rja14/#Med`

[68] RJ Anderson, “The Formal Verification of a Payment System”, chapter in *Industrial Strength Formal Methods: A Practitioners Handbook*, MG Hinchey and JP Bowen (editors), Springer Verlag (Sep 1999) pp 43–52

[69] RJ Anderson, “How to Cheat at the Lottery (or, Massively Parallel Requirements Engineering)”, in *15th Annual Computer Security Application Conference* (1997); pp xix–xxvii; at `http://www.cl.cam.ac.uk/~1rja14/lottery/lottery.html`

[70] RJ Anderson, “The Millennium Bug – Reasons not to Panic”, at `http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/y2k.html`

[71] 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`

[72] RJ Anderson, “The Correctness of Crypto Transaction Sets”, in *Proceedings of Security Protocols 2000*, Springer LNCS v 2133 pp 125–141

[73] RJ Anderson, “Why Information Security is Hard – An Economic Perspective”, in *ACSAC 2001* pp 358–365; also given as a distinguished lecture at SOSP, 2001

[74] RJ Anderson, “Cryptography and Competition Policy – Issues with ‘Trusted Computing’ ”, *Second Workshop on Economics and Information Security* (2003)

[75] RJ Anderson, “Open and Closed Systems are Equivalent (that is, in an ideal world)”, in *Perspectives on Free and Open Source Software*, MIT Press 2005, pp 127–142

[76] RJ Anderson, “Closing the Phishing Hole – Fraud, Risk and Nonbanks”, at *Nonbanks in the Payments System: Innovation, Competition, and Risk*, US Federal Reserve, Santa Fe, May 2–4 2007

[77] RJ Anderson, ‘*Security Economics Resource Page*’, at `http://www.cl.cam.ac.uk/~rja14/econsec.html`

[78] RJ Anderson, “A Merry Christmas to all Bankers”, at `https://www.lightbluetouchpaper.org`, Dec 25 2010

[79] RJ Anderson, “Security Economics – A Personal Perspective”, *ACSAC 2012*

[80] RJ Anderson, “Risk and Privacy Implications of Consumer Payment Innovation” *Consumer Payment Innovation in the Connected Age*, Kansas City Fed, March 2012

[81] RJ Anderson, “The privacy of our medical records is being sold off”, The Guardian Aug 28 2012

[82] RJ Anderson, “Will the Information Commissioner be consistent?”, *https://www.lightbluetouchpaper.org*, Nov 20 2012

[83] RJ Anderson, “How privacy is lost”, at `https://lightbluetouchpaper.org`, April 28 2013

[84] RJ Anderson, “Offender tagging”, at `https://lightbluetouchpaper.org`, Sep 2 2013

[85] RJ Anderson, “Privacy versus government surveillance: where network effects meet public choice”, in *Workshop on the Economics of Information Security* (2014)

[86] RJ Anderson, “Curfew tags – the gory details” `https://lightbluetouchpaper.org` Dec 13 2014

[87] RJ Anderson, “Meeting Snowden in Princeton”, at `https://lightbluetouchpaper.org` May 2 2015

[88] RJ Anderson, "He Who Pays The AI, Calls The Tune", *The Edge Question 2015: What do you think about machines that think?*, `https://www.edge.org/response-detail/26069`

[89] RJ Anderson, "Future ID", Mar 19 2019, at `https://www.lightbluetouchpaper.org/2019/03/19/future-id/`

[90] RJ Anderson, *Software and Security Engineering*, Cambridge University, 2020, at `https://www.cl.cam.ac.uk/teaching/1920/SWSecEng/materials.html`

[91] RJ Anderson, C Barton, R Böhme, R Clayton, M van Eeten, M Levi, T Moore, S Savage, "Measuring the Cost of Cybercrime", WEIS 2012

[92] RJ Anderson, C Barton, R Böhme, R Clayton, C Gañán, T Grasso, M Levi, T Moore, M Vasek, "Measuring the Changing Cost of Cybercrime", WEIS 2019

[93] RJ Anderson, T Berger-Wolf, "Privacy for Tigers", at *Usenix Security* 2018

[94] 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

[95] RJ Anderson, E Biham, LR Knudsen, "Serpent: A Proposal for the Advanced Encryption Standard", submitted to NIST as an AES candidate; at [96]

[96] RJ Anderson, E Biham, L Knudsen, *'The Serpent Home Page'*, at `http://www.cl.cam.ac.uk/~rja14/serpent.html`

[97] RJ Anderson, N Bohm, T Dowty, F Fisher, D Korff, E Munro, M Thomas, "Consultation response on The Data Sharing Review", *FIPR* Feb 15 2008

[98] RJ Anderson, R Böhme, R Clayton, T Moore, *'Security Economics and the Internal Market'*, ENISA, 2008

[99] RJ Anderson, M Bond, "API-Level Attacks on Embedded Systems", in *IEEE Computer* v 34 no 10 (October 2001) pp 67–75

[100] RJ Anderson, M Bond, "Protocol Analysis, Composability and Computation" in *Computer Systems: Theory, Technology and Applications*, Springer 2003, pp 7–10

[101] RJ Anderson, M Bond, J Clulow, S Skorobogatov, *'Cryptographic processors – a survey'*, Cambridge University Computer Laboratory Technical Report no 641 (July 2005); shortened version in *Proc. IEEE* v 94 no 2 (Feb 2006) pp 357–369

[102] RJ Anderson, I Brown, R Clayton, T Dowty, D Korff, E Munro, *'Children's Databases – Safety and Privacy'*, Information Commissioner's Office, UK, Nov 2006

[103] RJ Anderson, I Brown, T Dowty, W Heath, P Inglesant, A Sasse, *Database State*, Joseph Rowntree Reform Trust, 2009

[104] RJ Anderson, B Crispo, JH Lee, C Manifavas, V Matyás, FAP Petitcolas, *'The Global Internet Trust Register'*, MIT Press 1999, and at `http://www.cl.cam.ac.uk/Research/Security/Trust-Register/`

[105] R Anderson, S Fuloria, "Security Economics and Critical National Infrastructure", at *WEIS 2009*; in *Economics of Information Security and Privacy* (2010) pp 55–66

[106] R Anderson, S Fuloria, "Who controls the off switch?" at *IEEE SmartGridComm* (2010)

[107] RJ Anderson, MG Kuhn, "Tamper Resistance – a Cautionary Note", in *Proceedings of the Second Usenix Workshop on Electronic Commerce* (Nov 96) pp 1–11

[108] RJ Anderson, MG Kuhn, "Low Cost Attacks on Tamper Resistant Devices", in *Security Protocols* (1997) pp 125–136

[109] 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

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

[111] RJ Anderson, TW Moore, "Information Security Economics – and Beyond", in *Crypto 2007*, Springer LNCS 4622, pp 68–91

[112] RJ Anderson, TW Moore, "Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research", in *Oxford Handbook of the Digital Economy* (2011)

[113] RJ Anderson, RM Needham, "Robustness principles for public key protocols", in *Crypto 95* Springer LNCS v 963 pp 236–247

[114] RJ Anderson, RM Needham, "Programming Satan's Computer", in *'Computer Science Today'*, Springer Lecture Notes in Computer Science v 1000 (1995) pp 426–441

[115] RJ Anderson, RM Needham, A Shamir, "The Steganographic File System", in *Second International Workshop on Information Hiding*, Springer LNCS vol 1525 pp 74–84

[116] RJ Anderson, MR Roe, "The GCHQ Protocol and Its Problems", in *Eurocrypt 97*, Springer LNCS v 1233 pp 134–148

[117] RJ Anderson, I Shumailov, M Ahmed, A Rietmann, "Bitcoin Redux", *Workshop on the Economics of Information Security* (2018)

[118] T Anderson, "An Internet of Trouble lies ahead as root certificates begin to expire en masse, warns security researcher", *The Register* Jun 10 2020

[119] CM Andrew, V Mitrokhin, *'The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB'*, Basic Books 1999

[120] M Andrews, JA Whitaker, *'How to Break Web Software'*, Addison-Wesley 2006

[121] `http://www.anonymizer.com`

[122] Anonymous, "I'm the Google whistleblower. The medical data of millions of Americans is at risk", *The Guardian* Nov 14 2019

[123] *Anonymity Bibliography*, 2007, at `http://freehaven.net/anonbib/`

[124] JC Anselmo, "US Seen More Vulnerable to Electromagnetic Attack", in *Aviation Week and Space Technology* v 146 no 4 (Jul 28 1997) p 67

[125] D Antonioli, NO Tippenhauer and KB Rasmussen, "The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR", *Usenix 2019*

[126] D Antonioli, NO Tippenhauer and KB Rasmussen, "BIAS: Bluetooth Impersonation Attacks", *IEEE S&P 2020*

[127] APACS, "Fraud abroad drives up card fraud losses", October 3 2007; at `http://www.apacs.org.uk/media_centre/press/03.10.07.html`; see also *The Register*, `http://www.theregister.co.uk/2007/10/03/card_fraud_trends/`

[128] APACS, "Payment Advice – Protect Your PIN", Aug 16 2007; at `http://www.apacs.org.uk/media_centre/press/08_16_07.html`

[129] Apple, *'iOS Security'*, May 2019

[130] T Appleby, "Chilling debit-card scam uncovered", in *The Globe & Mail* (10/12/1999) p 1

[131] I Arghire, "Hardware-based Password Managers Store Credentials in Plaintext" *Security Week* Dec 9 2019

[132] Arm Inc., *'Cache Speculation Side-channels'* v 2.4, Oct 2018

[133] US Army, *'Electromagnetic Pulse (EMP) and Tempest Protection for Facilities'*, Corps of Engineers Publications Depot, Hyattsville (1990)

[134] A Arora, R Krishnan, A Nandkumar, R Telang, YB Yang, "Impact of Vulnerability Disclosure and Patch Availability – An Empirical Analysis", *Third Workshop on the Economics of Information Security* (2004)

[135] A Arora, CM Forman, A Nandkumar, R Telang, "Competitive and strategic effects in the timing of patch release", in *Workshop on the Economics of Information Security* (2006)

[136] SE Asch, *'Social Psychology'*, OUP 1952

[137] D Asonov, R Agrawal, “Keyboard Acoustic Emanations”, IBM Almaden Research Center, 2004

[138] *‘ASPECT – Advanced Security for Personal Communications Technologies’*, at `http://www.esat.kuleuven.ac.be/cosic/aspect/index.html`

[139] Associated Press, “Charges dropped against Ex-HP chairwoman – Three others charged in boardroom spying case receive no jail time”, Mar 14 2007, at `http://www.msnbc.msn.com/id/17611695/`

[140] C Aspinwall, A Giorgi, D DiFurio, “Several Boeing 737 Max 8 pilots in U.S. complained about suspected safety flaw”, *Dallas Morning News* Mar 12 2019

[141] R Atkinson, “The single most effective weapon against our deployed forces” and “The IED problem is getting out of control. We’ve got to stop the bleeding”, in the *Washington Post*, Sep 30 2007; “There was a two-year learning curve . . . and a lot of people died in those two years”, Oct 1 2007; “You can’t armor your way out of this problem”, Oct 2 2007; “If you don’t go after the network, you’re never going to stop these guys. Never”, Oct 3 2007; all linked from `https://web.archive.org/web/20080827220904/http://smallwarsjournal.com/blog/2007/09/print/weapon-of-choice/`

[142] D Aucsmith, “Tamper-Resistant Software: An Implementation”, in [63] pp 317–333

[143] D Aucsmith (editor), *Proceedings of the Second International Workshop on Information Hiding* (Portland, Apr 98), Springer LNCS 1525

[144] B Audone, F Bresciani, “Signal Processing in Active Shielding and Direction-Finding Techniques”, *IEEE Transactions on Electromagnetic Compatibility* v 38 no 3 (August 1996) pp 334-340

[145] B Auxier, L Rainie, M Anderson, A Perrin, M Kumar, E Turner, “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information”, *Pew Research Center* Nov 15 2019

[146] A Aviv, *‘Side channels enabled by smartphone interaction’*, PhD Thesis, University of Pennsylvania, 2012

[147] A Aviv, B Sapp, M Blaze, JM Smith, “Practicality of Accelerometer Side Channels on Smartphones” *ACSAC 2012*

[148] R Axelrod, *The Evolution of Cooperation*, Basic Books (1984)

[149] I Ayres, SD Levitt, “Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack”, in *Quarterly Journal of Economics* v 108 no 1 (Feb 1998), `http://www.nber.org/papers/w5928`

[150] D Austin, “Flood warnings”, in *Banking Technology* (Jul–Aug 1999) pp 28–31

[151] “Computer Combat Rules Frustrate the Pentagon”, in *Aviation Week and Space Technology* v 147 no 11 (15/9/97) pp 67–68

[152] J Bacon, *‘Concurrent Systems’*, Addison-Wesley 1997

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

[154] 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

[155] M Baggott, “The smart way to fight fraud”, *Scottish Banker* (Nov 95) pp 32–33

[156] M Baker, D Gates, “Boeing altered key switches in 737 MAX cockpit, limiting ability to shut off MCAS ”, *Seattle Times*, May 10 2019

[157] P Baker, “Five Takeaways From John Bolton’s Memoir”, *New York Times* Jun 18 2020

[158] G Baldini, E Leverett, R Clayton, R Anderson, “*Standardisation and Certification of Safety, Security and Privacy in the ‘Internet of Things’* ” European Commission Joint Research Centre, 2017

[159] D Balfanz, EW Felten, “Hand-Held Computers Can Be Better Smart Cards”, in *Eighth USENIX Security Symposium* (1999), pp 15–23

[160] T Balmforth, “Russia postpones sovereign internet test over coronavirus”, *Reuters* Mar 20 2020

[161] J Bamford, *‘The Puzzle Palace: A Report on NSA, America’s Most Secret Agency’*, Houghton, Mifflin 1982

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

[163] *'Enhancing cross-border payments: building blocks of a global roadmap – Stage 2 report to the G20'*, Bank for International Settlements, July 2020

[164] "Card Fraud: Banking's Boom Sector", in *Banking Automation Bulletin for Europe* (Mar 92) pp 1–5

[165] J Baniak, G Baker, AM Cunningham, L Martin, "Silent Sentry Passive Surveillance", *Lockheed Martin Mission Systems* (1999)

[166] S Bano, A Sonnino, M Al-Bassam, S Azouvi, P McCorry, S Meiklejohn, G Danezis, "SoK: Consensus in the Age of Blockchains", *arXiv:1711.03936*, Nov 10 2017

[167] B Barak, O Goldreich, R Impagliazzo, S Rudich, A Sahai, S Vadhan, K Yang, "On the (Im)possibility of Obfuscating Programs", *Crypto 2001*, `http://www.wisdom.weizmann.ac.il/~oded/p_obfuscate.html`

[168] M Barbaro, T Zeller, " A Face Is Exposed for AOL Searcher No. 4417749", in *New York Times* Aug 9 2006

[169] R Barbulescu, P Gaudry, A Joux, E Thomé, "A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic", *Eurocrypt 2014* pp 1–16

[170] A Barisani, B Bianco, "Practical EMV PIN interception and fraud detection", `https://github.com/abarisani/`, 2017

[171] JP Barlow, "The Economy of Ideas", *Wired* Mar 1 1994

[172] E Barkan, E Biham, N Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication" Technion Technical Report CS-2006-07

[173] R Barkan, S Ayal, D Ariely, "Ethical dissonance, justifications and moral behaviour", *Current Opinion in Psychology* v 6 (2015) pp 157–161

[174] RL Barnard, *'Intrusion Detection Systems'*, Butterworths 1988

[175] T Barnes, "NSA Whistleblower Reality Winner Was Held in Isolation for a Week and No One Has Explained Why", *The Intercept* Sep 26 2018

[176] A Barnett, "Britain's UFO secrets revealed", in *The Observer* Jun 4 2000

[177] S Baron-Cohen, *The Essential Difference: Men, Women, and the Extreme Male Brain*, Penguin, 2003

[178] S Baron-Cohen, AM Leslie, U Frith, "Does the autistic child have a 'theory of mind'?" Cognition (Oct 1985) v 21 no 1 pp 37–46

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

[180] B Barrow, B Quinn, "Millions in danger from chip and pin fraudsters" in *Daily Mail* June 5th 2006

[181] B Bartholomew, JA Guerrero-Saade, "Wave your false flags! Deception tactics muddying attribution in targeted attacks, *Karpersky Labs*, Oct 6 2016

[182] D Bartz, A Oreskovic, "UPDATE 3-Facebook settles privacy case with U.S. FTC" *Reuters* Nov 30 2011

[183] D Basin, R Sasse, J Toro, "The EMV Standard: Break, Fix, Verify", *arXiv:2006.08249*, Jun 15 2020

[184] R Baskerville, "Information Systems Security Design Methods: Implications for Information Systems Development", in *ACM Computing Surveys* v 265 (1993) pp 375–414

[185] PJ Bass, "Telephone Cards and Technology Development as Experienced by GPT Telephone Systems", in *GEC Review* v 10 no 1 (95) pp 14–19

[186] *'Bates and others v Post Office group litigation,'* 2019, at `https://www.postofficetrial.com/`

[187] W Bax, V Dekker, "Met zijn allen meekijken in de medische kaartenbak", in *Trouw* Dec 11 2007

[188] S Baxter, "US hits panic button as air force 'loses' nuclear missiles", in *Sunday Times* Oct 21 2007

[189] BBC News Online, "Tax records 'for sale' scandal", Jan 16 2003, at `https://news.bbc.co.uk/1/hi/business/2662491.stm`

[190] BBC News Online, " 'Relief' over fingerprint verdict", Feb 7 2006, at https://news.bbc.co.uk/1/hi/scotland/4689218.stm

[191] BBC News Online, "Schools get rules on biometrics", July 23 2007, at https://news.bbc.co.uk/1/hi/education/6912232.stm

[192] BBC News Online, "PC stripper helps spam to spread", Oct 30 2007, at https://news.bbc.co.uk/1/hi/technology/7067962.stm

[193] BBC News Online, "The mystery of Ireland's worst driver", Feb 19 2009, at http://news.bbc.co.uk/1/hi/northern_ireland/7899171.stm

[194] BBC News Online, "G4S and Serco lose tagging contracts", Dec 12 2013, at https://www.bbc.co.uk/news/uk-25348086

[195] BBC News Online, "Citizenship Amendment Bill: India's new 'anti-Muslim' law explained", Dec 11 2019

[196] S Beattie, S Arnold, C Cowan, P Wagle, C Wright, "Timing the Application of Security Patches for Optimal Uptime", in *LISA XVI* (2002) pp 101–110

[197] A Beautement, MA Sasse, M Wonham, "The Compliance Budget: Managing Security Behaviour in Organisations", *NSPW 2008*

[198] F Beck, *'Integrated Circuit Failure Analysis – A Guide to Preparation Techniques'*, Wiley 1998

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

[200] G De Becker, "Bezos Investigation Finds the Saudis Obtained His Private Data", *The Daily Beast* Mar 30 2019

[201] GS Becker, "Crime and Punishment: An Economic Approach", in *Journal of Political Economy* v 76 no 2 (March/April 1968) pp 169–217

[202] I Becker, A Hutchings, R Abu-Salma, RJ Anderson, N Bohm, SJ Murdoch, MA Sasse, G Stringhini, "International comparison of bank fraud reimbursement: customer perceptions and contractual terms", *Journal of Cybersecurity*, v 3 no 2 (2017) pp 109–125

[203] L Beckwith, C Kissinger, M Burnett, S Weidenbeck, J Lowrance, A Blackwell, C Cook, "Tinkering and Gender in End-User Programmers' Debugging", in *CHI '06*, Montreal, April 2006; at http://eusesconsortium.org/gender/

[204] JB Bédrune G Campana, "Everybody be cool, this is a robbery!", *Black Hat* 2019; at https://donjon.ledger.com/BlackHat2019-presentation/

[205] I Beer, "A very deep dive into iOS Exploit chains found in the wild", *Google Project Zero Blog* Aug 29 2019, at https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

[206] S Begley, "Fingerprint Matches Come Under More Fire As Potentially Fallible", *Wall Street Journal* Oct 7 2005 p B1; at http://online.wsj.com/article_print/SB112864132376462238.html

[207] HA Beker, C Amery, "Cryptography Policy", at https://www.cl.cam.ac.uk/~rja14/Papers/zergo_cryptographypolicy.html

[208] 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

[209] H Beker, F Piper, *'Cipher Systems'*, Northwood 1982

[210] 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

[211] DE Bell, L LaPadula, *'Secure Computer Systems'*, ESD-TR-73-278, Mitre Corporation; v I and II: November 1973, v III: Apr 1974

[212] 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

[213] M Bellare, P Rogaway, "Optimal Asymmetric Encryption", in *Advances in Cryptology – Eurocrypt 94*, Springer LNCS v 950 pp 103–113; see also RFC 2437

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

[215] SM Bellovin, "Defending Against Sequence Number Attacks", RFC 1948 (May 1996)

[216] SM Bellovin, "Problem Areas for the IP Security Protocols," in *Proceedings of the Sixth Usenix Unix Security Symposium* (1996); at `http://www.cs.columbia.edu/~smb/papers/badesp.pdf`

[217] SM Bellovin, "Debit-card fraud in Canada", in `comp.risks` v 20.69; at `http://catless.ncl.ac.uk/Risks/20.69.html`

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

[219] SM Bellovin, *'ICMP Traceback Messages'*, Internet Draft, March 2000, at `http://search.ietf.org/internet-drafts/draft-bellovin-itrace-00.txt`

[220] SM Bellovin, "More on Comcast Blocking Peer-to-Peer Traffic", Oct 22 2007, at `http://www.cs.columbia.edu/~smb/blog/2007-10/2007-10-22.html`; and "Comcast Apparently Blocking Some Peer-to-Peer Traffic", Oct 19 2007, ibid.

[221] S Bellovin, M Blaze, E Brickell, C Brooks, V Cerf, W Diffie, S Landau, J Peterson, J Treichler, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", `http://www.itaa.org/news/docs/CALEAVOIPreport.pdf`

[222] SM Bellovin, WR Cheswick, A Rubin, *'Firewalls and Internet Security, Second Edition: Repelling the Wily Hacker'*, Addison-Wesley 2003

[223] SM Bellovin, M Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", in *Proceedings of the IEEE Symposium on Security and Privacy* (1992) pp 72–84

[224] J Benaloh, "ElectionGuard Preliminary Specification v0.85", *Microsoft Research*, 2020

[225] M Benantar, R Guski, KM Triodle, "Access control systems: From host-centric to network-centric computing", in *IBM Systems Journal* v 35 no 1 (96) pp 94–112

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

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

[228] Y Benkler, *'Network Propaganda – Manipulation, Disinformation, and Radicalization in American Politics'*, Oxford 2018

[229] Y Berger, A Wool, A Yeredor, "Dictionary Attacks Using Keyboard Acoustic Emanations", *ACM CCS 2006*

[230] R Bergman, DM Halbfinger, "Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks", *New York Times* May 19 2020

[231] M Bernhard, J Benaloh, JA Halderman, RL Rivest, PYA Ryan, PB Stark, V Teague, PL Vora, DS Wallach, "Public Evidence from Secret Ballots", *arXiv:1707.08619*, Aug 4 2017

[232] J Bennetto, "How IRA plotted to switch off London", *The Independent*, Apr 12 1997

[233] DJ Bernstein, *'Cache-Timing Attacks on AES'*, preprint, 2005

[234] I Berres 2018, "Was Patienten jetzt wissen müssen", *Der Spiegel* Nov 26 2018

[235] J Bessen, "Industry Concentration and Information Technology", *SSRN 3044730*, 2019

[236] A Bessey, K Block, B Chelf, A Chou, B Fulton, S Hallem, C Henri-Gros, A Kamsky, S McPeak, D Engler, "A few billion lines of code later: using static analysis to find bugs in the real world", in *Communications of the ACM* v 53 no 2, Feb 2010

[237] B Beyer, C Jones, J Petoff, NR Murphy, *'Site Reliability Engineering'*, Google Books 2013

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

[239] S Biddle, "The NSA Leak Is Real, Snowden Documents Confirm", *The Intercept* Aug 19 2016

[240] AD Biderman, H Zimmer, *'The Manipulation of Human Behavior'*, Wiley 1961; at `http://www.archive.org/details/TheManipulationOfHumanBehavior`

[241] J Bidzos, "Oral History Interview with James Bidzos", *Charles Babbage Institute* Dec 11 2004

[242] B Biggio, F Rolli, "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning", *arXiv:1712.03141*, Jul 19 2018

[243] E Biham, A Biryukov, A Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials", in *Advances in Cryptology – Eurocrypt 97*, Springer LNCS v 1592 pp 12–23

[244] E Biham, O Dunkelman, S Indesteege, N Keller, B Preneel, "How To Steal Cars – A Practical Attack on KeeLoq", 2007, at `http://www.cosic.esat.kuleuven.be/keeloq/`

[245] E Biham, L Neumann, "Breaking the Bluetooth Pairing: Fixed Coordinate Invalid Curve Attack", *SAC 2019* pp 250–273

[246] E Biham, A Shamir, *'Differential Cryptanalysis of the Data Encryption Standard'*, Springer 1993

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

[248] C Bing, J Schectman, "Special Report: Inside the UAE's secret hacking team of U.S. mercenaries" *Reuters* Jan 30 2019

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

[250] R Bishop, R Bloomfield, "A Conservative Theory for Long-Term Reliability-Growth Prediction", in *IEEE Transactions on Reliability* v 45 no 4 (Dec 96) pp 550–560

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

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

[253] 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

[254] J Blackledge, "Making Money from Fractals and Chaos: Microbar", in *Mathematics Today* v 35 no 6 (Dec 99) pp 170–173

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

[256] B Blair, "Keeping Presidents in the Nuclear Dark", in *Bruce Blair's Nuclear Column*, Feb 11 2004, at `https://web.archive.org/web/20120511191600/http://www.cdi.org/blair/permissive-action-links.cfm`

[257] GR Blakley, "Safeguarding cryptographic keys", in *Proceedings of NCC AFIPS* (1979), pp 313–317

[258] B Blakley, R Blakley, RM Soley, *'CORBA Security: An Introduction to Safe Computing with Objects'*, Addison-Wesley 1999

[259] MA Blaze, "Protocol Failure in the Escrowed Encryption Standard", in *Second ACM Conference on Computer and Communications Security* pp 59–67

[260] Matt Blaze, "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks", at *IEEE Symposium on Security & Privacy* 2003

[261] MA Blaze, "Toward a Broader View of Security Protocols", in *Security Protocols 2004*, Springer LNCS v 3957, pp 106–132

[262] MA Blaze, "Safecracking for the computer scientist", U. Penn Technical Report (2004), at `http://www.crypto.com/papers/`

[263] MA Blaze, SM Bellovin, "Tapping, Tapping On My Network Door", in *Communications of the ACM* (Oct 2000), Inside Risks 124

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

[265] 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

[266] G Bleumer, *'Electronic Postage Systems – Technology, Security, Economics'*, Springer 2006

[267] B Blobel, "Clinical record Systems in Oncology. Experiences and Developments on Cancer Registers in Eastern Germany", in [64] pp 39–56

[268] 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

[269] P Bloom, *'Descartes' Baby: How Child Development Explains What Makes Us Human'*, Arrow (2005)

[270] S Blythe, B Fraboni, S Lall, H Ahmed, U de Riu, "Layout Reconstruction of Complex Silicon Chips", in *IEEE Journal of Solid-State Circuits* v 28 no 2 (Feb 93) pp 138–145

[271] WE Boebert, "Some Thoughts on the Occasion of the NSA Linux Release", in *Linux Journal*, Jan 24 2001; at `http://www.linuxjournal.com/article/4963`

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

[273] BW Boehm, *'Software Engineering Economics'*, Prentice Hall 1981

[274] A Bogdanov, D Khovratovich, C Rechberger, "Biclique Cryptanalysis of the Full AES", *Asiacrypt 2011*, and IACR preprint no. 2011-449

[275] R Böhme, N Christin, B Edelman, T Moore, "Bitcoin: Economics, Technology, and Governance", *Journal of Economic Perspectives* v 29 no 2 (Spring 2015) pp 213–238

[276] R Böhme, G Kataria, "Models and Measures for Correlation in Cyber-Insurance", at *WEIS 2006*

[277] R Böhme, T Moore, "The Iterated Weakest Link—A Model of Adaptive Security Investment", at *WEIS 2009*

[278] N Bohm, I Brown, B Gladman, *'Electronic Commerce – Who Carries the Risk of Fraud?'*, Foundation for Information Policy Research 2000

[279] K Bolan, "Richmond IT expert sentenced to 9 years in U.S. prison for helping violent criminal organizations", *Vancouver Sun*, May 29 2019

[280] M Bond, *'Understanding Security APIs'*, PhD Thesis, Cambridge, 2004

[281] M Bond, "BOOM! HEADSHOT! (Building Neo-Tactics on Network-Level Anomalies in Online Tactical First-Person Shooters)" (2006), at `http://www.lightbluetouchpaper.org/2006/10/02/`

[282] M Bond, "Action Replay Justice", Nov 22 2007, at `http://www.lightbluetouchpaper.org/2007/11/22/action-replay-justice/`

[283] M Bond, O Choudary, SJ Murdoch, S Skorobogatov, RJ Anderson, "Chip and Skim: cloning EMV cards with the pre-play attack", *IEEE Symposium on Security and Privacy* (2014)

[284] M Bond, D Cvrček, S Murdoch, *'Unwrapping the Chrysalis'*, Cambridge Computer Lab Tech Report no. 592, 2004

[285] M Bond, SJ Murdoch, J Clulow, *'Laser-printed PIN Mailer Vulnerability Report'*, 2005, at `https://murdoch.is/papers/cl05pinmailer-vuln.pdf`

[286] 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

[287] D Boneh, M Franklin, "Identity-Based Encryption from the Weil Pairing", in *Advances in Cryptology – Proceedings of CRYPTO 2001*, Springer LNCS 2139 pp 213–29

[288] D Boneh, V Shoup, *'A Graduate Course in Applied Cryptography'*, `https://cryptobook.us`, 2017

[289] 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

[290] J Bonneau, "Guessing human-chosen secrets", PhD thesis, *Cambridge University Computer Laboratory Tech Report 819*, 2012

[291] J Bonneau, "Deep Dive: EFF's New Wordlists for Random Passphrases" *EFF* July 19 2016

[292] J Bonneau, E Bursztein, I Caron, R Jackson, M Williamson, "Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google", *WWW 2015*

[293] J Bonneau, C Herley, PC van Oorschot, F Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes", *IEEE Security & Privacy 2012*, and full-length version as technical report

[294] J Bonneau, A Miller, J Clark, A Narayanan, JA Kroll, EW Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies" *IEEE Security & Privacy* (2015)

[295] J Bonneau, S Preibusch, "The password thicket: technical and market failures in human authentication on the web", *WEIS 2010*

[296] J Bonneau, S Preibusch, R Anderson, "A birthday present every eleven wallets? The security of customer-chosen banking PINs", *Financial Cryptography 2012*

[297] J Bonneau, E Shutova, "Linguistic properties of multi-word passphrases," *USEC 2012*

[298] SC Bono, M Green, A Stubblefield, A Juels, AD Rubin, M Szydlo, "Security Analysis of a Cryptographically-Enabled RFID Device", *Usenix 2005*

[299] V Bontchev, "Possible macro virus attacks and how to prevent them", in *Computers and Security* v 15 no 7 (96) pp 595–626

[300] N Borisov, I Goldberg, D Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", at *Mobicom 2001*

[301] NS Borenstein, "Perils and Pitfalls of Practical Cybercommerce", in *Communications of the ACM* v 39 no 6 (June 96) pp 36–44

[302] F Boudot, P Gaudry, A Guillevic, N Heninger, E Thomé, P Zimmermann, "Factorization of RSA-250", *Cado-nfs-discuss mailing list* Feb 28 2020

[303] E Bovenlander, invited talk on smartcard security, *Eurocrypt 97*, reported in [108]

[304] E Bovenlander, RL van Renesse, "Smartcards and Biometrics: An Overview", in *Computer Fraud and Security Bulletin* (Dec 95) pp 8–12

[305] O Bowcott, "UK-US surveillance regime was unlawful 'for seven years'", *The Guardian* Feb 6 2015

[306] 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

[307] D Bowen, *'Top-to-Bottom Review'*, Aug 2007, at `http://www.sos.ca.gov/elections/elections_vsr.htm`

[308] J Bowen, "Expulsion of diplomat sends a strong signal to Israel", *BBC News*, Mar 23 2011

[309] M Brader, "Car-door lock remote control activates another car's alarm", in `comp.risks` 21.56 (Jul 2001)

[310] M Brader, "How to lose 10,000,000 pounds", in `comp.risks` v 24 no 25, Apr 19 2006

[311] T Bradshaw, "Uber loses licence to operate in London", *Financial Times* Nov 25 2019

[312] RM Brady, RJ Anderson, "Maxwell's fluid model of magnetism", *arXiv 1502.05926* Feb 20 2015

[313] 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

[314] R Brandom, "Your phone's biggest vulnerability is your fingerprint", *The Verge* May 2, 2016

[315] S Brands, *'Rethinking Public Key Infrastructures and Digital Certificates – Building in Privacy'*, MIT Press 2000

[316] 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

[317] H Bray, " 'Face testing' at Logan is found lacking", in *Boston Globe* July 17 2002

[318] M Brelis, "Patients' files allegedly used for obscene calls", in *Boston Globe* April 11, 1995; also in `comp.risks` v 17 no 7

[319] M Brennan, S Afroz, R Greenstadt, "Adversarial stylometry: Circumventing authorship recogition to preserve privacy and anonymity", *ACM Transactions on Information System Security* v 15 no 3 (Nov 2012)

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

[321] B Brewin, "CAC use nearly halves DOD network intrusions, Croom says", in *fcw.com*, Jan 25 2007, at `http://www.fcw.com/article97480-01-25-07`

[322] T Brewster, "Inside America's Secretive Research Hub: Collecting Fingerprints from Facebook, Hacking Smartwatches and Fighting COVID-19", *Forbes* Jul 13 2020

[323] D Brin, *'The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?'* Perseus Press (1999) magazine version in *Wired*, Dec 1996, at `http://www.wired.com/wired/archive/4.12/fftransparent.html`

[324] R Briol "Emanation: How to keep your data confidential", in *Symposium on Electromagnetic Security For Information Protection, SEPI 91*, Rome, 1991

[325] British Standard 8220-1.2000, *'Guide for Security of Buildings Against Crime – part 1: Dwellings'*

[326] WJ Broad, J Markoff, DE Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *New York Times* Jan 15 2011

[327] J Brodkin, "FCC requires anti-robocall tech after 'voluntary' plan didn't work out", *Ars Technica* Apr 1 2020

[328] M Broersma, "Printer makers rapped over refill restrictions", *ZDnet*, Dec 20 2002, at `http://news.zdnet.co.uk/story/0,,t269-s2127877,00.html`

[329] F Brooks, *'The Mythical Man-Month: Essays on Software Engineering'*, Addison-Wesley (1995 Anniversary Edition)

[330] I Brown, CT Marsden, J Lee, M Veale, *'Cybersecurity for Elections – a Commonwealth Guide to Best Practice'*, Commonwealth Secretariat, 2020

[331] D Brumley, D Boneh, "Remote timing attacks are practical", in *Computer Networks* v 48 no 5 (Aug 2005) pp 701–716

[332] D Brown, "Unprovable Security of RSA-OAEP in the Standard Model", IACR eprint no 2006/223, at `http://eprint.iacr.org/2006/223`

[333] JDR Buchanan, RP Cowburn, AV Jausovec, D Petit, P Seem, XO Gang, D Atkinson, K Fenton, DA Allwood, MT Bryan, "Fingerprinting documents and packaging", in *Nature* v 436 no 28 (July 2005) p 475

[334] JM Buchanan, "The Constitution of Economic Policy", 1986 Nobel Prize Lecture, at `http://nobelprize.org/nobel_prizes/economics/laureates/1986/buchanan-lecture.html`

[335] RT Buchanan, "Stag party member claims he was 'grossly exploited' by lap dancing club Spearmint Rhino after spending third of his salary in single evening", *The Independent* Nov 11 2014

[336] J Buckman, MJ Hashim, T Woutersen, J Bockstedt, "Fool Me Twice? Data Breach Reductions Through Stricter Sanctions", *SSRN 3258599* Oct 31 2018

[337] 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`

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

[339] R Buhren, C Werling, JP Seifert, "Insecure Until Proven Updated: Analyzing AMD SEV's Remote Attestation", *CCS 2019*

[340] J Van Bulck, M Minkin, O Weisse, D Genkin, B Kasikci, F Piessens, M Silberstein, TF Wenisch, Y Yarom, R Strackx, "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution", *Usenix Security 2018*

[341] J Van Bulck, D Moghimi, M Schwarz, M Lipp, M Minkin, D Genkin, Y Yarom, B Sunar, D Gruss, F Piessens, "Lvi: Hijacking Transient Execution through Microarchitectural Load Value Injection", *IEEE Symposium on Security and Privacy* (2020)

[342] Bull, Dassault, Diebold, NCR, Siemens Nixdorf and Wang Global, *'Protection Profile: Automatic Cash Dispensers / Teller Machines'*, version 1.0 (1999), at `http://www.commoncriteriaportal.org/`

[343] DB Bulloch, "Tracking terrorist finances: The SWIFT program and the American Anti-Terrorist Finance Regime", *Amsterdam Law Forum v 3* (2011), SSRN 1964531

[344] 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`

[345] Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency), *'Elektromagnetische Schirmung von Gebäuden'*, 2007, BSI TR-03209

[346] Bundesverfassungsgericht, "Beschluss des Ersten Senats", Apr 4 2006, 1 BvR 518/02 Absatz-Nr. (1–184), at `http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html`

[347] 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

[348] M Burgess, "North Korea's elite hackers are funding nukes with crypto raids", *Wired* Apr 3 2019

[349] J Burke, P Warren, "How mobile phones let spies see our every move", in *The Observer* Oct 13 2002; at `http://observer.guardian.co.uk/uk_news/story/0,6903,811027,00.html`

[350] Buro Jansen & Janssen, *'Making up the rules: interception versus privacy'*, Aug 8 2000, at `http://www.statewatch.org/news/2002/nov/11jj.htm`

[351] N Burow, SA Carr, J Nash, P Larsen, M Franz, S Brunthaler, M Payer, "Control-Flow Integrity: Precision, Security, and Performance", *ACM Computing Surveys, 2017*

[352] 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

[353] T Burt, "New action to disrupt world's largest online criminal network", *Microsoft on the issues*, Mar 10 2020

[354] G Burton "Equifax used default 'admin' user name and password to secure hacked portal", *Computing* Oct 21 2019

[355] G Burton, "IT security specialists need to look at IoT security in buildings in a completely different way, says Cundall director Chris Grundy", *Computing* July 12 2019

[356] G Burton, "More than 600 US government entities hit with ransomware so far this year – and it's only going to get worse", *Computing* Oct 1 2019

[357] G Burton, "Google removes Avast and AVG extensions from Chrome web store over 'unnecessary' data collection", *Computing* Dec 18 2019

[358] J Busch, "How to Hack RWPFE Water Filters for Your GE Fridge", *Groovypost* May 7 2020

[359] L Butler, "Post Office boss receives 7% pay rise as postmaster salaries cut", *The Guardian* Oct 19 2018

[360] RW Butler, GB Finelli, "The infeasibility of experimental quantification of life-critical software reliability", in *ACM Symposium on Software for Critical Systems* (1991) pp 66–76

[361] D Byler, "The Global Implications of 'Re-education' Technologies in Northwest China", *Center for Global Policy* Jun 8 2020

[362] RW Byrne, A Whiten, *'Machiavellian Intelligence – Social Expertise and the Evolution of Intellect in Monkeys, Apes and Humans'*, Oxford, 1988; see also A Whiten, RW Byrne, *'Machiavellian Intelligence II – Extensions and Evaluations'*, Cambridge 1997

[363] Cabinet Office, *'National Risk Register Of Civil Emergencies'*, 2017

[364] *'A Comparative Introduction to 4G and 5G Authentication'*, Cable Labs, Winter 2019

[365] C Cadwalladr, "Facebook's role in brexit – and the threat to democracy", *TED2019*

[366] E Caesar, "The Cold War Bunker That Became Home to a Dark-Web Empire", *New Yorker*, July 27 2020

[367] L Cai, H Chen, "On the practicality of motion based keystroke inference attack", *Proceedings of the 5th International Conference on Trust and Trustworthy Computing, TRUST'12* pp 273–290

[368] A Cain, "Before Envelopes, People Protected Messages With Letterlocking", *Atlas Obscura* Nov 9 2018, at `https://www.atlasobscura.com/articles/what-did-people-do-before-envelopes-letterlocking`

[369] F Caldicott, *'Report on the review of patient-identifiable information'*, Department of Health, 1997

[370] RE Calem, "New York's Panix Service Is Crippled by Hacker Attack", *New York Times* Sep 14 1996

[371] A Caliskan, JJ Bryson, A Narayanan, "Semantics derived automatically from language corpora contain human-like biases", *Science* v 356 no 6334 pp 183–186

[372] A Caliskan-Islam, R Harang, A Liu, A Narayanan, C Voss, F Yamaguchi, R Greenstadt, "De-anonymizing programmers via code stylometry", *USENIX Security* (2015) pp 255-270

[373] J Camp, C Wolfram, "Pricing Security", in *Proceedings of the CERT Information Survivability Workshop* (Oct 24-26 2000) pp 31–39

[374] J Camp, S Lewis, *'Economics of Information Security'*, Springer 2004

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

[376] D Campbell, "Making history: the original source for the 1988 first Echelon report steps forward", (25 February 2000), at `http://cryptome.org/echelon-mndc.htm`

[377] D Campbell, "Operation Ore Exposed", *PC Pro*, Jul 2005, archived at `https://www.duncancampbell.org/content/operation-ore`

[378] D Campbell, "Sex, Lies and the Missing Videotape", *PC Pro*, Apr 2007, archived at `https://www.duncancampbell.org/content/operation-ore`

[379] D Campbell, P Lashmar, "The new Cold War: How America spies on us for its oldest friend – the Dollar", in *The Independent* (2 July 2000)

[380] K Campbell, L Gordon, M Loeb, L Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", in *Journal of Computer Security* v 11 no 3 (2003) pp 431–448

[381] O Campion-Awwad, A Hayton, L Smith, M Vuaran, "The National Programme for IT in the NHS", Cambridge 2014, at `https://www.lightbluetouchpaper.org/2014/08/13/largest-ever-civil-government-it-disaster/`

[382] C Canella, J Van Bulck, M Schwarz, M Lipp, B von Berg, P Ortner, F Piessens, D Evtyushkin, D Gruss, "A Systematic Evaluation of Transient Execution Attacks and Defenses", *USENIX Security Symposium* 2019

[383] C Canella, M Schwarz, M Haubenwallner, M Schwarzl, D Gruss, "KASLR: Break it, Fix it, Repeat", *ACM CCS* (2020)

[384] C Cant, S Wiseman, "Simple Assured Bastion Hosts", in *13th Annual Computer Security Application Conference* (1997) pp 24–33

[385] "Dark horse in lead for fingerprint ID card", *Card World Independent* (May 94) p 2

[386] "German A555 takes its toll", in *Card World International* (12/94–1/95) p 6

[387] BL Cardin, *'Putin's Asymmetric Assault on Democracy in Russia and Europe – Implications for U.S. National Security'* Minority Staff Report, Committee on Foreign Relations, U.S. Senate, Jan 10 2018

[388] "High tech helps card fraud decline", in *Cards International* no 117 (29 Sep 94)

[389] "Visa beefs up its anti-fraud technology", in *Cards International* no 189 (12/12/97) p 5

[390] JM Carlin, "UNIX Security Update", at *Usenix Security 93* pp 119–130

[391] M Carr, SF Shahandashti, "Revisiting Security Vulnerabilities in Commercial Password Managers", *arXiv 2003.01985* Mar 17 2020

[392] J Carroll, *'Big Blues: The Unmaking of IBM'*, Crown Publishers 1993

[393] H Carter, "Car clock fixer jailed for nine months", in *The Guardian* Feb 15 2000

[394] R Carter, "What You Are … Not What You Have", in *International Security Review* Access Control Special Issue (Winter 93/94) pp 14-16

[395] A Case, M Meltzer, S Adair, "Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs", *Volexity* Sep 2 2019

[396] M Castro, B Liskov, "Practical Byzantine Fault Tolerance", *Symposium on Operating Systems Design and Implementation* (1999)

[397] L Cauley, "NSA has massive database of Americans' phone calls", in *USA Today* Nov 11 2005, at `http://www.usatoday.com/news/washington/2006-05-10-nsa:x.htm`

[398] E Cebuc, "How are we doing with Android's overlay attacks in 2020?" *F-secure Labs* Mar 27 2020

[399] M Ceglowski, "What I Learned Trying To Secure Congressional Campaigns", *Idlewords*, May 26 2019, at `https://idlewords.com/2019/05/what_i_learned_trying_to_secure_congressional_campaigns.htm`

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

[401] L Cerulus, "EU Commission to staff: Switch to Signal messaging app", *Politico Pro* Feb 20 2020

[402] Chainalysis *'Crypto Crime Report'*, January 2019

[403] Chainalysis *'The 2020 State of Crypto Crime'*, January 2020

[404] "The Nature and Scope of Governmental Electronic Surveillance Activity", Center for Democracy and Technology, July 2006

[405] D Cerdeira, N Santos, P Fonseca, S Pinto, "SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems", *IEEE Symposium on Security and Privacy* 2020

[406] P Chain, F Filloux, "Code, on wheels: Reinventing the car, episode 5" *Mondaynote*, Aug 9 2020

[407] A Chakraborty, "How Boots went rogue", *The Guardian* Apr 13 2016

[408] Chaos Computer Club, *'How to fake fingerprints?'* at `https://web.archive.org/web/20090327044558/http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en` (2004)

[409] L Chapman, *'Your disobedient servant'*, Penguin Books 1979

[410] Chartered Institute of Building Services Engineers, *'Security Engineering'*, Applications Manual AM4 (1991)

[411] M Chase, T Perrin, G Zaverucha, "The Signal Private Group System and Anonymous Credentials Supporting Efficient Verifiable Encryption", *Cryptology ePrint 2019/1416* Dec 10 2019

[412] D Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", in *Communications of the ACM* v 24 no 2 (Feb 1981)

[413] D Chaum, "Blind signatures for untraceable payments", in *Crypto 82*, Plenum Press (1983) pp 199–203

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

[415] S Checkoway, J Maskiewicz, C Garman, J Fried, S Cohney, M Green, N Heninger, R-P Weinmann, E Rescorla, H Shacham, "A Systematic Analysis of the Juniper Dual EC Incident", *CCS 2016*

[416] A Chen, "The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed", *Wired* Oct 23 2014

[417] YS Cheng, XY Ji, TY Lu, WY Xu, "DeWiCam: Detecting Hidden Wireless Cameras via Smartphones" *AsiaCCS* 2018

[418] R Chesney, "Telephony Metadata: Is the Contact-Chaining Program Unsalvageable?" *Lawfare Blog* March 6 2019

[419] K Chiu, "The world's biggest online population is staying home and China's internet can't cope", *Abacus News* Feb 17 2020

[420] " 'Trial by Internet' Casts Spotlight on Korean Cyber Mobs", *Chosun Ilbo* July 8 2005

[421] MO Choudary, MG Kuhn, "Efficient, portable template attacks", *IEEE Transactions on Information Forensics and Security* v 13 no 2 (Feb 2018)

[422] T Christakis, "A fragmentation of EU/ECHR law on mass surveillance: initial thoughts on the Big Brother Watch judgment", *European Law blog* Sep 20 2018

[423] N Christin, " Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace", *WWW* 2013

[424] KH Chuang, E Bury, R Degraeve, B Kaczer, G Groeseneken, I Verbauwhede, D Linten, "Physically unclonable function using CMOS breakdown position", *IEEE International Reliability Physics Symposium (IRPS)* (2017)

[425] F Church (chairman), *'Intelligence Activities – Senate Resolution 21'*, US Senate, 94 Congress, First Session, at `http://cryptome.org/nsa-4th.htm`

[426] RB Cialdini, *'Influence: Science and Practice'*, Pearson 2009

[427] WS Ciciora, "Inside the set-top box", in *IEEE Spectrum* v 12 no 4 (Apr 95) pp 70–75

[428] C Cimpanu, "Newer Diameter Telephony Protocol Just As Vulnerable As SS7", *Bleeping Computer* July 2 2018

[429] C Cimpanu, "Backdoor found in Ruby library for checking for strong passwords", *ZDNet* July 8 2019

[430] C Cimpanu, "DNS-over-HTTPS causes more problems than it solves, experts say", *ZDNet* Oct 6 2019

[431] C Cimpanu, "Major vulnerability patched in the EU's eIDAS authentication system", *ZDNet* Oct 29 2019

[432] C Cimpanu, "Average tenure of a CISO is just 26 months due to high stress and burnout", *ZDNet* Feb 12 2020

[433] C Cimpanu, "Android malware can steal Google Authenticator 2FA codes", *ZDNet* Feb 27 2020

[434] C Cimpanu, "Microsoft Double Key Encryption enters public preview", *ZDNet* Jul 21 2020

[435] C Cimpanu, "China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI", *ZDNet* Aug 8 2020

[436] J Cipriani, "iOS 13: Top 5 new security and privacy features for your iPhone", *CNet* Sep 22 2019

[437] D Cireşan, U Meier, J Schmidhuber, "Multi-column deep neural networks for image classification", *arXiv:1202.2745* Feb 13 2012

[438] 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

[439] P Clark, H Warrell, T Bradshaw, S Neville "The rise and fall of Hancock's homegrown tracing app", *Financial Times* Jun 26 2020

[440] R Clark, *'The man who broke Purple'*, Little, Brown 1977

[441] I Clarke, *'The Free Network Project Homepage'*, at `http://freenet.sourceforge.net/`

[442] RW Clarke, "The Theory of Crime prevention Though Environmental Design"; see also *'Situational Crime Prevention: successful case studies'*, Harrow and Heston 1997

[443] R Clayton, "Techno-Risk", at *Cambridge International Symposium on Economic Crime* (2003), at `http://www.cl.cam.ac.uk/~rnc1/talks/030910-TechnoRisk.pdf`

[444] R Clayton, *'Anonymity and traceability in cyberspace'*, PhD Thesis; Cambridge University Technical Report UCAM-CL-TR-653, 2005

[445] R Clayton, "Insecure Real-Word Authentication Protocols (or Why Phishing is so Profitable)", at *Cambridge Security Protocols Workshop* 2005

[446] R Clayton, *private conversation*, 2006

[447] R Clayton, "When firmware attacks! (DDoS by D-Link)", *Light Blue Touchpaper*, Apr 7 2006

[448] R Clayton, "ClimateGate Email 'Hacking' ", 2009, at `https://www.cl.cam.ac.uk/~rnc1/climategate-20091215.pdf`

[449] R Clayton, M Bond, "Experience Using a Low-Cost FPGA Design to Crack DES Keys", *CHES Workshop* (2002), Springer LNCS 2523 pp 579–592

[450] R Clayton, SJ Murdoch, R Watson, "Ignoring the Great Firewall of China", at *6th Workshop on Privacy Enhancing Technologies* (2006)

[451] J Clulow, *'The Design and Analysis of Cryptographic APIs for Security Devices'*, MSc Thesis, University of Natal 2003

[452] FB Cohen, *'A Short Course on Computer Viruses'*, Wiley 1994

[453] K Cohn-Gordon, C Cremers, L Garratt, "Post-Compromise Security", *IACR preprint*, v 1.4 Oct 2019

[454] D Coldewey, "Uber in fatal crash detected pedestrian but had emergency braking disabled", *TechCrunch* May 24 2018

[455] B Collier, "The power to structure: exploring social worlds of technology, privacy and power in the Tor project", *Information, Communication and Society* (2020), `https://www.cl.cam.ac.uk/~bjc63/power_to_structure.pdf`

[456] B Collier, R Clayton, A Hutchings, D Thomas, "Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies", *Workshop on the Economics of Information Security* (2020)

[457] B Collier, D Thomas, R Clayton, A Hutchings, "Booting the booters: measuring the impact of law enforcement interventions on DoS markets", Internet Measurement Conference 2019

[458] P Collier, A Hoeffler, "Greed and grievance in civil war", in *Oxford Economic Papers* v 56 (2004) pp 563–595

[459] A Collins, "Court decides software time-locks are illegal", in *Computer Weekly* (19 August 93) p 1

[460] D Cohen, J Hashkes, "A system for controlling access to broadcast transmissions", European Patent no EP0428252

[461] "Telecomms Fraud in the Cellular Market: How Much is Hype and How Much is Real?' in *Computer Fraud and Security Bulletin* (Jun 97) pp 11–14

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

[463] Common Criteria, 'Collaborative Protection Profiles – The Benefits of an Evolved Common Criteria Implementation', Sep 2014

[464] *'Communicating Britain's Future'*, at `http://www.fipr.org/polarch/labour.html`

[465] A Compagno, M Conti, D Lain, G Tsudik, "Don't Skype & Type! Acoustic Eavesdropping in Voice-Over-IP", *arXiv:1609.09359* (2016); later *ASIA CCS* 2017 pp 703–715

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

[467] "Samsung rushes out fix for Galaxy S10 fingerprint security flaw", *Computing News* Oct 24 2019

[468] JB Condat, "Toll fraud on French PBX systems", in *Computer Law and Security Report* v 10 no 2 (Mar/April 94) pp 89–91

[469] D Conner, "Cryptographic techniques — secure your wireless designs", in *EDN* (18/1/96) pp 57–68

[470] K Connolly, "Treasures worth 'up to a billion euros' stolen from Dresden museum", *The Guardian* Nov 25 2019

[471] L Constantin, "One year after DigiNotar breach, Fox-IT details extent of compromise", *PC World* Oct 31 2012

[472] US Consumer Reports, *'2009 Chevy Malibu vs 1959 Bel Air Crash Test'*, 2009, at `https://www.youtube.com/watch?v=fPF4fBGNK0U`

[473] D Coppersmith, *'The Data Encryption Standard (DES) and its Strength Against Attacks'*, IBM report RC 18613 (81421)

[474] M Coppins, "The Billion-Dollar Disinformation Campaign to Reelect the President", *The Atlantic* Feb 10 2020

[475] Council of Europe, *'Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data'*, European Treaty Series no 108 (January 28, 1981)

[476] FJ Corbató, "On building systems that will fail", *Communications of the ACM* v 4 no 9, (1991) pp 72–81

[477] R Cordery, L Pintsov, "History and Role of Information Security in Postage Evidencing and Payment", in *Cryptologia* v XXIX no 3 (Jul 2005) pp 257–271

[478] S Cordier, "Bracelet électronique, ordonnance de protection, TGD … Ce que contient la loi sur les violences conjugales", *Le Monde* Dec 18 2019

[479] V Costan, S Devadas, "Intel SGX Explained", *IACR Cryptology ePrint 2016/086* (2016)

[480] F Courbon, SP Skorobogatov, C Woods, "Reverse engineering Flash EEPROM memories using scanning electron microscopy", *International Conference on Smart Card Research and Advanced Applications* (2016) pp 57–72

[481] G Corfield, "I helped catch Silk Road boss Ross Ulbricht: Undercover agent tells all" *The Register* Jan 29 2019

[482] G Corfield, "Proposed US fix for Boeing 737 Max software woes does not address Ethiopian crash scenario, UK pilot union warns" *The Register* Sep 23 2020

[483] L Cosmides, J Tooby, "Cognitive adaptations for social exchange", in *The Adapted Mind: Evolutionary psychology and the generation of culture* (1992)

[484] 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

[485] J Cox, "Criminals Are Tapping into the Phone Network Backbone to Empty Bank Accounts", *Vice* Jan 31 2019

[486] J Cox, "Hackers Are Breaking Directly Into Telecom Companies to Take Over Customer Phone Numbers", *Vice* Jan 10 2020

[487] J Cox, "Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years", *Vice* Feb 6 2019

[488] J Cox, "Malware That Spits Cash Out of ATMs Has Spread Across the World", *Vice* Oct 15 2019

[489] J Cox, "The Companies That Will Track Any Phone on the Planet", *The Daily Beast* Aug 28 2017

[490] LH Cox, JP Kelly, R Patil, "Balancing quality and confidentiality for multivariate tabular data" in *Privacy in Statistical Data Bases* (2004) Springer LNCS v 3050 pp 87–98

[491] J Cradden, "Printer-makers hit by new EU law", in *Electricnews.net* December 19 2002, at `http://www.electricnews.net/news.html?code=8859027`

[492] L Cranor, "Time to rethink mandatory password changes", *Tech@FTC blog* Mar 2 2016

[493] L Cranor, S Garfinkel, *'Security Usability'*, O'Reilly 2005

[494] S Craver, "On Public-key Steganography in the Presence of an Active Warden", in *Second International Workshop on Information Hiding* (1998), Springer LNCS v 1525 pp 355–368

[495] SA Craver, M Wu, BD Liu, A Stubblefield, B Swartzlander, DS Wallach, D Dean, EW Felten, "Reading Between the Lines: Lessons from the SDMI Challenge", in *Usenix Security Symposium* (2000)

[496] RJ Creasy, "The origin of the VM/370 time-sharing system", in *IBM Journal of Research & Development* v 25 no 5 (Sep 1981) pp 483–490

[497] J Crémer, YA de Montjoye, H Schweizter, *'Competition Policy for the digital era'*, European Commission DG Competition, 2019

[498] C Criado Perez, *'Invisible Women'*, Chatto & Windus 2019

[499] "El Gobierno dice que le hackearon el Boletín Official con falsas resoluciones sobre coronavirus", EL Cronista, Mar 15 2020

[500] H Crouch, "Two NHS trusts sign agreements with Sensyne Health", *DigitalHealth* Feb 4 2019

[501] Cryptome.org, Deepwater documents, May 2007; at `http://cryptome.org/deepwater/deepwater.htm`

[502] C Culnane, BIP Rubinstein, V Teague, "Stop the Open Data Bus, We Want to Get Off", *arXiv:1908.05004* Aug 15 2019

[503] J Cumberledge, *'First Do No Harm – The report of the Independent Medicines and Medical Devices Review'*, UK Department for Health and Social Care, July 2020

[504] W Curtis, H Krasner, N Iscoe, "A Field Study of the Software Design Process for Large Systems", in *Communications of the ACM* v 31 no 11 (Nov 88) pp 1268–87

[505] F D'Addario, "Testing Security's Effectiveness", in *Security Management Online* October 2001

[506] T Dafoe, "A Hacker Posing as a Venerable British Art Dealer Swindled a Dutch Museum Out of $3.1 Million", *Artnet News*, Jan 30 2020

[507] J Daemen, V Rijmen, *'The Design of Rijndael: AES – The Advanced Encryption Standard'*, Springer (2002)

[508] P Daian, S Goldfeder, T Kell, YQ Li, XY Zhao, I Bentov, L Breidenbach, A Juels, "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges", *arXiv:1904.05234* Apr 10 2019

[509] G Danezis, "Distributed Ledgers: what is so interesting about them?" *Conspicuous Chatter* Sep 27 2018

[510] G Danezis, B Wittneben, "The Economics of Mass Surveillance", *Fifth Workshop on the Economics of Information Security* (2006)

[511] G Danezis, RJ Anderson, "The Economics of Resisting Censorship", in *IEEE Security and Privacy* v 3 no 1 (2005) pp 45–50

[512] G Danezis, C Diaz, "Survey of Privacy Technology", 2007, at `http://homes.esat.kuleuven.be/~gdanezis/anonSurvey.pdf`

[513] JM Darley, B Latané, "Bystander Intervention in Emergencies: Diffusion of Responsibility", *Journal of Personality and Social Psychology* v 8 no 4 Pt 1 pp 377–383

[514] M Darman, E le Roux, "A new generation of terrestrial and satellite microwave communication products for military networks", in *Electrical Communication* (Q4 94) pp 359–364

[515] Two statements, made by the Data Protection Commissioners of EU and EES countries and Switzerland, *20th International Conference on Data Protection*, Santiago de Compostela, 16-18 September 1998

[516] Daubert v. Merrell Dow Pharmaceuticals, 113 S. Ct. 2786 (1993)

[517] J Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", in *IEEE Transactions on Pattern Analysis and Machine Intelligence* v 15 no 11 (Nov 93) pp 1148–1161

[518] J Daugman, *'Biometric decision landscapes'*, Technical Report no TR482, University of Cambridge Computer Laboratory.

[519] J Daugman, C Downing "Searching for doppelgängers: assessing the universality of the IrisCode impostors distribution," IET Biometrics (2015)

[520] G Davidson, "Scottish Government to scrap Named Person scheme, John Swinney confirms", *The Scotsman* Sep 19 2019

[521] DW Davies, WL Price, *'Security for Computer Networks'* Wiley 1984

[522] G Davies, *'A history of money from ancient times to the present day'*, University of Wales Press 1996

[523] W Davies, "What's wrong with WhatsApp", *The Guardian* Jul 2 2020

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

[525] J Davis, "Hackers Take Down the Most Wired Country in Europe", in *Wired*, Aug 21 2007

[526] D Deahl, "This 10-year-old was able to unlock his mom's iPhone using Face ID", *The Verge* Nov 14 2017

[527] 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* pp 190–200

[528] J Dean, "Google Research: Looking Back at 2019, and Forward to 2020 and Beyond ", *Google AI Blog*, Jan 9 2020

[529] C Deavours, D Kahn, L Kruh, G Mellen, B Winkel, *'Cryptology – Yesterday, Today and Tomorrow'*, Artech House (1987)

[530] C Deavours, D Kahn, L Kruh, G Mellen, B Winkel, *'Selections from Cryptologia – History, People and Technology'*, Artech House (1997)

[531] C Deavours, L Kruh, *'Machine Cryptography and Modern Cryptanalysis'*, Artech House 1985

[532] JF de Beer, "Constitutional Jurisdiction Over Paracopyright Laws", in *'The Public Interest: The Future of Canadian Copyright Law'*, Irwin Law (2005)

[533] CC Demchak, Y Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking", *Military Cyber Affairs* v 3 no 1 `https://scholarcommons.usf.edu/mca/vol3/iss1/7`

[534] B Demoulin, L Kone, C Poudroux, P Degauque, "Electromagnetic Radiation of Shielded Data Transmission Lines", in [701] pp 163–173

[535] 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

[536] I Denley, S Weston-Smith, "Privacy in clinical information systems in secondary care" in *British Medical Journal* v 318 (15 May 1999) pp 1328–1331

[537] DE Denning, "The Lattice Model of Secure Information Flow", in *Communications of the ACM* v 19 no 5 pp 236–248

[538] DE Denning, *'Cryptography and Data Security'*, Addison-Wesley 1982

[539] DE Denning, *'Information Warfare and Security'*, Addison-Wesley 1999

[540] DE Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", InfowarCon 2000

[541] DE Denning, PJ Denning, M Schwartz, "The tracker: a threat to statistical database security", in *ACM Transactions on Database Systems* v 4 no 1 (1979) pp 76–96

[542] DE Denning, PH MacDoran, "Location-Based Authentication: Grounding Cyberspace for Better Security", in *Computer Fraud and Security Bulletin* (Feb 96) pp 12–16

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

[544] Department of Defense, *'Department of Defense Trusted Computer System Evaluation Criteria'*, DoD 5200.28-STD, December 1985

[545] Department of Defense, *'A Guide to Understanding Covert Channel Analysis of Trusted Systems'*, NCSC-TG-030 (Nov 1993)

[546] Department of Defense, *'Password Management Guideline'*, CSC-STD-002-85 (1985)

[547] Department of Defense, *'A Guide to Understanding Data Remanence in Automated Information Systems'*, NCSC-TG-025 (1991)

[548] Department of Defense, *'Technical Rationale behind CSC-STD-003-85: computer security requirements'*, CSC-STD-004-85 (1985)

[549] Department of Defense, News Transcript, Oct 20 2007, at `http://cryptome.org/af-squirm/af-squirm.htm`

[550] Department of Justice, *'Guidelines for Searching and Seizing Computers'*, 1994; at `http://www.epic.org/security/computer_search_guidelines.txt`

[551] Department of Justice, "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin" Oct 16 2019

[552] Department of Justice, "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax", Feb 10 2020

[553] Department of Justice, "Ohio Resident Charged with Operating Darknet-Based Bitcoin 'Mixer,' which Laundered Over $300 Million" Feb 13 2020

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

[555] B De Sutter, C Collberg, M Dalla Preda, B Wyseur, "Software protection Decision Support and Evaluation Methodologies", *Report from Dagstuhl Seminar 19331* (2019)

[556] W Diffie, ME Hellman, "New Directions in Cryptography", in *IEEE Transactions on information theory* v 22 no 6 (Nov 76) pp 644–654

[557] W Diffie, ME Hellman, "Exhaustive cryptanalysis of the NBS Data Encryption Standard", in *Computer* v 10 no 6 (June 77) pp 74–84

[558] W Diffie, S Landau, *'Privacy on the Line – The Politics of Wiretapping and Encryption'*, MIT Press 1998

[559] M van Dijk, A Juels, A Oprea, RL Rivest, "FLIPIT: The Game of 'Stealthy Takeover' ", *Journal of Cryptology* v 26 no 4 (Oct 2013) pp 655–713; given as the Crypto 2011 distinguished lecture by Ron Rivest

[560] E Dijkstra, "Solution of a problem in concurrent programming control", in *Communications of the ACM* v 8 no 9 (1965) p 569

[561] R Dingledine, "Tor security advisory: 'relay early' traffic confirmation attack", *Tor Blog*, July 30 2014

[562] I Dinur, K Nissim, "Revealing information while preserving privacy", *Principles of database systems* (2003) pp 202–210

[563] 'Profil de Protection – Machine á Voter', Direction centrale de la sécurité de systèmes d'information (2007)

[564] R Diresta, C Miller, V Molter, J Pomfret, G Tiffert, *'Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives'*, Stanford Internet Observatory, July 2020

[565] *'The Annual Bullying Survey 2018'*, Ditch the Label

[566] AK Dixit, *'Lawlessness and Economics'*, Princeton University Press, 2003

[567] RC Dixon, *'Spread Spectrum Systems with Commercial Applications'*, Wiley 1994

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

[569] T Docan-Morgan, *'The Palgrave Handbook of Deceptive Communication'*, 2019

[570] C Doctorow, "SAMBA versus SMB: Adversarial interoperability is judo for network effects", *Boing Boing* July 17 2019

[571] C Doctorow, “Three years after the W3C approved a DRM standard, it’s no longer possible to make a functional indie browser”, *BoingBoing* Jun 29 2020

[572] V Dodd, “Hundreds arrested as UK organised crime network is cracked”, *The Guardian*, Jul 2 2020

[573] M Dodson, M Vingaard, AR Beresford. “Using Global Honeypot Networks to Detect Targeted ICS Attacks”, *International Conference on Cyber Conflict (CyCon)* 2020

[574] P Doerfler, M Marincenko, J Ranieri, J Yu, A Moscicki, D McCoy, K Thomas, “Evaluating Login Challenges and a Defense Against Accout Takeover”, *IW3C2* 2019

[575] Z Doffman, “New SIM Card Spyware Attack Puts 1 Billion Mobile Phones At Risk”, *Forbes* Sep 12 2019

[576] B Dole, S Lodin, E Spafford, “Misplaced Trust: Kerberos 4 Session Keys”, in *Internet Society Symposium on Network and Distributed System Security*, IEEE, pp 60–70

[577] L Donnelly, “Security breach fears over 26 million NHS patients”, *Daily Telegraph* Mar 17 2017

[578] Z Dorfman, J McLaughlin, “The CIA’s communications suffered a catastrophic compromise. It started in Iran”, *Yahoo News*, Nov 2 2018

[579] Z Dorfman, J McLaughlin, SD Naylor, “Exclusive: Russia carried out a ‘stunning’ breach of FBI communications system, escalating the spy game on U.S. soil”, *Yahoo News* Sep 16 2019

[580] JR Douceur, “The Sybil Attack”, IPTPS 2002, `http://www.divms.uiowa.edu/~ghosh/sybil.pdf`

[581] P Drahos, J Braithwaite, *‘Information Feudalism – Who Owns the Knowledge Economy?’*, Earthscan 2002

[582] S Drimer, “Banks don’t help fight phishing”, *Light Blue Touchpaper*, Mar 10 2006

[583] S Drimer, *‘Volatile FPGA design security – a survey’*, 2007

[584] S Drimer, SJ Murdoch, “Keep your enemies close: Distance bounding against smartcard relay attacks”, in *16th USENIX Security Symposium* (2007)

[585] S Drimer, SJ Murdoch, RJ Anderson, “Optimised to Fail: Card Readers for Online Banking”, *Financial Cryptography 2009*

[586] IE Dror, D Charlton, AE Péron, “Contextual information renders experts vulnerable to making erroneous identifications”, in *Forensic Science International* 156 (2006) 74–78

[587] IE Dror, D Charlton, “Why Experts Make Errors”, in *Journal of Forensic Identification* v 56 no 4 (2006) pp 600–616

[588] I Drury, “Pointing the finger”, in *Security Surveyor* v 27 no 5 (Jan 97) pp 15–17

[589] C Duckett, “Google Project Zero shifts to full 90-day disclosures to improve patch uptake”, *ZDNet* Jan 8 2020

[590] P Ducklin, “Why 3 million Let’s Encrypt certificates are being killed off today”, *Naked security by Sophos*, Mar 4 2020

[591] C Duhigg, “Is Amazon Unstoppable?” *New Yorker* (Oct 21 2019)

[592] I Duncan, L Aratani, “FAA gives preliminary approval on design fixes for 737 Max”, *Washington Post*, Aug 3 2020

[593] JM Dutertre, V Beroulle, P Candelier, S De Castro, LB Faber, ML Flottes, P Gendrier, D Hély, R Leveugle, P Maistri, G Di Natale, A Papadimitriou, B Rouzeyre, “Laser Fault Injection at the CMOS 28 nm Technology Node: an Analysis of the Fault Model”, *Workshop on Fault Diagnosis and Tolerance in Cryptography* (2018)

[594] C Dwork, A Roth, “The Algorithmic Foundations of Differential Privacy”, *Foundations and Trends in Theoretical Computer Science* v 9 nos 3–4 (2014) pp 211–407

[595] C Dwork, F McSherry, K Nissim, A Smith, “Calibrating noise to sensitivity in private data analysis”, *Third conference on Theory of Cryptography* (2006)

[596] A Dyck, A Morse, L Zingales, “Who Blows the Whistle on Corporate Fraud?”, *Journal of Finance* Nov 9 2010; first published as NBER Working paper 12882, Feb 2007

[597] C Dyer, “Europe’s concern over UK data protection ’defects’ revealed”, in *The Guardian* Oct 1 2007

[598] N Eagle, A Pentland, D Lazer, “Inferring Social Network Structure using Mobile Phone Data”, 2007, at `http://reality.media.mit.edu/pdfs/network_structure.pdf`

[599] D Easley, J Kleinberg, “Networks, Crowds, and Markets: Reasoning About a Highly Connected World”, *Cambridge University Press* (2010)

[600] D Easter, “The impact of ‘Tempest’ on Anglo-American communications security and intelligence, 1945–1970”, *Intelligence and National Security* (2020)

[601] W van Eck, “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?” in *Computers & Security* v 4 (1985) pp 269–286, at `https://cryptome.org/emr.pdf`

[602] *The Economist*, “Living in the global goldfish bowl ”, 18-24 Dec 1999, Christmas special

[603] *The Economist*, “A price worth paying?”, May 19 2005

[604] *The Economist*, “Getting the message, at last”, Dec 13 2007

[605] *The Economist*, “Russians are shunning state-controlled TV for YouTube”, March 7 2019

[606] *The Economist*, “In genetic disease, who has the right to know—or not know—what?” (“A not-so-merry dance” in the print edition), Sep 28 2019

[607] *The Economist*, “Why states are rushing to seal tens of millions of old criminal records” Nov 14 2019

[608] *The Economist*, “The financial world’s nervous system is being rewired”, May 7 2020

[609] *The Economist*, “America does not want China to dominate 5G mobile networks”, Apr 8 2020

[610] *The Economist*, “How Wirecard fooled most of the people all of the time”, Jun 25 2020

[611] *The Economist*, “After rigging an election, Belarus’s regime beats protesters” Aug 16 2020

[612] B Edelman, “Adverse Selection in Online ‘Trust’ Certificates”, at *Fifth Workshop on the Economics of Information Security* (2006); at `http://weis2006.econinfosec.org/`

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

[614] C Edwards, “The EV life-cycle conundrum”, *Engineering and Technology (E&T)* v 18 no 8 (Aug/Sep 2020) p 26–29

[615] S Edwards, D Guido, JP Smith, E Sultanik, “Voatz Security Assessment Vol I of II: Technical Findings”, *Trail of Bits*, Mar 12 2020

[616] V Edwards, “Controversial artist Spencer Tunick protests the Facebook and Instagram ban on female nipples with a gathering of nude models in New York City”, *Daily Mail* June 2 2019

[617] 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

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

[619] Electronic Frontier Foundation, *‘Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design’*, EFF (1998); `http://cryptome.org/cracking-des.htm`

[620] Electronic Frontier Foundation, *Felten, et al., v. RIAA, et al.* at `http://www.eff.org/IP/DMCA/Felten_v_RIAA/`

[621] Electronic Frontier Foundation, “DocuColor Tracking Dot Decoding Guide”, at `http://w2.eff.org/Privacy/printers/docucolor/`

[622] G Elich, “North Korea And The Supernote Enigma”, *Korea Policy Institute* Ap 14 2008

[623] P Elkington, A Dickinson, M Mavrogordato, D Spencer, R Gillams, A De Grazia, S Rosini, D Garay Baquero, L Diment, N Mahobia, H Morgan “A Personal Respirator Specification for Health-care Workers Treating COVID-19 (PeRSo)” `https://engrxiv.org/rvcs3/`, spec and videos at `https://www.southampton.ac.uk/publicpolicy/support-for-policymakers/policy-projects/perso.page`

[624] M Ellims, J Botham, “Issues with Rules for Autonomous Vehicle Safety”, *Safety Critical Systems Club Symposium*, 2020

[625] M Ellims, “Is Security Necessary for Safety?”, in *ESCAR 2006*

[626] JH Ellis, *The History of Non-secret Encryption*, 1987, at `http://www.jya.com/ellisdoc.htm`

[627] M Elliott, E MacKey, K O’Hara, C Tudor, *‘The Anonymisation Decision-Making Framework’*, Manchester University, 2016; at `https://ukanon.net/ukan-resources/ukan-decision-making-framework/`

[628] 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`

[629] M Emms, B Arief, N Little, A van Moorsel, “Risks of Offline Verify PIN on Contactless Cards”, *Financial Cryptography* (2013) pp 313–321

[630] EMV documents available from EMVCo LLP at `http://www.emvco.com/`

[631] P Enge, T Walter, S Pullen, CD Kee, YC Chao, YJ Tsai, “Wide Area Augmentation of the Global Positioning System”, in *Proceedings of the IEEE* v 84 no 8 (Aug 96) pp 1063–1088

[632] EPIC – Electronic Privacy Information Center, `http://www.epic.org`

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

[634] 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`

[635] 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

[636] J Epstein, R Pascale, “User Interface for a High Assurance Windowing System”, in *Ninth Annual Computer Security Applications Conference* (1993), pp 256–264

[637] RG Epstein, S Ember, T Gabriel, M Baker, “How the Iowa Caucuses Became an Epic Fiasco for Democrats”, *New York Times* Feb 11 2020

[638] T Escamilla, *‘Intrusion Detection – Network Security beyond the Firewall’*, Wiley (1998)

[639] J Essinger, *‘ATM Networks – Their Organisation, Security and Future’*, Elsevier 1987

[640] *‘CYBER; Cyber Security for Consumer Internet of Things’*, ETSI EN 303 645 v 2.0.0, Nov 26 2019

[641] A Etzioni, *‘The Limits of Privacy’*, Basic Books 1999

[642] European Commission, *‘Impact assessment – amending Framework Decision 2002/475/JHA on combating terrorism’*, Brussels, Nov 6 2007, SEC(2007) 1424

[643] European Digital Rights, at `https://www.edri.org`

[644] European Parliament, *‘Development of surveillance technology and risk of abuse of economic information’*, Luxembourg (April 1999) PE 166.184 / Part 3/4, at `http://www.gn.apc.org/duncan/stoa.htm`

[645] European Parliament and Council, *‘Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC’*

[646] European Telecommunications Standards Institute, *‘CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements’*, ETSI EN 303 645 V2.1.0 (2020–04)

[647] 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

[648] European Union, *‘Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks’*, 2006/24/EC

[649] European Union, “Promoting Data Protection by Privacy Enhancing Technologies (PETs)”, COM(2007) 228 final, Brussels, May 2nd 2007

[650] European Union, *'Council Regulation (EC) No 1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology'*

[651] European Union, *'COMMISSION DIRECTIVE 2009/4/EC – counter measures to prevent and detect manipulation of records of tachographs'* Jan 23 2009

[652] European Union, *'Regulation (EU) 2017/745 of the European Parliament and of the Council'* 2017

[653] European Union, *RAPEX A12/0157/19*, Safety Gate Rapid Alert System for dangerous non-food products, Feb 2019

[654] European Union, *'ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)'*, Apr 17 2019

[655] European Union, *'Directive (EU) 2019/771 of the European Parliament and of the Council on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC'*, May 20 2019

[656] Eurosmart, *'Protection Profile – Smart Card Integrated Circuit With Embedded Software'*, 1999, at `http://www.commoncriteriaportal.org/`

[657] R Evans, D Leigh, "GM subsidiary paid conman for 'blagged' private data, court told", *The Guardian* Apr 24, 2007

[658] R Evans, "Trade unionist was refused job after police gave details to blacklist" *The Guardian* Mar 7 2019

[659] I Evtimov, WD Cui, E Kamar, E Kiciman, Ti Kohno, J Li, "Security and Machine Learning in the Real World", *arXiv:2007.07205*, Jul 3 2020

[660] M Fairhurst, "Signature verification revisited: promoting practical exploitation of biometric technology", in *Electronics and Communication Engineering Journal* v 9 no 6 (Dec 97) pp 273–280

[661] C Farivar, "Russian man pleads guilty, admits he ran notorious Kelihos botnet" *Ars Technica* Sep 13 2018

[662] K Faulkner, P Bentley, L Osborne, "Your secrets for sale: Now the NHS is in the dock after it's revealed details of patients who bought prescriptions online are sold off", *Daily Mail*

[663] B Feder, "Face-Recognition Technology Improves", *New York Times* Mar 14 2003

[664] Federal Aviation Administration, "Further Actions are Needed to Improve FAA's Oversight of the Voluntary Disclosure Reporting Program", Office of Inspector General Audit Report no. AV-2014-036, Apr 10 2014

[665] Federal Aviation Administration, "Airworthiness Directives; The Boeing Company Airplanes", *Federal Register* v 83 no 237 (Dec 11 2018) pp 63561–5

[666] Federal Aviation Administration, *'A Brief History of the FAA'*, `https://www.faa.gov/about/history/brief_history/`, June 2020

[667] Federal Committee on Statistical Methodology, *' Statistical Policy Working Paper 22 (Revised 2005) – Report on Statistical Disclosure Limitation Methodology'*

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

[669] Federal Trade Commission and Department of Commerce, *'Electronic Signatures in Global and National Commerce Act – The Consumer Consent Provision in Section 101(c)(1)(C)(ii) '*, June 2001

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

[671] Federal Trade Commission, *'ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress'*, Jan 26 2006 `http://www.ftc.gov/opa/2006/01/choicepoint.shtm`

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

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

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

[675] AP Felt, A Ainslie, RW Reeder, S Consolvo, S Thyagaraja, A Bettes, H Harris, J Grimes, "Improving SSL Warnings: Comprehension and Adherence", CHI 2015

[676] AP Felt, E Ha, S Egelman, A Haney, E Chin, D Wagner, "Android Permissions: User Attention, Comprehension, and Behavior", *SOUPS 2012*

[677] AG Ferguson, "Policing Predictive Policing", *Washington University Law Review* v 94 no 5 (2017)

[678] D Ferraiolo, R Kuhn, "Role-Based Access Control", in *15th National Computer Security Conference*, NIST (1992) pp 554–563

[679] D Ferraiolo, R Kuhn, R Chandramouli, *'Role-Based Access Control'*, Artech House 2007

[680] H Ferradi, R Géraud, D Naccache, A Tria, "When Organized Crime Applies Academic Results – A Forensic Analysis of an In-Card Listening Device", *IACR Cryptology ePrint Archive Report 2015/963*, Oct 5, 2015

[681] J Ferrigno, M Hlaváč, "When AES blinks: introducing optical side channel", *IET Information Security* v 2 no 3 (2008) pp 94–98

[682] D Fewer, P Gauvin, A Cameron, "Digital Rights Management Technologies and Consumer Privacy – An Assessment of DRM Applications Under Canadian Privacy Law", *Canadian Internet Policy and Public Interest Clinic*, September 2007

[683] A Fiat, M Naor, "Broadcast Encryption", in *Crypto '93*, Springer LNCS v 773 pp 480–491

[684] S Figueroa-Lorenzo, J Añorga, S Arrizabalaga, "A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS", *ACM Computing Surveys* v 55 no 2 (Apr 2020)

[685] PFJ Fillery, AN Chandler, "Is lack of quality software a password to information security problems?", in *IFIP SEC 94* paper C8

[686] "FCA fines RBS, NatWest and Ulster Bank Ltd £42 million for IT failures", *Financial Conduct Authority*, Nov 20 2014

[687] "Final Notice, Tesco Personal Finance plc, Reference Number 186022", *Financial Conduct Authority*, Oct 1 2018

[688] "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies", *US Financial Crimes Enforcement Network* May 9 2019

[689] "Psychologists and banks clash over merits of photographs on cards", in *Financial Technology International Bulletin* v 13 no 5 (Jan 96) pp 2–3

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

[691] A Finkelstein, M Shattuck, "CAPSA and its implementation: Report to the Audit Committee and the Board of Scrutiny, University of Cambridge", *Cambridge University Reporter* No 5861, Nov 2 2001

[692] P Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic" *Washington Post* May 19 2007

[693] ML Finucane, P Slovic, CK Mertz, J Flynn, TA Satterfield, "Gender, race, and perceived risk: the 'white male' effect", *Health, risk & society* v 2 no 2 (2000) pp 159–172

[694] G Fiorentini, S Pelzman, *'The Economics of Organised Crime'*, Cambridge University Press 1995

[695] RA Fisher, *'The Genetical Theory of Natural Selection'*, Clarendon Press, Oxford (1930); 2nd ed. Dover 1958

[696] J Flanagan, "Prison Phone Phraud (or The RISKS of Spanish)", reporting *University of Washington staff newspaper*, in `comp.risks` v 12.47 (Oct 10 1991); at `http://catless.ncl.ac.uk/Risks/12.47.html`

[697] M Fleet, "Five face sentence over notes that passed ultraviolet tests", in *The Daily Telegraph* (23/12/1999), available at `http://www.telegraph.co.uk:80/`

[698] N Fletcher, "Barclays boss Jes Staley fined £642,000 over whistleblower scandal", *The Guardian* May 11 2018

[699] E Flitter, "The Price of Wells Fargo's Fake Account Scandal Grows by $3 Billion", *New York Times* Feb 21 2020

[700] SN Foley, "Aggregation and separation as noninterference properties", in *Journal of Computer Security* v 1 no 2 (1992) pp 158–188

[701] Fondazione Ugo Bordoni, *'Symposium on Electromagnetic Security for Information Protection'*, Rome, Italy, 21–22 November 1991

[702] "Target's CEO Steps Down Following The Massive Data Breach And Canadian Debacle", *Forbes*, May 8 2014

[703] J Ford, T Kinder, "After Wirecard: is it time to audit the auditors?", *Financial Times* Jul 3 2020

[704] "The New China Scare – Why America Shouldn't Panic About Its Latest Challenger", *Foreign Affairs* Dec 6 2019

[705] S Forrest, SA Hofmeyr, A Somayaji, "Computer Immunology", in *Communications of the ACM* v 40 no 10 (Oct 97) pp 88–96

[706] DS Fortney, JJ Lim, "A technical approach for determining the importance of information in computerised alarm systems", in *Seventeenth National Computer Security Conference* (1994), proceedings published by NIST; pp 348–357

[707] K Foster, C Greene, J Stavins, "The 2018 Survey of Consumer Payment Choice: Summary results", *Federal Reserve Bank of Atlanta* (2019)

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

[709] B Fox, "Do not adjust your set . . . we have assumed radio control", in *New Scientist* 8 Jan 2000

[710] LJ Fraim, "SCOMP: A Solution to the Multilevel Security Problem", in *IEEE Computer* v 16 no 7 (July 83) pp 26–34

[711] L Franceschi-Bicchierai, "AT&T Contractors and a Verizon Employee Charged With Helping SIM Swapping Criminal Ring", *Vice* May 31 2019

[712] L Franceschi-Bicchierai, "Verizon Makes SIM Swapping Hard. Why Doesn't AT&T, Sprint, and T-Mobile?" *Vice* Sep 19 2019

[713] T Frank, "Tougher TSA bomb tests raise stakes for screeners", in *USA Today* Oct 18 2007

[714] J Franklin, V Paxson, A Perrig, S Savage, "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants", *ACM CCS* (2007)

[715] J Franks, P Hallam-Baker, J Hostetler, S Lawrence, P Leach, A Luotonen, L Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617

[716] "Banks fingerprint customers to cut cheque fraud", in *Fraud Watch* (1997) no 1 p 9

[717] "Chip cards reduce fraud in France", in *Fraud Watch* (1996) no 1 p 8

[718] "Counterfeit and cross border fraud on increase warning', in *Fraud Watch* (1996) no 1 pp 6–7

[719] "Finger minutiae system leaps the 1:100,000 false refusal barrier", in *Fraud Watch* (1996) no 2 pp 6–9

[720] "Widespread card skimming causes European concern", in *Fraud Watch* (1997) v 3 pp 1–2

[721] SJ Freedberg, "Army Awards Lockheed $75M For AI Cyber/Jamming Pod", *Breaking Defense* Apr 29 2020

[722] P Freiberger, M Swaine, *'Fire in the Valley - the Making of the Personal Computer'*, McGraw-Hill (1999)

[723] A French, "The Secret History of a Cold War Mastermind" *Wired* Mar 11 2020

[724] J Fridrich, *'Steganography in Digital Media: Principles, Algorithms, and Applications'*, Cambridge University Press 2009

[725] P Frigo, E Vannacci, H Hassan, V van der Veen, O Mutlu, C Giuffrida, H Bos, K Razavi "TRRespass: Exploiting the Many Sides of Target Row Refresh", *arXiv:2004.01807* Apr 3 2020

[726] A Frik, N Malkin, M Harbach, E Peer, S Egelman, "A Promise Is A Promise – The Effect Of Commitment Devices On Computer Security Intentions", *CHI 2019*

[727] J Frizell, T Phillips, T Groover, “The electronic intrusion threat to national security and emergency preparedness telecommunications: an awareness document”, *NCSC* (NIST, 1994) pp 378–399

[728] M Frost, *‘Spyworld: Inside the Canadian & American Intelligence Establishments’*, Diane Publishing Co (1994)

[729] N Frost, “How the McDonnell Douglas-Boeing merger led to the 737 Max crisis”, *Quartz*, Jan 3 2020

[730] DA Fulghum, “Communications Intercepts Pace EP-3s”, in *Aviation Week and Space Technology* v 146 no 19 (5/5/97) pp 53–54

[731] S Fuloria, R Anderson, F Alvarez, K McGrath, “Key Management for Substations: Symmetric Keys, Public Keys or No Keys?” at *IEEE Power Systems Conference and Exhibition (PSCE 2010)*

[732] P Fussey, D Murphy, *‘Independent Report on the London Metropolitan Police’s Trial of of Live Facial Recognition Technology’*, Human Rights Centre, University of Essex (2019)

[733] M Galecotti, “Russia’s eavesdroppers come out of the shadows”, in *Jane’s Intelligence Review* v 9 no 12 (Dec 97) pp 531–535

[734] R Gallagher, “The Inside Story of How British Spies Hacked Belgium’s Largest Telco”, *The Intercept* Dec 13 2014

[735] R Gallagher, “How U.K. Spies Hacked a European Ally and Got Away With It” *The Intercept* Feb 17 2018

[736] LA Galloway, T Yunusov, “First Contact: New Vulnerabilities in Contactless Payments”, *https://leigh-annegalloway.com/presentation-materials/* Dec 4 2019

[737] E Galperin, M Marquis-Boire, J Scott-Railton, “Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns”, *EFF and Citizen Lab*

[738] Sir, F Galton, “Personal identification and description,” in *Nature* (21/6/1888) pp 173-177

[739] Sir, F Galton, *‘Finger Prints’*, Macmillan, 1892

[740] HF Gaines, *‘Cryptanalysis – a study of ciphers and their solution’*, Dover (1939, 1956)

[741] J Gamba, M Rashed, A Razaghpanah, J Tapiador, N Vallina-Rodriguez, “An Analysis of Pre-installed Android Software”, *IEEE S&P 2020*

[742] D Gambetta, *‘Codes of the Underworld: How Criminals Communicate’*, Princeton (2009)

[743] J Gamblin, “Nearly 20% of the 1000 Most Popular Docker Containers Have No Root Password”, *Kenna Security Blog* May 20 2019

[744] T Gandy, “Brainwaves in fraud busting”, *Banking Technology* (Dec 95/Jan 96) pp 20–24

[745] F Ganji, S Tajik, JP Seifert, “Why Attackers Win: On the Learnability of XOR Arbiter PUFs’, *Trust and Trustworthy Computing* 2015 pp 22–39

[746] HC Gao, JX Yan, F Cao, ZY Zhang, L Lei, MY Tang, P Zhang, X Zhou, XQ Wang, JW Li, “A Simple Generic Attack on Text Captchas”, *NDSS 2016*

[747] FD Garcia, G de Koning Gans, R Muijrers, P van Rossum, R Verdult, R Wickers Schreur, B Jacobs, “Dismantling MIFARE Classic”, *ESORICS 2008*, Springer LNCS v 5283 pp 97–114

[748] FD Garcia, D Oswald, T Kasper, P Pavlidés, “Lock It and Still Lose It – On the (In)Security of Automotive Remote Keyless Entry Systems”, *Usenix 2016*

[749] R Gardner, A Yasinsac, M Bishop, T Kohno, Z Hartley, J Kerski, D Gainey, R Walega, E Hollander, M Gerke, *‘Software Review and Security Analysis of the Diebold Voting Machine Software’*, Florida State University, Jul 27 2007

[750] S Garfinkel, *‘Database Nation’*, O’Reilly and Associates 2000

[751] S Garfinkel, *‘Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable’*, PhD Thesis, MIT 2005, at `http://www.simson.net/thesis/`

[752] S Garfinkel, JM Abowd, C Martindale, “Understanding Database Reconstruction Attacks on Public Data”, *ACM Queue* v 16 no 5, Nov 28 2018

[753] S Garfinkel, G Spafford, *‘Practical Unix and Internet Security’*, O’Reilly and Associates (1996)

[754] B Gassend, D Clarke, M van Dijk, S Devadas, "Silicon Physical Random Functions", *ACM CCS 2002*

[755] W Gates, W Buffett, "The Bill & Warren Show", in *Fortune*, 20/7/1998

[756] B Gellman, "Edward Snowden, after months of NSA revelations, says his mission's accomplished", *Washington Post* Dec 23 2013

[757] B Gellman, D Linzer, CD Leonnig, "Surveillance Net Yields Few Suspects", *Washington Post* Feb 5 2006 p A01

[758] RM Gerecht, "The Counterterrorist Myth", in *Atlantic Monthly*, Jul-Aug 2001

[759] C Gerlinsky, "How do I Crack Satellite and Cable Pay TV?"*Chaos Communications Congress – CC33* (2016), at `https://media.ccc.de/v/33c3-8127-how_do_i_crack_satellite_and_cable_pay_tv`

[760] J Germain, "And we return to Munich's migration back to Windows – it's going to cost what now?! €100m!" *The Register* Jan 4 2018

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

[762] E German, "Legal Challenges to Fingerprints", at `http://www.onin.com/fp/daubert_links.html`

[763] JJ Gibson, *'The Ecological Approach to Visual Perception'*, Houghton Mifflin 1979

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

[765] D Gilbert, "If only gay sex caused global warming", *LA Times*, July 2 2006

[766] N Gilens, "New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance", *ACLU blog*, Sep 27 2012

[767] M Gill, A Spriggs, *'Assessing the impact of CCTV'*, UK Home Office Research Study 292

[768] J Gillum, J Kao, J Larson, "Millions of Americans' Medical Images and Data Are Available on the Internet. Anyone Can Take a Peek." *ProPublica* Sep 17 2019

[769] J Gilmore, "Nacchio affects spy probe", in *Denver Post* Oct 20 2007; cited in "NSA solicited illegal Qwest mass wiretaps right after Bush inauguration", *Cryptography List* Oct 20 2007

[770] T Gilovich, D Griffin, D Kahneman, *'Heuristics and Biases – The Psychology of Intuitive Judgment'*, Cambridge University Press 2002

[771] 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

[772] V Goel, "Verizon will pay $350 million less for Yahoo", *New York Times* Feb 21 2017

[773] WN Goetzmann, *'Financing Civilization'*, `http://viking.som.yale.edu/will/finciv/chapter1.htm`

[774] 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

[775] B Goldacre, "Care.data is in chaos. It breaks my heart", *The Guardian* Feb 28 2014

[776] I Goldberg, D Wagner, "Randomness and the Netscape browser", in *Dr Dobbs Journal* no 243 (Jan 96) pp 66–70

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

[778] S Goldwasser, S Micali, "Probabilistic encryption", in *J Comp Sys Sci* v 28 (1984) pp 270–299

[779] G Goller, G Sigl, "Side channel attacks on smartphones and embedded devices using standard radio equipment", *COSADE 2015* pp 255–270

[780] D Gollmann, *'Computer Security'*, Third edition, Wiley 2010

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

[782] R Golman, D Hagman, G Loewenstein, "Information Avoidance", *Journal of Economic Literature* v LV (Mar 2017)

[783] S Golovnev, P Gaudry, "Breaking the encryption scheme of the Moscow internet voting system", *Financial Cryptography 2020*

[784] L Gong, *'Inside Java 2 Platform Security: Architecture, API Design, and Implementation'*, Addison-Wesley (1999)

[785] L Gong, DJ Wheeler, "A matrix key-distribution scheme", in *Journal of Cryptology* v 2 no 1 (1990) pp 51–59

[786] R Gonggrijp, WJ Hengeveld, A Bogk, D Engling, H Mehnert, F Rieger, P Scheffers, B Wels, "Nedap/Groenendaal ES3B voting computer – a security analysis", Oct 2006, at `http://www.wijvertrouwenstemcomputersniet.nl/Nedap-en`

[787] D Goodin, "Anatomy of an eBay scam", in *The Register*, Mar 21 2007; at `http://www.theregister.co.uk/2007/03/21/ebay_fraud_anatomy/`

[788] D Goodin, "Firefox leak could divulge sensitive info", in *The Register*, Aug 13 2007

[789] D Goodin, "TJX agrees to pay banks $41m to cover Visa losses", in *The Channel Register*, Dec 3 2007

[790] D Goodin, "Ukrainian eBay scam turns Down Syndrome man into cash machine", in *The Register* Nov 8 2007

[791] D Goodin, "How Soviets used IBM Selectric keyloggers to spy on US diplomats", *The Register* Oct 13 2015

[792] D Goodin, "How 3ve's BGP hijackers eluded the Internet—and made $29M", *Ars Technica*, Dec 21 2018

[793] D Goodin, "Police decrypt 258,000 messages after breaking pricey IronChat crypto app", *Ars Technica*, Jul 11 2018

[794] D Goodin, "Developer of Checkm8 explains why iDevice jailbreak exploit is a game changer", *Ars Technica* Sep 28 2019

[795] D Goodin, "Five months after returning rental car, man still has remote control", *Ars Technica*, Oct 28 2019

[796] D Goodin, "Forum cracks the vintage passwords of Ken Thompson and other Unix pioneers", *Ars Technica* Oct 10 2019

[797] D Goodin, "Google Play app with 100 million downloads executed secret payloads", *Ars Technica* Aug 27 2019

[798] D Goodin, "Kingpin of Evil Corp lived large. Now there's a $5 million bounty on his head", *Ars Technica* Dec 5 2019

[799] D Goodin, "What the newly released Checkra1n jailbreak means for iDevice security", *Ars Technica* Nov 15 2019

[800] D Goodin, "A Flaw in Billions of Wi-Fi Chips Let Attackers Decrypt Data", *Wired* Feb 27 2020

[801] "Content delistings due to copyright", *Google Transparency Report* (2018), at `https://transparencyreport.google.com/copyright/overview`

[802] KE Gordon, RJ Wong, "Conducting Filament of the Programmed Metal Electrode Amorphous Silicon Antifuse", in *Proceedings of International Electron Devices Meeting*, Dec 93; reprinted as pp 6-3 to 6-10, *Quick-Logic Data Book* (1994)

[803] HM Government, *'Collection – Government security'*, at `https://www.gov.uk/government/collections/government-security` (2019)

[804] MF Grady, F Parisi, *'The Law and economics of Cybersecurity'*, Cambridge University Press, 2006

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

[806] FT Grampp, RH Morris, "UNIX Operating System Security", *AT&T Bell Laboratories Technical Journal* v 63 no 8 (Oct 84) pp 1649–1672

[807] S Granneman, "Electronic Voting Debacle", in *The Register* Nov 18 2003

[808] 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)

[809] J Gray, P Syverson, "A Logical Approach to Mulilevel Security of Probabilistic Systems," in *Distributed Computing* v 11 no 2 (1988)

[810] A Greenberg, "A 'Blockchain Bandit' Is Guessing Private Keys and Scoring Millions", *Wired* Apr 23, 2019

[811] A Greenberg, "A Mysterious Hacker Group Is On a Supply Chain Hijacking Spree", *Wired* Mar 3, 2019

[812] A Greenberg, "The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet", *Wired* May 12, 2020

[813] T Greening, "Ask and Ye Shall Receive: A Study in Social Engineering", in *SIGSAC Review* v 14 no 2 (Apr 96) pp 9–14

[814] A Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired* Aug 22 2018

[815] G Greenwald, "NSA collecting phone records of millions of Verizon customers daily", *The Guardian* June 7 2013

[816] G Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet' ", *The Guardian* July 13 2013

[817] G Greenwald, *'No Place to Hide'*, Penguin 2015

[818] G Greenwald, E MacAskill, "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian* June 9 2013

[819] G Greenwald, E MacAskill, L Poitras, "Edward Snowden: the whistleblower behind the NSA surveillance revelations", *The Guardian* June 11 2013

[820] M Gregory, P Losocco, "Using the Flask Security Architecture to Facilitate Risk Adaptable Access Controls", in *2007 Security Enhanced Linux Symposium*, at `http://selinux-symposium.org/2007/agenda.php`

[821] J Grierson, "Ringleader of gang responsible for £113m fraud jailed for 11 years", *The Guardian* Sep 21 2016

[822] A Griew, R Currell, *'A Strategy for Security of the Electronic Patient Record'*, Institute for Health Informatics, University of Wales, Aberystwyth, March 1995

[823] JM Griffin, A Shams, "Is Bitcoin Really Un-Tethered?" *SSRN 3195066* 2018

[824] H Griffiths, "Car crime rises again with 113,000 vehicles stolen last year", *Auto Express* Apr 25 2019

[825] H Griffiths, N Willis, "Klein Heidleberg – a WW2 bistatic radar system that was decades ahead of its time", (2010), at `https://www.cdvandt.org/k-h.htm`

[826] V Groebner, J Peck, M Kyburz, *'Who Are You?: Identification, Deception, and Surveillance in Early Modern Europe'*, Zone Books, 2007

[827] E Groll, " 'Obama's General' Pleads Guilty to Leaking Stuxnet Operation", *Foreign Policy* Oct 16 2016

[828] J Gross, "Keeping Patients' Details Private, Even From Kin", in *New York Times* July 3 2007

[829] P Grother, M Ngan, K Hanaoka, *'Face Recognition Vendor Test (FRVT)'* NIST IR 2871, Sep 11 2019

[830] D Grover, *'The protection of computer software – its technology and applications'*, British Computer Society / Cambridge University Press 1992

[831] D Gruhl, W Bender, "Information Hiding to Foil the Casual Counterfeiter", in *Proceedings of the Second International Workshop on Information Hiding* (Portland, Apr 98), Springer LNCS v 1525 pp 1–15

[832] L Gudgeon, P Moreno-Sanchez, S Roos, P McCorry, A Gervais, "SoK: Layer-Two Blockchain Protocols", *Financial Cryptography 2020*

[833] LC Guillou, M Ugon, JJ Quisquater, "The Smart Card – A Standardised Security Device Dedicated to Public Cryptology", in [1752] pp 561–613

[834] U Guin, K Huang, D DiMase, JM Carulli, M Tehranipoor, Y Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", *Proc IEEE* v 102 no 8 (Aug 2014)

[835] GD Guo, N Zhang, "A survey on deep learning based face recognition", *Computer Vision and Image Understanding* 189 (2019) 102805

[836] R Gupta, SA Smolka, S Bhaskar, "On Randomization in Sequential and Distributed Algorithms", in *ACM Computing Surveys* v 26 no 1 (March 94) pp 7–86

[837] M Gurman, "Apple Lets Some Video Apps Sell Shows Without Taking 30% Cut", *Bloomberg*, Apr 1 2020

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

[839] P Gutmann, "Software Generation of Practically Strong Random Numbers", in *Seventh Usenix Security Symposium Proceedings* (Jan 1998) pp 243–257

[840] P Gutmann, "Auckland's Power Outage, or Auckland – Your Y2K Beta Test Site", `https://www.cs.auckland.ac.nz/~pgut001/misc/mercury.txt` May 24 1998

[841] P Gutmann, "Data Remanence in Semiconductor Devices", in *Usenix Security Symposium* (2001)

[842] P Gutmann, "Invalid banking cert spooks only one user in 300", *Cryptography List* May 16 2005

[843] P Gutmann, "A Cost Analysis of Windows Vista Content Protection", April 2007, at `http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html`

[844] P Gutmann, "Commercial CAPTCHA-breakers for sale", *Cryptogaphy List* Oct 22 2007

[845] S Haber, WS Stornetta, "How to time-stamp a digital document", in *Journal of Cryptology* v 3 no 2 (1991) pp 99–111

[846] S Haber, WS Stornetta, "Secure Names for Bit-Strings", in *4th ACM Conference on Computer and Communications Security* (1997) pp 28–35

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

[848] "Chris Carey Arrested In New Zealand", in *Hack Watch News* (9/1/1999)

[849] C Hagen, C Weinert, S Sendner, A Dimitrienko, T Schneider, "All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers", University of Würzburg, 2020

[850] N Hager, *'Secret Power – New Zealand's Role in the International Spy Network'*, Craig Potton Publishing (1996), at `http://www.nickyhager.info/Secret_Power.pdf`

[851] N Hager, R Gallagher, "Snowden revelations / The price of the Five Eyes club: Mass spying on friendly nations", *New Zealand Herald* and *Seemorerocks* Mar 5 2015

[852] D Hakim, RJ Epstein, S Saul, "Anatomy of an Election 'Meltdown' in Georgia", *New York Times* Jul 25 2020

[853] JA Halderman, "Amazon's MP3 Store Wisely Forgoes Watermarks", Oct 2 2007, at `http://www.freedom-to-tinker.com/?p=1207`

[854] JA Halderman, N Heninger, "How is NSA breaking so much crypto?" Oct 14 2015, *Freedom to Tinker*

[855] JA Halderman, SD Schoen, N Heninger, W Clarkson, W Paul, JA Calandrino, AJ Feldman, J Appelbaum, EW Felten, "Lest we remember: cold-boot attacks on encryption keys", Communications of the ACM v 52 no 5 (2009) pp 91–98

[856] 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

[857] M Hamburg, "Understanding Intel's Ivy Bridge Random Number Generator", *Electronic Design* Dec 11 2012

[858] C Hamby, C Moses, "Boeing Refuses to Cooperate With New Inquiry Into Deadly Crash", *New York Times* Feb 6 2020

[859] J Hammer, "The Billion-dollar Bank Job", *New York Times* May 13 2018

[860] C Han, I Reyes, Á Feal, J Reardon, P Wijesekera, N Vallina-Rodriguez, A Elazari, KA Bamberger, S Egelman, "The Price is (Not) Right: Comparing Privacy in Free and Paid Apps", *PoPETS* (2020)

[861] H Handschuh, P Paillier, J Stern, "Probing attacks on tamper-resistant devices", in *Cryptographic Hardware and Embedded Systems – CHES 99* pp 303–315

[862] R Hanley, "Millions in thefts plague New Jersey area", in *New York Times*, Feb 9, 1981, lc A; p 1

[863] R Hanson, "Can wiretaps remain cost-effective?", in *Communications of the ACM v 37 no 12 (Dec 94)* pp 13–15

[864] D Hardt, "The OAuth 2.0 Authorization Framework", *IETF RFC 6749* Oct 2012

[865] C Harper, "How the PlusToken Scam Absconded With Over 1 Percent of the Bitcoin Supply", *Botcoin Magazine* Aug 19 2019

[866] V Harrington, P Mayhew, *'Mobile Phone Theft'*, UK Home Office Research Study 235, January 2002

[867] K Harris, *'The State of Human Trafficking in California'*, California Department of Justice, 2012

[868] T Harris, "How Technology is Hijacking Your Mind – from a Magician and Google Design Ethicist", *Medium* May 18 2016

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

[870] D Harz, "Stealing All of Maker's Collateral", *Medium* Feb 20 2020

[871] A Hassey, M Wells, "Clinical Systems Security – Implementing the BMA Policy and Guidelines", in [64] pp 79–94

[872] R Hastings, "Freedom & Responsibility Culture", 2009, published 2011; archived at `https://www.slideshare.net/reed2001/culture-2009`; updated in 2017 as "Netflix Culture", at `https://jobs.netflix.com/culture`

[873] AJ Hawkins, "Waymo's driverless car: ghost-riding in the back seat of a robot taxi", *The Verge*, Dec 9 2019

[874] S Haykin, "Cognitive Radar: A Way of the Future" *IEEE Journal of Signal Processing* Feb 2006

[875] Health and Human Services, 'Standards for Privacy of Individually Identifiable Health Information', HHS 45 CFR parts 160–164, 65 *Federal Register* at 82461–82,510; see also 82,777–82,779

[876] *'HSE Team Inspection of the Control and Supervision of Operations at BNFL's Sellafield Site'*, Health and Safety Executive, 2000

[877] *'Annual Review 2018–9'*, Healthcare Safety Investigation Branch, NHS

[878] LJ Heath, *'An Analysis of the Systemic Security Weaknesses of the US Navy Fleet Broadcasting System 1967–1974, as Exploited by CWO John Walker'*, MSc Thesis, Georgia Tech, at `http://www.fas.org/irp/eprint/heath.pdf`

[879] B Heath, "U.S. secretly tracked billions of calls for decades", *USA Today* Apr 8 2015

[880] T Heim, "Outrage at 500,000 DNA database mistakes", *Daily Telegraph*, Aug 28 2007

[881] N Heintze, "Scalable Document Fingerprinting", in *Second USENIX Workshop on Electronic Commerce* (1996) pp 191–200

[882] P Helland, "Identity by any other name", *Communications of the ACM* April 2019 pp 80–87

[883] S Helmers, "A Brief History of anon.penet.fi – The Legendary Anonymous Remailer", *CMC Magazine*, Sep 1997; at `http://www.december.com/cmc/mag/1997/sep/helmers.html`

[884] JL Hennessy, DA Patterson, *'Computer Architecture: A Quantitative Approach'*, Morgan Kaufmann 2017

[885] A Henney, R Anderson, "Smart Metering – Ed Milliband's Poisoned Chalice", *Lightbluetouchpaper* Feb 8 2012

[886] E Henning, "The Stamp of Incompetence", *c't magazine*, Sep 3 2007; at `http://www.heise-security.co.uk/articles/95341`

[887] ER Henry, *'Classification and Uses of Finger Prints'* George Rutledge & Sons, London, 1900

[888] I Herbert, "No evidence against man in child porn inquiry who 'killed himself' ", in *The Independent* Oct 1 2005

[889] C Herley, "The Plight of the Targeted Attacker in a World of Scale", *WEIS* 2010

[890] A Hern, "Microsoft president's criticism of app stores puts pressure on Apple", *The Guardian* June 21 2020

[891] Herodotus, *'Histories'*; Book 1 123.4, Book 5 35.3 and Book 7 239.3

[892] T Herr, J Lee, W Loomis, S Scott, "Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain", *Atlantic Council* Jul 2020

[893] J Van den Herrewegen, FD Garcia, "Beneath the Bonnet: a Breakdown of Diagnostic Security", *ESORICS 2018*

[894] A Herzberg, M Jakobsson, S Jarecki, H Krawczyk, M Yung, "Proactive Public Key and Signature Systems", *4th ACM CCS* (1997) pp 100–110

[895] *'IA-64 Instruction Set Architecture Guide'*, Hewlett-Packard 2000

[896] TS Heydt-Benjamin, DV Bailey, K Fu, A Juels, T O'Hare, "Vulnerabilities in First-Generation RFID-enabled Credit Cards", in *Eleventh International Conference on Financial Cryptography and Data Security*, 2007

[897] HM Heys, "A Tutorial on Linear and Differential Cryptanalysis", in *Cryptologia* v XXVI no 3 (Jul 2002) pp 189–221

[898] HJ Highland "Electromagnetic Radiation Revisited", in *Computers & Security* v5 (1986) 85–93 and 181–184

[899] K Hill, "The Secretive Company That Might End Privacy as We Know It", *New York Times* Jan 18 2020

[900] K Hill, A Krolik, "How Photos of Your Kids Are Powering Surveillance Technology", *New York Times* Oct 11 2019

[901] K Hill, H Murphy, "Your DNA Profile is Private? A Florida Judge Just Said Otherwise", *New York Times* Nov 5 2019

[902] K Hill, S Mattu, "The House That Spied on Me", *Gizmodo* Feb 7 2018

[903] R Hill, "European Commission orders mass recall of creepy, leaky child-tracking smartwatch", *The Register* Feb 4 2019

[904] TF Himdi, RS Sandhu, "Lattice-Based Models for Controlled Sharing of Confidential Information in the Saudi Hajj System", in *13th Annual Computer Security Applications Conference* pp 164–174

[905] E von Hippel, "Open Source Software Projects as User Innovation Networks", Open Source Software Economics 2002

[906] W von Hippel, R Trivers, "The evolution and psychology of self-deception", T*Behavioral and Brain Sciences* v 34 (2011) pp 1–16

[907] J Hirshleifer, "Privacy: its Origin, Function and Future", in *Journal of Legal Studies* v 9 (Dec 1980) pp 649–664

[908] J Hirshleifer, "From weakest-link to best-shot: the voluntary provision of public goods", in *Public Choice* v 41, (1983) pp 371–386

[909] J Hirshleifer, *'Economic behaviour in Adversity'*, University of Chicago Press, 1987

[910] T Hobbes, *'Leviathan, or The Matter, Forme and Power of a Common Wealth Ecclesiasticall and Civil, commonly called Leviathan'*, 1651

[911] H Hodson, "DeepMind and Google: the battle to control artificial intelligence", *The Economist 1848* April/May 2019

[912] J Hoffman, "Implementing RBAC on a Type Enforced System", in *13th Annual Computer Security Applications Conference* (1997) pp 158–163

[913] G Hoglund, G McGraw, *'Exploiting Software – How to Break Code'*, Addison Wesley 2004

[914] G Hoglund, G McGraw, *'Exploiting Online Games – Cheating Massively Distributed Systems'*, Addison-Wesley 2007

[915] R Holiday, *'Trust me, I'm lying – Confessions of a media manipulator'*, Profile Books 2018

[916] P Hollinger, “Single language for barcode Babel”, in *Financial Times* Jul 25 2000

[917] C Holloway, “Controlling the Use of Cryptographic Keys”, in *Computers and Security* v 14 no 7 (95) pp 587–598

[918] G ’t Hooft, “The cellular automaton interpretation of quantum mechanics”, *arXiv 1405.1548*, 2014

[919] N Homeier, R Horne, M Maran, D Wade, “Solar storm risk to the north American electric grid” *Lloyd’s of London* 2013

[920] BD Hong, SW Bae, YD Kim, “GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier”, *NDSS 2018*

[921] N Hopkins, “Ofgem exploited national security law to silence us, whistleblowers claim”, *The Guardian* Sep 17 2018

[922] AL Hopkins, TB Smith, JH Lala, “FTMP – A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft”, *Proceedings of the IEEE* v 66 no 10 (Oct 1978) pp 1221–1240

[923] DI Hopper, “Authorities Sue Adult Web Sites”, in *Washington Post* Aug 23 2000

[924] 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

[925] JD Horton, R Harland, E Ashby, RH Cooper, WF Hyslop, DG Nickerson, WM Stewart, OK Ward, “The Cascade Vulnerability Problem”, in *Journal of Computer Security* v 2 no 4 (93) pp 279–290

[926] M Horton, “Historical drivers’ hours offences: 1 year on”, *Moving On* Mar 20 2019

[927] House of Commons Health Committee, *‘The Electronic Patient Record’*, 6th Report of Session 2006–7, at `http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422.pdf`

[928] 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`

[929] M Howard, D LeBlanc, *‘Writing Secure Code’*, (second edition), Microsoft Press 2002

[930] J Hsu, M Gaboardi, A Haeberlen, S Khanna, A Narayan, BC Pierce, A Roth, “Differential Privacy: An Economic Method for Choosing Epsilon”, *CSF* (2014)

[931] Q Hu, JY Yang, Q Zhang, K Liu, XJ Shen, “An automatic seal imprint verification approach”, in *Pattern Recognition* v 28 no 8 (Aug 95) pp 251–266

[932] A Huang, *‘Hacking the Xbox – An Introduction to Reverse Engineering’*, No Starch Press 2003

[933] Huawei Cyber Security Evauation Centre Oversight Board, *Annual Report* (2019)

[934] G Huber, “CMW Introduction”, in *ACM SIGSAC* v 12 no 4 (Oct 94) pp 6–10

[935] M Hughes, “Smart fridges are cool, but after a few short years you could be stuck with a big frosty brick in the kitchen”, *The Register* Jun 8 2020

[936] N Humphrey, “The social function of intellect”, in *Growing Points in Ethology* (1976) pp 303–317

[937] D Hurst 2020, “Cyber-attack Australia: sophisticated attacks from ‘state-based actor’, PM says” *The Guardian* Jun 19 2020

[938] A Hutchings, “Flying in Cyberspace: Policing Global Travel Fraud”, *Policing: A Journal of Policy and Practice* Sep 10 2018

[939] A Hutchings, “Leaving on a jet plane: the trade in fraudulently obtained airline tickets” *Crime, law, and social change* v 70 no 4, pp 461–487

[940] A Hutchings, R Clayton, R Anderson, “Taking down websites to prevent crime”, *eCrime 2016*

[941] A Hutchings, S Pastrana, R Clayton, “Displacing Big Data”, in *The Human Factor of Cybercrime*, Rutger Leukfeldt and Thomas J Holt (eds) Routledge, 2020

[942] N Htoo-Mosher, R Nasser, N Zunic, J Straw, “E4 ITSEC Evaluation of PRISM on ES/9000 Processors”, in *19th National Information Systems Security Conference* (1996), proceedings published by NIST, pp 1–11

[943] M Hypponen, "Malware goes mobile", in *Scientific American* Nov 2006 pp 70–77

[944] "Role of Communications in Operation Desert Storm", in *IEEE Communications Magazine* (Special Issue) v 30 no 1 (Jan 92)

[945] "New England shopping mall ATM scam copied in UK", in *Information Security Monitor* v 9 no 7 (June 94) pp 1–2

[946] "Pink Death Strikes at US West Cellular", in *Information Security Monitor* v 9 no 2 (Jan 94) pp 1–2

[947] Independent Security Evaluators Inc., "Content Protection for Optical Media", May 2005

[948] Information Systems Audit and Control Association, *'Control Objectives for Information and related Technology'*, at `http://www.isaca.org/cobit.htm`

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

[950] "Feds Praise Open Data Health Cloud Launch", *InformationWeek* Nov 12 2013

[951] International Atomic Energy Authority (IAEA), *'The Physical Protection of Nuclear Material and Nuclear Facilities'*, INFCIRC/225/Rev.4 (1999)

[952] *'International Standard on Auditing 315 (Revised 2019)'*, International Auditing and Assurance Standard Board, Dec 2019

[953] IBM, *'IBM 4758 PCI Cryptographic Coprocessor – CCA Basic Services Reference and Guide*, Release 1.31 for the IBM 4758-001

[954] *IEEE Carnahan Conference*, `http://www.carnahanconference.com/`

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

[956] CC Ife, Y Shen, SJ Murdoch, G Stringhini, "Waves of Malice: A Longitudinal Measurement of the Malicious File Delivery Ecosystem on the Web", *AsiaCCS 2019*

[957] I Ilves, "Why are Google and Apple dictating how European democracies fight coronavirus?" *The Guardian* June 16 2020

[958] "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

[959] Information Commissioner's Office, *'Investigation into the use of data analytics in political campaigns'*, July 11 2018

[960] Information Commissioner's Office, *'Mobile phone data extraction by police forces in England and Wales'*, June 2020

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

[962] Intel Corporation and others, *'Advanced Access Content System (AACS) – Technical Overview (informative)'*, July 21 2004

[963] International Electrotechnical Commission, *'Digital Audio Interface'*, IEC 60958, Geneva, February 1989

[964] International Organization for Standardization, *'Road Vehicles – Cybersecurity Engineering'*, ISO/SAE DIS 21434, 2020

[965] M Isaac, K Conger, "Google, Facebook and Others Broaden Group to Secure U.S. Election", *New York Times*, Aug 12 2020

[966] KK Ispoglu, B AlBassam, T Jaeger, M Payer, "Block Oriented Programming: Automating Data-Oriented Attacks", *CCS 2018*

[967] T Iwata, K Kurosawa, "OMAC: One-Key CBC MAC", in *Fast Software Encryption* (2003) Springer LNCS v 2887 pp 129–153

[968] R Iyengar, "Apple will pay up to $500 million to settle lawsuit over slowing down older iPhones", *CNN* Mar 2 2020

[969] C Jackson, DR Simon, DS Tan, A Barth, "An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks", *USEC 2007*

[970] I Jackson, *personal communication*

[971] L Jackson, "BT forced to pay out refunds after free calls fraud", in *The Sunday Telegraph* Feb 9 1997

[972] B Jacobs, "Maximator: European signals intelligence cooperation, from a Dutch perspective", *Journal of Intelligence and National Security* Apr 7 2020

[973] TN Jagatic, NA Johnson, M Jakobsson, F Menczer, "Social Phishing", in *Communications of the ACM* v 50 no 10 (Oct 2007) pp 94–100

[974] G Jagpal, *'Steganography in Digital Images'*, undergraduate thesis, Cambridge University, 1995

[975] AK Jain, L Hong, S Pankanti, R Bolle, "An Identity-Authentication System Using Fingerprints", in *Proceedings of the IEEE* v 85 no 9 (Sep 97) pp 1365–1388

[976] S Jajodia, W List, G McGregor, L Strous (editors), *'Integrity and Internal Control in Information Systems – Volume 1: Increasing the confidence in information systems'*, Chapman & Hall (1997)

[977] M Jakobsson, "Modeling and Preventing Phishing Attacks", *Financial Cryptography 2005*

[978] M Jakobsson, S Myers, *'Phishing and Countermeasures'*, Wiley 2007

[979] A Jamieson, "Securing digital payments – Transformation of the payments industry", *Underwriters' Laboratories* (2019)

[980] *'Horizontal Integration: Broader Access Models for Realizing Information Dominance'*, JASON Program Office report JSR-04-132, 2004

[981] M Jay, "ACPO's intruder policy — underwritten?", in *Security Surveyor* v 26 no 3 (Sep 95) pp 10–15

[982] 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

[983] F Jejdling, *'Ericsson Mobile Report'*, Nov 2019

[984] R Jenkins, "Hole-in-wall thief used MP3 player", in *The Times* Nov 15 2006

[985] S Jha, "Network Security Knowledge Area", *Cyber Security Body of Knowledge* v 1.0 Oct 2019

[986] KX Jin, "Keeping People Safe and Informed About the Coronavirus", *Facebook*, Mar 26 2020, at `https://about.fb.com/news/2020/03/coronavirus/`

[987] D Joel, Z Berman, I Tavor, N Wexler, O Gaber, Y Stein, N Shefi, J Pool, S Urchs, DS Margulies, F Liem, J Hänggi, L Jäncke, Y Assaf, "Sex beyond the genitalia: The human brain mosaic" *PNAS* Dec 2015 v 112 no 50 pp 15468–15473; first published November 30, 2015

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

[989] LK John, A Acquisti, G Loewenstein, "Strangers on a plane: Context-dependent willingness to divulge sensitive information", *Journal of consumer research* v 37 no 5 (2011) pp 858–873

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

[991] RG Johnston, ARE Garcia, "Vulnerability Assessment of Security Seals", in *Journal of Security Administration* v 20 no 1 (June 97) pp 15–27; backed up at `http://www.cl.cam.ac.uk/~rja14/preprints/Johnston/`

[992] DW Jones, B Simons, "Broken Ballots – Will Your Vote Count in the Electronic Age?" *Stanford* (2012)

[993] RV Jones, *'Most Secret War'*, Wordsworth Editions (1978, 1998)

[994] RV Jones, *'Reflections on Intelligence'*, Octopus 1989

[995] J Jonsson, B Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447

[996] A Jøsang, K Johannesen, "Authentication in Analogue Telephone Access Networks", in *Pragocrypt 96*, CTU Publishing, pp 324–336

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

[998] A Juels, RL Rivest, "Honeywords: Making Password-Cracking Detectable", *IEEE SIGSAC* 2013

[999] MY Jung, "Biometric Market and Industry Overview", IBG, Dec 8 2005

[1000] M Kaczorowski, B Baker, "BeyondProd: How Google moved from perimeter-based to cloud-native security", *Google Cloud Blog* Dec 17 2019

[1001] P Kafka, "Facebook's political ad problem, explained by an expert" *Vox*, Dec 10 2019

[1002] B Kahle, "Libraries have been bringing older books to digital learners: Four publishers sue to stop it", *Internet Archive Blogs*, July 22 2020

[1003] D Kahn, *'The Codebreakers'*, Macmillan 1967

[1004] D Kahn, *'Seizing the Enigma'*, Houghton Mifflin 1991

[1005] D Kahn, "Soviet Comint in the Cold War", in *Cryptologia* v XXII no 1 (Jan 98) pp 1–24

[1006] D Kahneman, "Maps of Bounded Rationality: a Perspective on Intuitive Judgment and Choice", *Nobel Prize Lecture*, 2002

[1007] D Kahneman, *'Thinking, Fast and Slow'*, Penguin 2012

[1008] L Kahney, "The FBI Wanted a Backdoor to the iPhone. Tim Cook Said No", *Wired* Apr 16 2019

[1009] AM Kakhki, S Jero, D Choffnes, C Nita-Rotaru, A Mislove, "Taking a Long Look at QUIC", *IMC 2017*

[1010] B Kaliski, "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315

[1011] JB Kam, GI Davida, "A Structured Design of Substitution-Permutation Encryption Network", in *Foundations of Secure Computation*, Academic Press (1978)

[1012] M Kam, G Fielding, R Conn, "Writer Identification by Professional Document Examiners", in *Journal of Forensic Sciences* v 42 (1997) pp 778–786

[1013] 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

[1014] MH Kang, IS Moskowitz, "A Pump for Rapid, Reliable, Secure Communications", in *1st ACM CCS*, 1993, pp 118–129

[1015] 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

[1016] MH Kang, IS Moskowitz, DC Lee, "A Network Pump", in *IEEE Transactions on Software Engineering* v 22 no 5 (May 96) pp 329–338

[1017] MH Kang, IS Moskowitz, B Montrose, J Parsonese, "A Case Study of Two NRL Pump Prototypes", in *12th ACSAC*, 1996, pp 32–43

[1018] MH Kang, IS Moskowitz, S Chincheck, "The Pump: A Decade of Covert Fun", at *21st ACSAC* (2005)

[1019] CS Kaplan, "Privacy Plan Likely to Kick Off Debate", in *New York Times*, July 28 2000

[1020] ED Kaplan, C Hegarty, *'Understanding GPS – Principles and Applications'*, Artech House 2006

[1021] PA Karger, VA Austell, DC Toll, "A New Mandatory Security Policy Combining Secrecy and Integrity", *IBM Research Report* RC 21717 (97406) Mar 15 2000

[1022] PA Karger, RR Schell, "Thirty Years Later': Lessons from the Multics Security Evaluation", at *ACSAC 2002* pp 119–126

[1023] F Kasiski, *'Die Geheimschriften und die Dechiffrier-Kunst'*, Mittler & Sohn, Berlin (1863)

[1024] *'KASUMI Specification'*, ETSI/SAGE v 1 (23/12/1999), at `http://www.etsi.org/dvbandca/`

[1025] J Katz, Y Lindell, *'Introduction to Modern Cryptography'*, CRC Press 2015

[1026] S Katzenbeisser, FAP Petitcolas, *'Information hiding – Techniques for steganography and digital watermarking'*, Artech House 2000

[1027] A Katwala, “The race to create a perfect lie detector – and the dangers of succeeding” *The Guardian* Sep 5 2019

[1028] C Kaufman, R Perlman, M Speciner, *‘Network Security – Private Communication in a Public World’*, Prentice Hall 1995

[1029] EM Kearns, AE Betus, AF Lemieux, “Why Do Some Terrorist Attacks Receive More Media Attention Than Others?” Justice Quarterly, 2018

[1030] DT Keitkemper, SF Platek, KA Wolnik, “DNA versus fingerprints, in *Journal of Forensic Sciences* v 40 (1995) p 534

[1031] MB Kelley, “Obama Administration Admits Cyberattacks Against Iran Are Part Of Joint US-Israeli Offensive”, *Business Insider* June 1 2012

[1032] GC Kelling, C Coles, *‘Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities’*, Martin Kessler Books 1996

[1033] H Kelly, “Facebook, Twitter penalize Trump for posts containing coronavirus misinformation”, *Washington Post*, Aug 7 2020

[1034] 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

[1035] 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

[1036] J Kelsey, B Schneier, D Wagner, C Hall, “Side Channel Cryptanalysis of Product Ciphers,” in *ESORICS 98*, Springer LNCS v 1485 pp 97–110

[1037] 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

[1038] 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

[1039] 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

[1040] T Kendall, “Pornography, Rape, and the Internet”, at *The Economics of the Software and Internet Industries* (Softint 2007)

[1041] ST Kent, MI Millett, *‘Who Goes There? Authentication Through the Lens of Privacy’*, National Research Council 2003; at `http://www.nap.edu/catalog.php?record_id=10656`

[1042] JO Kephardt, SR White, “Measuring and Modeling Computer Virus Prevalence”, in *Proceedings of the 1993 IEEE Symposium on Security and Privacy* pp 2–15

[1043] JO Kephardt, SR White, DM Chess, “Epidemiology of computer viruses”, in *IEEE Spectrum* v 30 no 5 (May 93) pp 27–29

[1044] A Kerckhoffs, “La Cryptographie Militaire”, in *Journal des Sciences Militaires*, 9 Jan 1883, pp 5–38; `http://www.cl.cam.ac.uk/users/fapp2/kerckhoffs/`

[1045] D Kesdogan, H Federrath, A Jerichow, “Location Management Strategies Increasing Privacy in Mobile Communication”, in *12th International Information Security Conference* (1996) pp 39–48

[1046] LM Khan, “Amazon’s antitrust paradox”, *Yale Law Journal* v 126 pp 710–805 (2017)

[1047] J Kieselbach, JP Ziegler, “Mit der Axt”, *Der Spiegel* Nov 25 2019

[1048] JD Kilgallin, “Securing RSA Keys & Certificates for IoT Devices”, `https://info.keyfactor.com/factoring-rsa-keys-in-the-iot-era`, Dec 18 2020

[1049] 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

[1050] YG Kim, R Daly, Jeremie Kim, C Fallin, JH Lee, DH Lee, C Wilkerson, K Lai O Mutlu, "Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors", *ISCA 2014*

[1051] T Kinder, "Regulator outlines plans to break up Big Four accounting firms", *Financial Times* Feb 27 2020

[1052] T Kinder, "Big Four told to outline plans for audit split by October", *Financial Times* Jul 6 2020

[1053] T Kinder, D McCrum, "EY fights fires on three audit cases that threaten its global reputation", *Financial Times* Jun 8 2020

[1054] J King, "Bolero — a practical application of trusted third party services", in *Computer Fraud and Security Bulletin* (July 95) pp 12–15

[1055] S Kirchgaessner, "Jeff Bezos hack: Amazon boss's phone 'hacked by Saudi crown prince' ", *The Guardian* Jan 22 2020

[1056] S Kirchgaessner, "Revealed: Saudis suspected of phone spying campaign in US", *The Guardian* Mar 29 2020

[1057] N Kitroeff, "Boeing Underestimated Cockpit Chaos on 737 Max, N.T.S.B. Says", *New York Times*, Sep 26 2019

[1058] DV Klein, "Foiling the Cracker; A Survey of, and Improvements to Unix Password Security", *Proceedings of the USENIX Security Workshop* (1990)

[1059] P Klemperer, *'Auctions: Theory and Practice – The Toulouse Lectures in Economics'*, Princeton 2004; at `http://www.nuffield.ox.ac.uk/users/klemperer/VirtualBook/VBCrevisedv2.asp`

[1060] RL Klevans, RD Rodman, *'Voice Recognition'*, Artech House 1997

[1061] HM Kluepfel, "Securing a Global Village and its Resources: Baseline Security for Interconnected Signaling System # 7 Telecommunications Networks", in *First ACM CCS* (1993) pp 195–212; later version in *IEEE Communications Magazine* v 32 no 9 (Sep 94) pp 82–89

[1062] N Koblitz, *'A Course in Number Theory and Cryptography'*, Springer Graduate Texts in Mathematics no 114 (1987)

[1063] N Koblitz, A Menezes, "Another Look at 'Provable Security'", in *Journal of Cryptology* v 20 no 1 (2007) pp 3–37

[1064] ER Koch, J Sperber, *'Die Datenmafia'*, Rohwolt Verlag (1995)

[1065] M Kochanski, "A Survey of Data Insecurity Devices", in *Cryptologia* v IX no 1 (1987) pp 1–15

[1066] 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

[1067] P Kocher, "Differential Power Analysis", in *Advances in Cryptology – Crypto 99* Springer LNCS v 1666 pp 388–397

[1068] P Kocher, "Design and Validation Strategies for Obtaining Assurance in Countermeasures to Power Analysis and Related Attacks", at *FIPS Physical Security Workshop*, Hawaii 2005; at `http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper09.pdf`

[1069] P Kocher, J Jaffe, B Jun, P Rohatgi, "Introduction to differential power analysis", *Journal of Cryptographic Engineering* (2011) v 1 pp 5–27

[1070] P Kocher, D Genkin, D Gruss, W Haas, M Hamburg, M Lipp, S Mangard, T Prescher, M Schwarz, Y Yarom, "Spectre Attacks: Exploiting Speculative Execution", *arXiv:1801.01203* Jan 3 2018

[1071] P Kocher, J Horn, A Fogh, D Genkin, D Gruss, W Haas, M Hamburg, M Lipp, S Mangard, T Prescher, M Schwarz, Yuval Yarom, "Spectre Attacks: Exploiting Speculative Execution", IEEE Symposium on Security and Privacy 2019

[1072] J Koebler, "Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware", *Vice*, Mar 21 2017

[1073] J Koebler, "Hacker Bypasses GE's Ridiculous Refrigerator DRM", *Vice* Jul 12 2020

[1074] BI Koerner, "Inside the Cyberattack That Shocked the US Government", *Wired* Oct 23 2016

[1075] J Koetsier, "Apple Just Crippled IDFA, Sending An $80 Billion Industry Into Upheaval", *Forbes* Jun 24 2020

[1076] A Kofman, "Digital Jail: How Electronic Monitoring Drives Defendants Into Debt", *New York Times Magazine*, July 3, 2019

[1077] T Kohno, A Stubblefield, AD Rubin, DS Wallach, "Analysis of an Electronic Voting System", Johns Hopkins TR 2003-19; also published in *IEEE Symposium on Security and Privacy* (2004)

[1078] S Kokolakis, "Privacy attitudes and privacy behaviour", *Computers and Security* v 64 (2017)

[1079] 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

[1080] O Kömmerling, MG Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors", in *Usenix Workshop on Smartcard Technology*, (1999) pp 9–20

[1081] O Kömmerling, F Kömmerling, "Anti tamper encapsulation for an integrated circuit", US Patent 7,005,733, Dec 26 2000

[1082] A Kondi, R Davis, "Software Encryption in the DoD", in *20th National Information Systems Security Conference* NIST (1997) pp 543–554

[1083] MR Koot, "After Ennetcom, Dutch police makes arrests re: PGP Safe, another Dutch company, for allegedly providing crypto phones to (primarily?) the underworld", *Mattijs R. Koot's Notebook*, May 14 2017

[1084] C Kopp, "Electromagnetic Bomb – Weapon of Electronic Mass Destruction", at `https://web.archive.org/web/20120218213215/http://www.abovetopsecret.com/forum/thread59555/pg1`

[1085] DP Kormann, AD Rubin, "Risks of the Passport Single Signon Protocol", in *Computer Networks* (July 2000); at `http://avirubin.com/vita.html`

[1086] K Korosec, "VW fires jailed Audi CEO Rupert Stadler" *Techcrunch* Oct 2 2018

[1087] K Koscher, A Czeskis, F Roesner, S Patel, T Kohno, S Checkoway, D McCoy, B Kantor, D Anderson, H Shacham, S Savage, "Experimental security analysis of a modern automobile" *2010 IEEE Symposium on Security and Privacy* pp 447–462

[1088] M Kosinski, D Stillwell, T Graepel, "Private traits and attributes are predictable from digital records of human behavior", PNAS April 9, 2013 v 110 no 15 pp 5802–5805

[1089] M Kotadia, "Citibank e-mail looks phishy: Consultants", *Zdnet* Nov 9 2006

[1090] KPHO, "Sodomized Ex-McDonald's Employee Wins $6.1M", KPHO, Oct 6 2007

[1091] H Krawczyk, M Bellare, R Canetti, *'HMAC: Keyed-Hashing for Message Authentication'*, RFC 2104 (Feb 1997)

[1092] B Krebs, "Just How Bad Is the Storm Worm?" in *The Washington Post* Oct 1 2007

[1093] B Krebs, "Salesforce.com Acknowledges Data Loss", in *The Washington Post* Nov 6 2007

[1094] B Krebs, "Busting SIM Swappers and SIM Swap Myths" *Krebs on Security* Nov 7 2018

[1095] B Krebs, "Experts: Breach at IT Outsourcing Giant Wipro" *Krebs on Security* Apr 15 2019

[1096] B Krebs, "Romanian Skimmer Gang in Mexico Outed by KrebsOnSecurity Stole $1.2 Billion" *Krebs on Security* Jun 3 2020

[1097] S Krempl, "Lauschangriff am Geldautomaten", in *Der Spiegel* Jan 8 1999; at `http://web.archive.org/web/20001031024042/http://www.spiegel.de/netzwelt/technologie/0,1518,13731,00.html`

[1098] S Krishna, "The man who put us through password hell regrets everything", *Engadget* Aug 8 2017

[1099] HM Kriz, "Phreaking recognised by Directorate General of France Telecom", in *Chaos Digest* 1.03 (Jan 93)

[1100] A Krizhevsky, I Sutskever, GE Hinton, “ImageNet classification with deep convolutional neural networks”, *NIPS 2012* pp 1097–1105

[1101] I Krsul, EH Spafford, “Authorship analysis: identifying the author of a program”, in *Computers and Security* v 16 no 3 (1996) pp 233–257

[1102] H Kuchler, “Can we ever trust Google with our health data?” *Financial Times* Jan 20 2020

[1103] D Kügler, “ ‘Man in the Middle’ Attacks on Bluetooth”, in *Financial Cryptography 2004*, Springer LNCS v 2742 pp 149–161

[1104] 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

[1105] MG Kuhn, “Optical Time-Domain Eavesdropping Risks of CRT Displays”, in *IEEE Symposium on Security and Privacy* (2002)

[1106] MG Kuhn, “Electromagnetic Eavesdropping Risks of Flat-Panel Displays”, in *PET 2004*, at `http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf`

[1107] MG Kuhn, RJ Anderson, “Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations”, in *Information Hiding* (1998), Springer LNCS v 1525 pp 126–143

[1108] R Kuhn, P Edfors, V Howard, C Caputo, TS Philips, “Improving Public Switched Network Security in an Open Environment”, in *Computer*, August 1993, pp 32–35

[1109] M Kumar, “New SIM Card Flaw Lets Hackers Hijack Any Phone Just By Sending SMS”, *Hacker News* Sep 12 2019

[1110] S Kumar, C Paar, J Pelzl, G Pfeiffer, M Schimmler, “Breaking Ciphers with COPACOBANA – A Cost-Optimized Parallel Code Breaker”, in *CHES 2006*

[1111] D Kundaliya, “Android devices are being increasingly targeted by undeletable adware, researchers warn”, *Computing* July 7 2020

[1112] L Kuo, “Chinese surveillance company tracking 2.5m Xinjiang residents”, in The Guardian Feb 18 2019

[1113] J Kuo, “Storm Drain”, in *Anti-Malware Engineering Team blog*, Sep 20 2007, at `http://blogs.technet.com/antimalware/default.aspx`

[1114] GD Kutz, G Aloise, JW Cooney, *‘NUCLEAR SECURITY – Actions Taken by NRC to Strengthen Its Licensing Process for Sealed Radioactive Sources Are Not Effective’*, GAO Report GAO-07-1038T, July 12, 2007

[1115] K Kwiatkowski, “The New Pentagon Papers – A High-Ranking Military Officer Reveals how Defense Department Extremists Suppressed Information and Twisted the Truth to Drive the Country to War”, *Salon* Mar 10 2004

[1116] A Kwong, D Genkin, D Gruss, Y Yarom, “RAMBleed: Reading Bits in Memory Without Accessing Them”, *IEEE Symposium on Security & Privacy* (2020)

[1117] *‘LophtCrack 2.52 for Win95/NT’*, at `http://www.l0pht.com/l0phtcrack/`

[1118] J Lacy, SR Quackenbush, A Reibman, JH Snyder, “Intellectual Property Protection Systems and Digital Watermarking”, in *Information Hiding* (1998), Springer LNCS v 1525 pp 158–168

[1119] RJ Lackey, DW Upmal, “Speakeasy: The Military Software Radio”, in *IEEE Communications Magazine* v 33 no 5 (May 95) pp 56–61

[1120] F Lambert, “Tesla driver on Autopilot admits to watching a movie when crashing into police car” *Elektrek*, Aug 26 2020

[1121] F Lambert, “The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately he’s a good guy”, *Elektrek*, Aug 27 2020

[1122] G Lambourne, *‘The Fingerprint Story’*, Harrap 1984

[1123] L Lamont, “And the real Lotto winner is … that man at the cash register”, *Sydney Morning Herald*, May 3 2007

[1124] 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

[1125] L Lamport, Email message sent to a DEC SRC bulletin board at 12:23:29 PDT on 28 May 1987, link No. 75

[1126] L Lamport, R Shostak, M Pease, "The Byzantine Generals Problem", in *ACM Transactions on Programming Languages and Systems* v 4 no 3 (1982) pp 382–401

[1127] B Lampson, "A Note on the Confinement Problem", in *Communications of the ACM* v 16 no 10 (Oct 1973) pp 613–615

[1128] S Landau, A Lubin, "Examining the Anomalies, Explaining the Value: Should the USA FREEDOM Act's Metadata Program be Extended?" *Harvard National Security Journal* v 11 pp 308–358 (2020)

[1129] R Landley, "Son of DIVX: DVD Copy Control", *Motley Fool*, `http://www.fool.com/portfolios/rulemaker/2000/rulemaker000127.htm`

[1130] P Landrock, "Roles and Responsibilities in BOLERO", in *TEDIS EDI trusted third parties workshop* (1995)

[1131] CE Landwehr, AR Bull, JP McDermott, WS Choi, *'A Taxonomy of Computer Program Security Flaws, with Examples'*, US Navy Report NRL/FR/5542–93-9591 Nov 19 1993

[1132] T Lavin, "The Fetid, Right-Wing Origins of 'Learn to Code' " *The New Republic* Feb 1 2019

[1133] J Leake, "Workers used forged passes at Sellafield", in *Sunday Times* Apr 2 2000

[1134] S LeBlanc, KE Register, *'Constant Battles: Why We Fight'*, St Martin's (2003)

[1135] D Lee, "Blackberry modified to 'help drug cartels' ", *BBC News*, Mar 16 2018

[1136] DY Lee, DH Jung, IT Fang, CC Tsai, RA Popa, "An Off-Chip Attack on Hardware Memory Enclaves Using the Memory Bus", *IEEE Symposium on Security and Privacy* (2000)

[1137] HC Lee, RE Guesslen (eds), *'Advances in Fingerprint Technology'*, Elsevier 1991

[1138] K Lee, B Kaiser, J Meyer, A Nayaranan, "An Empirical Study of Wireless Carrier Authentication for SIM Swaps", *CITP, Princeton*, Jan 10 2020

[1139] W Lee, "Malware and Attack Technologies Knowledge Area", *Cyber Security Body of Knowledge*, v 1.0 October 2019

[1140] D Leigh, "Crackdown on firms stealing personal data", in *The Guardian* Nov 15 2006

[1141] D Leloup, M Untersinger, "Comment les services de renseignement font la chasse aux employés des télécoms", *Le Monde* Dec 8 2016

[1142] AK Lenstra, JP Hughes, M Augier, JW Bos, T Kleinjung, C Wachter, "Ron was wrong, Whit is right", *IACR ePrint 2012/064*

[1143] AK Lenstra, HW Lenstra, *'The development of the number field sieve'*, Springer Lecture Notes in Mathematics v 1554 (1993)

[1144] D Leppard, P Nuki, "BA staff sell fake duty-free goods", in *Sunday Times* Sep 12 1999

[1145] J Lerner, J Tirole, "A Model of Forum Shopping", *American Economic Review* v 96 no 4 pp 1091–1113 (2006)

[1146] L Lessig, *'Code and Other Laws of Cyberspace'*, Basic Books 2000; *'Code: Version 2.0'*, Basic Books 2006; at `https://www.lessig.org/`

[1147] L Lessig, *'Free Culture: The Nature and Future of Creativity'*, Penguin (2005); at `https://www.lessig.org/`

[1148] G Leurant, T Peyrin, "SHA-1 is a Shambles: First Chosen-prefix Collision and Application to the PGP Web of Trust", *IACR Preprint 2020-014*, Jan 7 2020

[1149] É Leverett, *'Quantitatively Assessing and Visualising Control System Attack Surfaces'*, MPhil Thesis, University of Cambridge, 2011

[1150] É Leverett, R Clayton, R Anderson "Standardisation and Certification of Safety, Security and Privacy in the Internet of Things", European Commission 2017

[1151] NG Leveson, *'Safeware – System Safety and Computers'*, Addison-Wesley (1995), and in particular the appendix, "Medical Devices – The Therac-25"

[1152] NG Leveson, "An Improved Design Process for Complex, Control-Based Systems Using STPA and a Conceptual Architecture", *MIT*, Jan 11 2020

[1153] S Levitt, SJ Dubner, *'Freakonomics: A Rogue Economist Explores the Hidden Side of Everything'*, William Morrow 2005

[1154] HM Levy, *'Capability-Based Computer Systems'*, Digital Press 1984

[1155] I Levy, C Robinson, "Principles for a More Informed Exceptional Access Debate", *Lawfare blog* Nov 29 2018

[1156] K Levy, B Schneier, "Privacy threats in intimate relationships", *Journal of Cybersecurity* v 6 no 1 (2020)

[1157] A Lewcock, "Bodily Power", in *Computer Business Review* v 6 no 2 (Feb 98) pp 24–27

[1158] O Lewis, "Re: News: London nailbomber used the Net", post to `ukcrypto` mailing list, Jun 5 2000, archived at `http://www.chiark.greenend.org.uk/mailman/listinfo/ukcrypto`

[1159] Lexmark International, Inc., vs Static Control Components, Inc., US Court of Appeals (6th Circuit), Oct 26 2004, at `www.eff.org/legal/cases/Lexmark_v_Static_Control/20041026_Ruling.pdf`

[1160] J Leyden, "Thai police crack credit card wiretap scam", in *The Register* Aug 4 2006

[1161] J Leyden, "Hacked to the TK Maxx", in *The Register* Jan 19 2007

[1162] J Leyden, "Italy tops global wiretap league", in *The Register*, Mar 7 2007

[1163] J Leyden, "Feds told they need warrants for webmail", in *The Register* June 19 2007

[1164] MY Li, Y Meng, JY Liu, HJ Zhu, XH Liang, Y Liu, N Ruan, "When csi meets public wifi: Inferring your mobile phone password via wifi signals", *CCS 2016* pp 1068–1079

[1165] S Liao "Spyware app abused iOS enterprise certificate to track targets", *The Verge*, Apr 8 2019

[1166] LS Liebst, R Philpot, P Poder, MR Lindegaard, "The Helpful Bystander: Current Evidence from CCTV-Captured Public Conflicts", *Discover Society* June 5 2019

[1167] H Lin, "Doctrinal Confusion and Cultural Dysfunction in the Pentagon Over Information and Cyber Operations", *Lawfare Blog* Mar 27 2020

[1168] R Linde, "Operating Systems Penetration," *National Computer Conference*, AFIPS (1975) pp 361–368

[1169] David Lindenmayer, Ben Scheele "Do Not Publish", *Science Magazine* v 356 no 6340 (May 26 2017) pp 800–801

[1170] JPMG Linnartz, "The 'Ticket' Concept for Copy Control Based on Embedded Signalling", *ESORICS 98*, Springer LNCS 1485 pp 257–274

[1171] JPMG Linnartz, M van Dijk, "Analysis of the Sensitivity Attack Against Electronic Watermarks in Images", in [143] pp 258–272

[1172] SB Lipner, "The Birth and Death of the Orange Book", *Annals of the History of Computing* (2015)

[1173] M Lipp, M Schwarz, D Gruss, T Prescher, W Haas, S Mangard, P Kocher, D Genkin, Y Yarom, M Hamburg, "Meltdown", *arXiv:1801.01207* Jan 3 2018

[1174] A Liptak, "Hackers reportedly used a tool developed by the NSA to attack Baltimore's computer systems", *The Verge* May 25 2019

[1175] D Litchfield, C Anley, J Heasman, B Grindlay, *'The Database Hacker's Handbook: Defending Database Servers'*, Wiley 2005

[1176] B Littlewood, "Predicting software reliability", in *Philosophical Transactions of the Royal Society of London* A327 (1989), pp 513–527

[1177] FF Liu, Y Yarom, Q Ge, G Heiser, RB Lee, "Last-Level Cache Side-Channel Attacks are Practical", *IEEE Symposium on Security and Privacy* 2015

[1178] XY Liu, Z Zhou, WR Diao, Z Li, KH Zhang, “When good becomes evil: Keystroke inference with smartwatch”, *ACM CCS 2015* pp 1273–1285

[1179] WF Lloyd, *‘Two Lectures on the Checks to Population’*, Oxford University Press (1833)

[1180] C Loch, A DeMeyer, MT Pich, *‘Managing the Unknown’*, Wiley 2006

[1181] L Loeb, *‘Secure Electronic Transactions – Introduction and technical Reference’*, Artech House 1998

[1182] N Lomas, “Targeted ads offer little extra value for online publishers, study suggests”, *Techcrunch* May 31 2019

[1183] N Lomas, “Ireland’s data watchdog slammed for letting adtech carry on ‘biggest breach of all time’ ”, *Techcrunch* Sep 21 2020

[1184] London School of Economics & Political Science, *‘The Identity Project – An assessment of the UK Identity Cards Bill & its implications’*, 2005, at `http://eprints.lse.ac.uk/id/eprint/29117`

[1185] J Long, *Google Hacking Database*, at `http://johnny.ihackstuff.com/ghdb.php`

[1186] D Longley, S Rigby, “An Automatic Search for Security Flaws in Key Management”, *Computers & Security* v 11 (March 1992) pp 75–89

[1187] HC Longuet-Higgins, K Prazdny, “The interpretation of a moving retinal image”, *Proc Roy Soc B* v 208 (1980) pp 385–397

[1188] 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* (1998) pp 303–314

[1189] PA Loscocco, SD Smalley, “Integrating Flexible Support for Security Policies into the Linux Operating System”, in *Proceedings of the FREENIX Track: 2001 USENIX Annual Technical Conference (FREENIX ’01)* (June 2001). See also NSA SELinux site: `http://www.nsa.gov/selinux`

[1190] JR Lott, *‘More Guns, Less Crime: Understanding Crime and Gun-Control Laws’*, University of Chicago Press 2000

[1191] J Loughry, DA Umphress, “Information leakage from optical emanations”, in *ACM Transactions on Information and System Security* v 5 no 3 (Aug 2002) pp 262–289

[1192] B Lovejoy, “Apple being sued for refusing to help iTunes gift card scam victims”, *9to5Mac* Jul 20 2020

[1193] WW Lowrance, *‘Privacy and Health Research’*, Report to the US Secretary of Health and Human Services (May 1997)

[1194] J Lukàš, J Fridrich, M Goljan, “Digital ‘bullet scratches’ for images”, in *ICIP 05*

[1195] I Lunden, “Apple fined record $1.2B in France over anti-competitive sales practices”, *TechCrunch* Mar 16 2020

[1196] JM Luo, Y Cao, R Barzilay, “Neural Decipherment via Minimum-Cost Flow: from Ugaritic to Linear B”, *arXiv* 1906.06718 (June 16 2019)

[1197] HT Luong, HD Phan, DV Chu, VQ Nguyen, KT Le, Luc, LT Hoang, “Understanding Cybercrimes in Vietnam: From Leading-Point Provisions to Legislative System and Law Enforcement”, *International Journal of Cyber Criminology* (2019) pp 290–308

[1198] J Lynch, “HART: Homeland Security’s Massive New Database Will Include Face Recognition, DNA, and Peoples’ ‘Non-Obvious Relationships’ ”, *EFF* June 7 2018

[1199] B Lysyk, *‘Annual report of the Auditor General of Ontario’*, 2014

[1200] M Lyu, *‘Software Reliability Engineering’*, IEEE Computer Society Press 1995

[1201] E MacAskill, J Borger, N Hopkins, N Davies, J Ball, “GCHQ taps fibre-optic cables for secret access to world’s communications”, June 21 2013

[1202] R Maclean, “Mali’s President Resigns After Being Arrested in Military Coup”, *New York Times*, Aug 18 2020

[1203] D Mackenzie, *'Mechanising Proof – Computing, Risk and Trust'*, MIT Press 2001

[1204] D Mackett, "A Pilot on Airline Security", in *Hot Air*, July 16 2007, at `http://hotair.com/archives/2007/07/16/a-pilot-on-airline-security/`

[1205] B Macq, *'Special Issue – Identification and protection of Multimedia Information', Proceedings of the IEEE* v 87 no 7 (July 1999)

[1206] M Madden, L Rainie, "Americans' Attitudes About Privacy, Security and Surveillance", *Pew Research Center* May 20 2015

[1207] W Madsen, "Crypto AG: The NSA's Trojan Whore?" in *Covert Action Quarterly* (Winter 1998), at `http://www.mediafilter.org/caq/cryptogate/`

[1208] W Madsen, "Government-Sponsored Computer Warfare and Sabotage", in *Computers and Security* v 11 (1991) pp 233–236

[1209] M Magee, "HP inkjet cartridges have built-in expiry dates – Carly's cunning consumable plan", *The Inquirer*, 29 April 2003, at `http://www.theinquirer.net/?article=9220`

[1210] K Maguire, "Muckraker who feeds off bins of the famous", in *The Guardian* Jul 27 2000

[1211] S Maguire, *'Debugging the Development Process'*, Microsoft Press 1994

[1212] F Main, "Your phone records are for sale", *Chicago Sun-Times*, Jan 5 2006

[1213] D Maio, D Maltoni, "Direct Gray-Scale Minutiae Detection in Fingerprints", in *IEEE Transactions on Pattern Analysis and Machine Intelligence* v 19 no 1 (Jan 97) pp 27–40

[1214] S Makkaveev, "Pwn2Own Qualcomm compute DSP for fun and profit", *DefCon 2020*; also on CheckPoint Blog as "Over 400 vulnerabilities on Qualcomm's Snapdragon chip threaten mobile phones' usability worldwide", Aug 7 2020

[1215] D Maltoni, D Maio, AK Jain, S Prabhakar, *'Handbook of Fingerprint Recognition'*, Springer-Verlag New York, 2003

[1216] S Mangard, E Oswald, T Popp, *'Power Analysis Attacks – Revealing the Secrets of Smartcards'*, Springer 2007

[1217] G Manaugh, "The Rise and Fall of an All-Star Crew of Jewel Thieves", *The Atlantic* Dec 17 2019

[1218] F Manjoo, "The computer virus turns 25", *Salon*, Jul 12 2007

[1219] T Mansfield, G Kelly, D Chandler, J Kane, *'Biometric Product Testing Final Report*, Issue 1.0, 19 March 2001, National Physical Laboratory

[1220] W Marczak, J Dalek, S McKune, A Senft, J Scott-Railton, R Deibert, "BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?" *Munk School, Toronto* Mar 9 2018

[1221] W Marczak, J Scott-Railton, "The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", University of Toronto Aug 24 2016

[1222] D Margolis, M Risher, B Ramakrishnan, A Brotman, J Jones, "SMTP MTA Strict Transport Security (MTA-STS)" *RFC 8461* (Sep 2018)

[1223] A Marino, "Vergecast: Is Facebook ready for 2020?" *The Verge* Aug 27 2019

[1224] J Markoff, *'What the Dormouse Said: How the 60s Counterculture Shaped the Personal Computer'*, Viking Adult (2005)

[1225] J Markoff, "Vast Spy System Loots Computers in 103 Countries", *New York Times* Mar 28 2009

[1226] L Marks, *'Between Silk and Cyanide – a Codemaker's War 1941–1945'*, Harper Collins 1998

[1227] P Marks, "Picking Locks with Audio Technology", *Communications of the ACM*, Aug 13 2020

[1228] M Marlinspike, "Technology preview: Private contact discovery for Signal", *Signal Blog*, Sep 26 2017

[1229] M Marlinspike, T Perrin, "The X3DH Key Agreement Protocol", `https://signal.org/docs/specifications/` Nov 4 2016

[1230] V Marotta, V Abhishek, A Acquisti, “Online Tracking and Publishers’ Revenues: An Empirical Analysis”, *WEIS 2019*

[1231] P Marquardt, A Verma, H Carter, P Traynor, “(sp)iphone: Decoding vibrations from nearby keyboards using mobile phone accelerometers”, *CCS 2011* pp 551–562

[1232] M Marquis-Boire, G Greenwald, M Lee, “XKEYSCORE – NSA’s Google for the World’s Private Communications”, *The Intercept* July 1 2015

[1233] M Marquis-Boire, B Marczak, C Guarnieri, J Scott-Railton, “You Only Click Twice – FinFisher’s Global Proliferation” *Munk School, Toronto*, Mar 13 2013

[1234] S Marsh, “US joins UK in blaming Russia for NotPetya cyber-attack”, *The Guardian* Feb 15 2018

[1235] L Martin, “Using Semiconductor Failure Analysis Tools for Security Analysis”, FIPS Physical Security Workshop, Hawaii 2005

[1236] AG Martínez, “How Trump Conquered Facebook—Without Russian Ads”, *Wired* Feb 23 2018

[1237] JL Mashaw, DL Harfst, *‘The struggle for auto safety’*, Harvard 1990

[1238] S Mason, *‘Electronic Evidence – Disclosure, Discovery and Admissibility’*, LexisNexis Butterworths 2007

[1239] S Masondo, “Postbank Forced to Replace 12-Million Bank Cards after Employees Steal ‘Master Key’ ”, *Sunday Times* Jun 14 2020

[1240] M Mastanduno, “Economics and Security in Statecraft and Scholarship”, *International Organization* v 52 no 4 (Autumn 1998)

[1241] S Matala, T Nyman, N Asokan, “Historical insight into the development of Mobile TEEs”, *Aalto University Secure Systems Group blog*, June 20 2019

[1242] JM Matey, O Naroditsky, K Hanna, R Kolczynski, DJ LoIacono, S Mangru, M Tinker, TM Zappia, WY Zhao, “Iris on the Move: Acquisition of Images for Iris recognition in Less Constrained Environments”, in *Proc IEEE* v 94 no 11 (Nov 2006) pp 1936–1947

[1243] SA Mathieson. “Gone phishing in Halifax – UK bank sends out marketing email which its own staff identify as a fake”, in *Infosecurity News*, Oct 7 2005

[1244] A Mathur, G Acar, M Friedman, E Lucherini, J Mayer, M Chetty, A Narayanan, “Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites”, *arxiv:1907.07032* July 16 2019

[1245] M Matsubara, “The Japanese Automobile Industry Is Taking Next Steps for Cybersecurity Collaboration”, *Lawfare* Jul 7 2020

[1246] M Matsui, “Linear Cryptanalysis Method for DES Cipher”, in *Eurocrypt 93*, Springer LNCS v 765 pp 386–397

[1247] M Matsui, “New Block Encryption Algorithm MISTY”, in *Fourth International Workshop on Fast Software Encryption* (1997), Springer LNCS v 1267 pp 54–68

[1248] T Matsumoto, H Matsumoto, K Yamada, S Hoshino, “Impact of Artificial ‘Gummy’ Fingers on Fingerprint Systems” *Proceedings of SPIE* v 4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002

[1249] R Matthews, “The power of one”, in *New Scientist* Jul 10 1999 pp 26–30

[1250] T Matthews, K O’Leary, A Turner, M Sleeper, J Palzkill Woelfer, M Shelton, C Manthorne, EF Churchill, S Consolvo, “Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse” *CHI 2017*

[1251] 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

[1252] V Mavroudis, P Svenda, “JavaCard: The execution environment you didn’t know you were using”, *Software Sustainability Institute* July 13 2018

[1253] J Maynard Smith, G Price, “The Logic of Animal Conflict”, in *Nature* v 146 (1973) pp 15–18

[1254] R Mayrhofer, J Vander Stoep, C Brubaker, N Kralevich, “The Android Platform Security Model”, *arXiv:1904.05572*, Apr 11 2019

[1255] K McCarthy, "Here's that hippie, pro-privacy, pro-freedom Apple y'all so love: Hong Kong protest safety app banned from iOS store", *The Register*, Oct 2 2019

[1256] K McCarthy, "The Internet of Things is a security nightmare reveals latest real-world analysis: unencrypted traffic, network crossover, vulnerable OSes", *The Register*, Mar 11 2020

[1257] J McCormac. *'European Scrambling Systems – The Black Book'*, version 5, Waterford University Press 1996

[1258] D McCrum, "Wirecard: the timeline", *Financial Times* Jun 25 2020

[1259] D McCullagh, "U.S. to Track Crypto Trails", in *Wired*, May 4 2000; statistics at `http://www.uscourts.gov/wiretap99/contents.html`

[1260] D McCullagh, R Zarate, "Scanning Tech a Blurry Picture", in *Wired*, Feb 16 2002

[1261] K McCurley, Remarks at IACR General Meeting. *Crypto 98*, Santa Barbara, Ca., Aug 1998

[1262] 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

[1263] P McDaniel, K Butler, W Enck, H Hursti, S McLaughlin, P Traynor, MA Blaze, A Aviv, P Černý, S Clark, E Cronin, G Shah, M Sherr, A Vigna, R Kemmerer, D Balzarotti, G Banks, M Cova, V Felmetsger, W Robertson, F Valeur, JL Hall, L Quilter, *'EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing'*, Final Report, Dec 7, 2007

[1264] AD McDonald, MG Kuhn, "StegFS: A Steganographic File System for Linux", in [1522] pp 463–477

[1265] D MacEoin, *'The hijacking of British Islam – How extremist literature is subverting mosques in the UK'*, Policy Exchange (2007)

[1266] M McFarland, "Feds blame distracted test driver in Uber self-driving car death", *CNN* Nov 20 2019

[1267] E McGaughey, "The extent of Russian-backed fraud means the referendum is invalid", *LSE* Nov 14 2018

[1268] G McGraw, *'Software Security – Building Security In'*, Addison-Wesley 2006

[1269] G McGraw, H Figueroa, V Shepardson, R Bonett, *'An architectural risk analysis of machine learning systems: Towards more secure machine learning'*, BIML, 2020

[1270] D McGrew, J Viega, "The Galois/Counter Mode of Operation (GCM)", Submission to NIST Modes of Operation Process, January 2004; updated May 2005

[1271] J McGroddy, HS Lin, *'A Review of the FBI's Trilogy Information Technology Modernization Program'*, National Academies Press, 2004

[1272] J McHugh, "An EMACS Based Downgrader for the SAT" in *Computer and Network Security*, IEEE Computer Society Press (1986) pp 228–237

[1273] N McInnes, G Wills, E Zaluska, "Analysis of threats on a VoIP based PBX honeypot", *Infonomics Society* (2019) pp 113–118

[1274] I McKie, "Total Vindication for Shirley McKie!" Jun 23 2000, at `http://onin.com/fp/mckievindication.html`

[1275] I McKie, M Russell, *'Shirley McKie – The Price of Innocence'*, Birlinn 2007

[1276] J McLaughlin, Z Dorfman, " 'Shattered': Inside the secret battle to save America's undercover spies in the digital age", *Yahoo News* Dec 30 2019

[1277] J McLean, "The Specification and Modeling of Computer Security", in *Computer* v 23 no 1 (Jan 1990) pp 9–16

[1278] J McLean, "Security Models," in *Encyclopedia of Software Engineering*, Wiley 1994

[1279] 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

[1280] D McLeod, "FNB backs down on password decision after backlash", *Tech Central* Aug 20 2019

[1281] J McMillan, "Mobile Phones Help Secure Online Banking", in *PC World*, Sep 11 2007

[1282] R McMillan, "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster", *Wired* Mar 3 2014

[1283] "Health data, AI, and Google DeepMind", MedConfidential, 2018, at `https://medconfidential.org/whats-the-story/health-data-ai-and-google-deepmind/`

[1284] J Meek, "Robo Cop", in *The Guardian*, June 13 2002

[1285] N Megaw, "UK consumers dragged into Wirecard's collapse", *Financial Times* Jun 29 2020

[1286] C Meijer, R Verdult, "Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards", *ACM CCS* (2015)

[1287] C Meijer, B van Gastel, "Self-encrypting deception: weaknesses in the encryption of solid-state drives", *IEEE Security & Privacy* (2019)

[1288] J Meikle, "G4S and Serco hand over offender tagging contracts over fraud claims", *The Guardian*, Dec 12 2013

[1289] M Mehrnezhad, M Aamir Ali, F Hao, A van Moorsel, "NFC payment spy: a privacy attack on contactless payments", *International Conference on Research in Security Standardisation* (2016) pp 92–111

[1290] J Mendez, "How Steam Employs DRM & What That Means For Your Game", *Black Shell Media*, Jun 28 2017

[1291] AJ Menezes, PC van Oorschot, SA Vanstone, *'Handbook of Applied cryptography'*, CRC Press (1997); available online at `http://www.cacr.math.uwaterloo.ca/hac/`

[1292] J Menn, "Exclusive: Secret contract tied NSA and security industry pioneer", *Reuters* Dec 20 2013

[1293] J Menn, "Exclusive: High-security locks for government and banks hacked by researcher", *Reuters* Aug 6 2019

[1294] J Menn, K Paul, R Satter, "Exclusive: More than 1,000 people at Twitter had ability to aid hack of accounts", *Reuters* Jul 23 2020

[1295] J Mercer, "Document Fraud Deterrent Strategies: Four Case Studies", in *Optical Security and Counterfeit Deterrence Techniques II* (1998), IS&T and SPIE v 3314, pp 39–51

[1296] H Mercier, D Sperber, "Why Do Humans Reason? Arguments for an Argumentative Theory", *Behavioral and Brain Sciences* v 34 no 2 pp 57–74, 2011, and at SSRN 1698090

[1297] R Mercuri, "Physical Verifiability of Computer Systems", *5th International Computer Virus and Security Conference* (March 1992); see also R Mercuri, *'Electronic Vote Tabulation Checks & Balances'*, PhD Thesis, U Penn, 2000, at `http://www.notablesoftware.com/evote.html`

[1298] R Merkle, "Protocols for public key cryptosystems", *IEEE Symposium on Security and Privacy* 1980

[1299] M Mesa, "Phish Scales: Malicious Actor Combines Personalized Email, Variety of Malware To Target Execs", *ProofPoint* Apr 5 2016

[1300] TS Messergues, EA Dabish, RH Sloan, "Investigations of Power Analysis Attacks on Smartcards", in *Usenix Workshop on Smartcard Technology* (1999) pp 151–161

[1301] E Messmer, "DOD looks to put pizzazz back in PKI", *Network World* Aug 15 2005

[1302] C Metz, "AI Is Transforming Google Search. The Rest of the Web Is Next", *Wired* Feb 4 2016

[1303] CH Meyer, SM Matyas, *'Cryptography: A New Dimension in Computer Data Security'*, Wiley 1982

[1304] C Meyer, J Schwenk, "SoK: Lessons Learned From SSL/TLS Attacks", *WISA 2013* pp 189–209

[1305] R Meyer-Sommer, "Smartly analyzing the simplicity and the power of simple power analysis on Smartcards", in *Workshop on Cryptographic Hardware and Embedded Systems* (2000); Springer LNCS v 1965 pp 78–92

[1306] A Michael, "Cyber Probing: The Politicisation of Virtual Attack", *Defence Academy of the United Kingdom* Oct 2012

[1307] J Micklethwait, A Wooldridge, *'The Witch Doctors – What the management gurus are saying, why it matters and how to make sense of it'*, Random House 1997

[1308] Microsoft Inc, *'Architecture of Windows Media Rights Manager'*, May 2004

[1309] Microsoft Inc, "Sony DRM Rootkit", Nov 12 2005

[1310] Microsoft Inc, "Security Development Lifecycle – Simplified Implementation of the Microsoft SDL" Nov 4 2010

[1311] Microsoft Azure, "What is Azure Key Vault?" Jan 7 2019

[1312] A Midgley, "R.I.P. and NHSNet", `ukcrypto` mailing list, Jul 1 2000

[1313] S Mihm, *'A Nation of Counterfeiters'*, Harvard 2007

[1314] S Milgram, *'Obedience to Authority: An Experimental View'*, HarperCollins, (1974, reprinted 2004)

[1315] J Millen, "A Resource Allocation Model for Denial of Service Protection", in *Journal of Computer Security* v 2 no 2–3 (1993) pp 89–106

[1316] A Miller, "SourMint: malicious code, ad fraud, and data leak in iOS", *Synk*, Aug 26 2020

[1317] B Miller, "Vital Signs of Security", in *IEEE Spectrum* (Feb 94) pp 22–30

[1318] C Miller, C Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle", `https://www.illmatics.com` Aug 10 2015

[1319] GA Miller, "The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information", in *Psychological Review* v 63 (1956) pp 81–97

[1320] ML Miller, IJ Cox, JA Bloom, "Watermarking in the Real World: An Application to DVD", in *Sixth ACM International Multimedia Conference* (1998); v 41 of *GMD Report*, pp 71–76

[1321] JR Minkel, "Confirmed: The U.S. Census Bureau Gave Up Names of Japanese-Americans in WW II", in *Scientific American* Mar 30 2007

[1322] SF Mires, "Production, Distribution, and Use of Postal Security Devices and Information-Based Indicia", *Federal Register* v 65 no 191 Oct 2, 2000 pp 58682–58698

[1323] A Mirian, Z Ma, D Adrian, M Tischer, T Chuenchujit, T Yardley, R Berthier, J Mason, Z Durumeric, JA Halderman, M Bailey, "An Internet-Wide View of ICS Devices", *Conference on Privacy, Security and Trust* 2016

[1324] A Mirian, J DeBlasio, S Savage, GM Voelker, K Thomas, "Hack for Hire: Exploring the Emerging Market for Account Hijacking", *The World Wide Web Conference* 2019 pp 1279–1289

[1325] "BBC fined £400,000 by Ofcom for fake competitions", *Daily Mirror* July 30 2008

[1326] Mitchell and Webb, "Identity Theft", *YouTube* (2007)

[1327] KD Mitnick, *'The Art of Deception: Controlling the Human Element of Security'*, Wiley (2002)

[1328] V Mladenov, C Mainka, K Mayer zu Selhausen, M Grothe, J Schwenk "1 trillion Dollar Refund – How to Spoof PDF Signatures", *CCS 2019*

[1329] D Modic, RJ Anderson, "Reading This May Harm Your Computer: The Psychology of Malware Warnings", *Computers in Human Behavior* v 41 pp 71–79 and SSRN 2374379

[1330] A Moghimi, G Irazoqui, T Eisenbarth, "CacheZoom: How SGX Amplifies The Power of Cache Attacks" *CHES 2017* pp 69–90

[1331] D Moghimi, B Sunar, T Eisenbarth, N Heninger, "TPM-FAIL: TPM meets Timing and Lattice Attacks", *arXiv:1911.05673* Nov 13 2019

[1332] "Card fraud nets Esc6 billion', F Mollet, *Cards International* Sep 22 1995 p 3

[1333] JV Monaco, "SoK: Keylogging Side Channels", *IEEE Symposium on Security and Privacy* (2018)

[1334] "Démantèlement d'un réseau de téléphonie cryptée, utilisé par des organisations criminelles", *Le Monde* Jul 2 2020

[1335] YA de Montjoye, CA Hidalgo, M Verleysen, VD Blondel, "Unique in the Crowd: The privacy bounds of human mobility", *Scientific Reports* v 3 no 1376 (2013)

[1336] YA de Montjoye, J Quoidbach, F Robic, A Pentland, "Predicting Personality Using Novel Mobile Phone-Based Metrics", *2013 International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction* (SBP 2013) pp 48–55

[1337] B Moore, “Lessons from Christchurch: How the media finally acknowledged far-right terrorism”, *Signal* April 3 2019

[1338] SW Moore, RJ Anderson, R Mullins, G Taylor, J Fournier, “Balanced Self-Checking Asynchronous Logic for Smart Card Applications”, in *Microprocessors and Microsystems Journal* v 27 no 9 (Oct 2003) pp 421–430

[1339] T Moore, R Anderson, “How brain type influences online safety”, *Security and Human Behaviour* (2008)

[1340] T Moore, A Friedman, A Procaccia, “Would a ‘Cyber Warrior’ Protect Us? Exploring Trade-offs Between Attack and Defense of Information Systems”, *New Security Paradigms Workshop* (2010) pp 85–94.

[1341] T Moore, N Christin, “Beware the middleman: Empirical analysis of Bitcoin-exchange risk”, *Financial Cryptography* 2013 pp 25–33

[1342] L Moran, “Tweeters Make Chilling Point About Jack Dorsey’s Account Being Compromised”, *Huffington Post*, Aug 31 2019

[1343] B Morgan, “Strip club which gave client £50k bill loses license”, *Evening Standard* Jan 31 2020

[1344] R Morris, “A Weakness in the 4.2BSD Unix TCP/IP Software”, Bell Labs Computer Science Technical Report no. 117, February 25, 1985; at `http://www.cs.berkeley.edu/~daw/security/seq-attack.html`

[1345] R Morris, Invited talk, *Crypto 95*

[1346] R Morris, K Thompson, “Password security: A case history”, in *Communications of the ACM* v 22 no 11 (November 1979) pp 594–597

[1347] M Motoyama, D McCoy, K Levchenko, S Savage, GM Voelker, “An Analysis of Underground Forums”, *IMC* (2011)

[1348] DP Moynihan, *‘Secrecy – The American Experience’*, Yale University Press (1999)

[1349] P Mozur, “Skype Vanishes From App Stores in China, Including Apple’s”, *New York Times*, Nov 21 2017

[1350] P Mozur, “With Hacks and Cameras, Beijing’s Electronic Dragnet Closes on Hong Kong”, *New York Times*, Aug 25 2020

[1351] C Mueller, S Spray, J Grear, “The Unique Signal Concept for Detonation Safety in Nuclear Weapons”, Sand91-1269, UC-706

[1352] J Mueller, *‘Overblown – How Politicians and the Terrorism Industry Inflate National Security Threats, and Why we Believe Them’*, Simon and Schuster 2006

[1353] S Mukherjee, “What the Coronavirus Crisis Reveals About American Medicine”, *New Yorker* 27 April 2020

[1354] 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

[1355] S Mullender (ed), *‘Distributed Systems’*, Addison-Wesley 1993

[1356] E Munro, “Munro review of child protection: final report – a child-centred system”, *Department for Education* May 10 2011

[1357] SJ Murdoch, “Browser storage of passwords: a risk or opportunity?” *Light Blue Touchpaper* Apr 18 2006

[1358] SJ Murdoch, “Hot or Not: Revealing Hidden Services by their Clock Skew”, in *13th ACM Conference on Computer and Communications Security*, 2006

[1359] SJ Murdoch, “The role of software engineering in electronic elections”, *Light Blue Touchpaper* Jul 13 2007

[1360] SJ Murdoch, *‘Covert channel vulnerabilities in anonymity systems’*, PhD Thesis, Cambridge 2007

[1361] SJ Murdoch, “Embassy email accounts breached by unencrypted passwords”, *Light Blue Touchpaper* Sep 10 2007

[1362] SJ Murdoch, “Comparison of Tor Datagram Designs”, *Tor Tech Report 2011-11-001*, Nov 7 2011

[1363] SJ Murdoch, “UK Parliament on protecting consumers from economic crime”, *Bentham’s Gaze* Nov 5 2019

[1364] SJ Murdoch, RJ Anderson, “Verified by Visa and MasterCard SecureCode, or How Not to Design Authentication”, *Financial Cryptography* (2010)

[1365] SJ Murdoch, G Danezis, "Low-Cost Traffic Analysis of Tor", in *IEEE Symposium on Security and Privacy* (2005)

[1366] SJ Murdoch, S Drimer, RJ Anderson, M Bond, "Chip and PIN is Broken", *IEEE Symposium on Security and Privacy* (2010)

[1367] SJ Murdoch, Piotr Zieliński, "Sampled Traffic Analysis by Internet-Exchange-Level Adversaries", at PETS 2007

[1368] K Murdock, D Oswald, FD Garcia, J Van Bulck, D Gruss, F Piessens, "Plundervolt: Software-based Fault Injection Attacks against Intel SGX", at `https://www.plundervolt.com` (2019)

[1369] JC Murphy, D Dubbel, R Benson, "Technology Approaches to Currency Security", in *Optical Security and Counterfeit Deterrence Techniques II* (1998), IS&T and SPIE v 3314 pp 21–28

[1370] K Murray, "Protection of computer programs in Ireland", in *Computer Law and Security Report* v 12 no 3 (May/June 96) pp 57–59

[1371] O Mutlu, JS Kim, "RowHammer: A Retrospective", *arXiv:1904.09724* Apr 22 2019

[1372] R Nader, *'Unsafe at Any Speed: The Designed-In Dangers of The American Automobile'*, Grossman 1965

[1373] A Nadler, A Aminov, A Shabtai, "Detection of Malicious and Low Throughput Data Exfiltration Over the DNS Protocol", *arXiv 1709.08395*

[1374] A Nadkarni, B Andow, W Enck, S Jha, "Practical DIFC Enforcement on Android", *Usenix Security* (2016)

[1375] S Nagaraja, RJ Anderson, "The Topology of Covert Conflict", *Fifth Workshop on the Economics of Information Security* (2006)

[1376] S Nagaraja, RJ Anderson, "The snooping dragon: social-malware surveillance of the Tibetan movement", *University of Cambridge Computer Laboratory Technical Report 746* (2009)

[1377] S Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", `http://bitcoin.org/bitcoin.pdf` (2008)

[1378] E Nakashima, "Verizon Says It Turned Over Data Without Court Orders", in *The Washington Post* Oct 16 2007

[1379] E Nakashima, "A Story of Surveillance – Former Technician 'Turning In' AT&T Over NSA Program", in *The Washington Post* Nov 7 2007

[1380] E Nakashima, "FBI Prepares Vast Database Of Biometrics – $1 Billion Project to Include Images of Irises and Faces", in *The Washington Post* Dec 22 2007

[1381] E Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies" in *The Washington Post* May 27 2013

[1382] Major General RFH Nalder, *'History of the Royal Corps of Signals'*, published by the Royal Signals Institution (1958)

[1383] *Napster*, `http://en.wikipedia.org/wiki/Napster`

[1384] A Narayanan, "How to recognize AI snake oil", *Arthur Miller lecture on science and ethics, Massachusetts Institute of Technology*, Nov 18 2019

[1385] A Narayanan, J Bonneau, E Felten, A Miller, S Goldfeder, *'Bitcoin and Cryptocurrency Technologies'*, Princeton University Press, 2016

[1386] A Narayanan, V Shmatikov, "How To Break Anonymity of the Netflix Prize Dataset", (Nov 2007) at `http://arxiv.org/abs/cs/0610105`

[1387] M Nash, "MS Security VP Mike Nash Replies", on *Slashdot* Jan 26 2006, at `http://interviews.slashdot.org/interviews/06/01/26/131246.shtml`

[1388] M Nash, R Kennett, "Implementing Security policy in a Large Defence Procurement", in *12th ACSAC*, 1996, pp 15–23

[1389] B Nassi, Y Pirutin, A Shamir Y Elovici, B Zadov, "Lamphone – Real-Time Passive Sound Recovery from Light Bulb Vibrations", *BlackHat USA* (2020)

[1390] National Academies of Sciences, Engineering and Medicine, *'Securing the Vote: Protecting American Democracy'*, National Academies Press (2018)

[1391] National Audit Office, *'Ministry of Defence: Combat Identification'*, 2002

[1392] National Audit Office, *'The National Programme for IT in the NHS: an update on the delivery of detailed care records systems'* May 18 2011

[1393] National Audit Office, *'Rolling out smart meters'*, Nov 23 2018

[1394] National Audit Office, *'Investigation into Verify'*, Mar 5 2019

[1395] National Cyber Security Centre, *'Annual Review 2019'*

[1396] National Highway Traffic Safety Administration, *'Special Crash Investigations: On-Site Automated Driver Assistance System Crash Investigation of the 2015 Tesla Model S 70D'*, Report No. DOT HS 812 481, 2018

[1397] National Institute of Standards and Technology, archive of publications on computer security, `http://csrc.nist.gov/publications/history/index.html`

[1398] National Institute of Standards and Technology, *'Common Criteria for Information Technology Security Evaluation'*, Version 2.0 / ISO IS 15408 (May 1998); Version 3.1 (Sep 2006–Sep 2007), at `http://www.commoncriteriaportal.org`

[1399] National Institute of Standards and Technology, *'Data Encryption Standard (DES)'* FIPS 46-3, Nov 1999 incorporating upgrade to triple DES

[1400] National Institute of Standards and Technology, *'Escrowed Encryption Standard'*, FIPS 185, Feb 1994

[1401] National Institute of Standards and Technology, *'Security Requirements for Cryptographic Modules'* (11/1/1994)

[1402] National Institute of Standards and Technology, *'SKIPJACK and KEA Algorithms'*, Jun 23 1998, `http://csrc.nist.gov/encryption/skipjack-kea.htm`

[1403] National Institute of Standards and Technology, *'Advanced Encryption Standard'*, FIPS 197, Nov 26, 2001

[1404] National Institute of Standards and Technology, *'Digital Signature Standard (DSS)'*, FIPS 186-2, Jan 2000, with change notice Oct 2001

[1405] National Institute of Standards and Technology, *'Digital Signature Standard (DSS)'*, FIPS 186-3, draft, Mar 2006

[1406] National Institute of Standards and Technology, *'Recommendation for Block Cipher Modes of Operation'*, Special Publication 800-38A 2001 Edition

[1407] National Institute of Standards and Technology, *'Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication'*, Special Publication 800–38B, May 2005

[1408] National Institute of Standards and Technology, *'Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality'*, Special Publication 800–38C, May 2004

[1409] National Institute of Standards and Technology, *'Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC'*, NIST Special Publication 800–38D, November 2007

[1410] National Institute of Standards and Technology, *'Recommendation for Key Management – Part 1: General (Revised)*, Special Publication 800-57, May 2006

[1411] National Institute of Standards and Technology, *'Announcing request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family'*, in *Federal Register* v 72 no 212, Nov 2 2007, pp 62212–20

[1412] National Institute of Standards and Technology, "Comments received on NIST's Request for Information regarding 'Government use of standards for security and conformance requirements for cryptographic algorithm and cryptographic module testing and validation programs", *Federal Register Notice 2015-19743* (2018)

[1413] National Research Council, *'Cryptography's Role in Securing the Information Society'*, National Academies Press (1996)

[1414] National Research Council, *'For the Record: Protecting Electronic Health Information'*, National Academies Press (1997)

[1415] National Research Council, *'Strengthening Forensic Science in the United States: A Path Forward'* (2009)

[1416] National Security Agency, *'The NSA Security Manual'*, leaked at `http://www.cl.cam.ac.uk/ftp/users/rja14/nsaman.tex.gz`

[1417] "Interim report", *National Security Commission on Artificial Intelligence*, Nov 2019

[1418] National Statistics, "Protocol on Data Access and Confidentiality", at `http://www.statistics.gov.uk`

[1419] J Naughton, "Forget driverless tech – white-van man will keep on trucking", *The Guardian* Apr 16 2017

[1420] J Naughton, "Facebook's Vassal State", in *Memex 1.1* March 5, 2019

[1421] J Naughton, "The law that helped the internet flourish now undermines democracy", *The Guardian* Dec 21 2019

[1422] P Naur, B Randell, *'Software Engineering – Report on a Conference'*, NATO Scientific Affairs Division, Garmisch 1968

[1423] Y Nawaz, "Blockchain and Cryptography at JPMorgan Chase", *Financial Cryptography 2018*, at `https://www.lightbluetouchpaper.org/2018/02/26/financial-cryptography-2018/`

[1424] R Neame, "Managing Health Data Privacy and Security", in [64] pp 225–232

[1425] RM Needham, "Denial of Service: An Example", in *Communications of the ACM* v 37 no 11 (Nov 94) pp 42–46

[1426] RM Needham, "Naming", in [1355], pp 318–127

[1427] RM Needham, "The Hardware Environment", in *Proceedings of the 1999 IEEE Symposium on Security and Privacy* p 236

[1428] RM Needham, MD Schroeder, "Using Encryption for Authentication in Large Networks of Computers", in *Communications of the ACM* v 21 no 12 (Dec 78) pp 993–999

[1429] U Neisser, *'Cognition and reality: Principles and implications of cognitive psychology'*, Freeman, 1976

[1430] M Nesbitt, "Deep Chain Reorganization Detected on Ethereum Classic (ETC)", *Coinbase blog* Jan 7 2019

[1431] P Neumann, *'Computer Related Risks'*, Addison-Wesley 1995

[1432] P Neumann, *'Principled Assuredly Trustworthy Composable Architectures'*, CHATS Project final report (2004), at `http://www.csl.sri.com/users/neumann/`

[1433] J Neumann, "A Taxonomy of Moats", *Reaction Wheel* Sep 19, 2019

[1434] New South Wales Supreme Court, RTA v. Mitchell, New South Wales Supreme Court, Mar 24 2006, reported in "Australia: NSW Supreme Court Backs Away from Camera Decision", `http://www.thenewspaper.com/news/10/1037.asp`

[1435] MEJ Newman, "The structure and function of complex networks", in *SIAM Review* v 45 no 2 (2003) pp 167–256

[1436] MEJ Newman, "Modularity and community structure in networks", in *Proc. Natl. Acad. Sci. USA* v 103 pp 8577–8582 (2006); at `http://arxiv.org/abs/physics/0602124`

[1437] O Newman, *'Defensible Space: People and Design in the Violent City'*, MacMillan 1972

[1438] R Newman, S Gavette, L Yonge, RJ Anderson, "Protecting Domestic Power-line Communications", in *SOUPS* 2006 pp 122–132

[1439] R Newman, S Gavette, L Yonge, RJ Anderson, "HomePlug AV Security Mechanisms", *2007 IEEE International Symposium on Power Line Communications and Its Applications*

[1440] C Newton, "The Trauma Floor", *The Verge*, Feb 25, 2019

[1441] C Newton, "Mark Zuckerberg says Facebook will shift to emphasize encrypted ephemeral messages", *The Verge*, Mar 6 2019

[1442] J Newton, “Countering the counterfeiters”, in *Cards International* (21/12/94) p 12

[1443] J Newton, *‘Organised Plastic Counterfeiting’*, HMSO 1996

[1444] “The Vanishing Salad Oil: A $100 Million Mystery”, *New York Times* Jan 6 1964

[1445] Nex, “The New Old Frontier of Interception”, *Newsletter blog* Jul 28 2020

[1446] Andrew Ng, “How the Equifax hack happened, and what still needs to be done”, *Cnet* Sep 7 2018

[1447] S Nichols “Silence of the WANs: FBI DDoS-for-hire greaseball takedowns slash web flood attacks ‘by 11%’” *The Register* 19 Mar 2019

[1448] S Nichols “Apple drops a bomb on long-life HTTPS certificates: Safari to snub new security certs valid for more than 13 months”, *The Register* Feb 20 2019

[1449] SJ Nightingale, H Farid, “Assessing the reliability of a clothing-based forensic identification”, *PNAS* Jan 15 2020

[1450] N Nisan, T Roughgarden, E Tardos, VV Vazirani, *‘Algorithmic Mechanism Design’*, CUP 2007

[1451] A Nixon, “Fraudsters Taught Us that Identity is Broken”, *Financial Cryptography 2020* Feb 2 2020, at `https://www.lightbluetouchpaper.org/2020/02/10/fc-2020/`

[1452] K Nohl, D Evans, H Plötz, “Reverse-Engineering a Cryptographic RFID Tag”, *Usenix Security 2008*; earlier version at Chaos Computer Congress 2007

[1453] DA Norman, “Cautious Cars and Cantankerous Kitchens: How Machines Take Control”, chapter 1 of *The Design of Future Things* (2009)

[1454] A Noroozian, J Koenders, E Van Veldhuizen, CH Ganan, S Alrwais, D McCoy, M Van Eeten, “Platforms in everything: analyzing ground-truth data on the anatomy and economics of bullet-proof hosting”, *USENIX Security 2019* pp 1341–1356

[1455] R v Ipswich Crown Court ex parte NTL Ltd, [2002] EWHC 1585 (Admin), at `http://www.cyber-rights.org/documents/ntl_case.htm`

[1456] *‘White Paper – 5G Evolution and 6G’*, NTT Docomo, January 2020

[1457] Nuclear Regulatory Commission, US Government, `www.nrc.gov`

[1458] H Nugent, “Adulterers who call 118 118 for an affair”, in *The Times*, May 27 2006

[1459] F Oberholzer, K Strumpf, “The Effect of File Sharing on Record Sales – An Empirical Analysis”, June 2004; journal version F Oberholzer-Gee, K Strumpf, “The Effect of File Sharing on Record Sales: An Empirical Analysis, *Journal of Political Economy* v 115 (2007) pp 1–42

[1460] *‘Victimation et Perceptions de la Sûreté’*, Observatoire National de la Délinquance et de Responses Pénales (2017)

[1461] AM Odlyzko, “Tragic loss or good riddance? The impending demise of traditional scholarly journals”, *Notices Amer. Math. Soc.*, Jan 1995

[1462] AM Odlyzko, *‘The history of communications and its implications for the Internet’*, at `http://www.dtc.umn.edu/~odlyzko/doc/networks.html`

[1463] AM Odlyzko, “Smart and stupid networks: Why the Internet is like Microsoft”, *ACM netWorker*, Dec 1998, pp 38–46

[1464] AM Odlyzko, “Privacy, economics, and price discrimination on the Internet”, in *ICEC ’03: Proceedings of the 5th international conference on electronic commerce*, pp 355–366

[1465] AM Odlyzko, “Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation”, *TPRC 2004*

[1466] Office of the Director of National Intelligence, *‘Statistical Transparency Report Regarding Use of National Security Authorities – Calendar Year 2017’*

[1467] P Ohm, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization”, *UCLA Law Review* v 57 (2010) pp 1701–77

[1468] S O'Kane, "Daimler fined nearly $1 billion for selling cars that cheated emissions tests", *The Verge*, Sep 24 2019

[1469] N Okuntsev, *'Windows NT Security'*, R&D Books 1999

[1470] *"Nicht nachmachen: Dieser Vignetten-Trick kostet Sie 300 Euro"*, *Online Focus*, June 12 2015

[1471] Open Net Initiative, *'Internet Filtering in China in 2004-2005: A Country Study'*, April 14, 2005, at `https://opennet.net/`

[1472] Open Net Initiative, *'China (including Hong Kong)'*, Country report 2006, at `https://opennet.net/`

[1473] Open Net Initiative, *'Pulling the Plug'*, Oct 2007, at `https://opennet.net/research/bulletins/013`

[1474] Open Rights Group, *'May 2007 Election Report – Findings of the Open Rights Group Election Observation Mission in Scotland and England'*, at `http://www.openrightsgroup.org/e-voting-main`

[1475] A Orben, T Dienlin, AK Przybylski, "Social media's enduring effect on adolescent life satisfaction", *PNAS* April 16 2019

[1476] A Orlowski, "Schrems busts Privacy Shield wide open", *The Register*, Oct 3 2017

[1477] A Orlowski, "UK spy agency warns Brit telcos to flee from ZTE gear", *The Register* April 16 2018

[1478] Organization for Economic Cooperation & Development, *'Guidelines for the Protections of Privacy and Transborder Flow of Personal Data'*, OECD Doc No C(80)58 (1981)

[1479] Organization for Economic Cooperation & Development, *'CO4.4: Teenage suicides (15-19 years old)'* OECD Family Database (2017)

[1480] M Orozco, Y Asfaw, A Adler, S Shirmohammadi, A El Saddik, "Automatic Identification of Participants in Haptic Systems", in *IEEE Instrumentation and Measurement Technology Conference* (2005) pp 888–892

[1481] B Osborn, J McWilliams, B Beyer, M Saltonstall, "BeyondCorp – Design to Deployment at Google", *;login:* (Spring 2016) v 41 no 1

[1482] C Osborne, "University of California SF pays ransomware hackers $1.14 million to salvage research", *ZDNet*, Jun 30 2020

[1483] C Osborne, "In one click: Amazon Alexa could be exploited for theft of voice history, PII, skill tampering", *ZDNet*, Aug 13 2020

[1484] J Osen, "The Cream of Other Men's Wit: Plagiarism and Misappropriation in Cyberspace", in *Computer Fraud and Security Bulletin* (11/97) pp 13–19

[1485] DA Osvik, A Shamir, E Tromer, "Cache attacks and countermeasures: the case of AES," in *RSA Conference Cryptographers Track* 2006, LNCS 3860, pp 1–20

[1486] D Oswald, C Paar, "Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World", *CHes 2011* pp 207–222

[1487] *Out-law News*, "SWIFT broke data protection law, says Working Party", Nov 27 2006, at `http://www.out-law.com/page-7518`

[1488] *Out-law News*, "SWIFT will stop some US processing in 2009", Oct 15 2007, at `http://www.out-law.com/page-8548`

[1489] A Ozment, S Schechter, "Bootstrapping the Adoption of Internet Security Protocols", at *Workshop on the Economics of Information Security*, 2006

[1490] A Ozment, S Schechter, "Milk or Wine: Does Software Security Improve with Age?" in *15th Usenix Security Symposium* (2006)

[1491] D Page, *'Theoretical Use of Cache Memory as a Cryptanalytic Side-Channel'*, Technical Report CSTR-02-003, University of Bristol, June 2002

[1492] G Pahl, W Beitz, *'Konstruktionslehre'*; translated as *'Engineering Design: A Systematic Approach'*, Springer 1999

[1493] S Pancho, "Paradigm shifts in protocol analysis", in *Proceedings of the 1999 New Security Paradigms Workshop*, ACM (2000), pp 70–79

[1494] A Papadimoulis, "Wish-It-Was Two-Factor", Sep 20 2007, at `http://worsethanfailure.com/Articles/WishItWas-TwoFactor-.aspx`

[1495] N Papernot, "A Marauder's Map of Security and Privacy in Machine Learning", *arXiv 1811.01134* Nov 3 2018

[1496] DJ Parker, "DVD Copy Protection: An Agreement At Last? – Protecting Intellectual Property Rights In The Age Of Technology", in *Tape/Disc Magazine* (Oct 96)

[1497] C Parsons, A Molnar, J Dalek, J Knockel, M Kenyon, B Haselton, C Khoo, R Deibert, *'The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry'*, Munk School, June 12 2019

[1498] N Partridge, *'Data Release review'*, Department of Health, June 2014

[1499] J Pastor,"CRYPTOPOST – A cryptographic application to mail processing", in *Journal of Cryptology* v 3 no 2 (Jan 1991) pp 137–146

[1500] S Pastrana, G Suarez-Tangil, "A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth", *arXiv:1901.00846* Jan 3 2019

[1501] S Pastrana, DR Thomas, A Hutchings, R Clayton, "CrimeBB: Enabling Cybercrime Research on Underground Forums at Scale", World Wide Web Conference (2018) pp 1845–1854

[1502] K Paul, "Twitter employees charged with spying for Saudi Arabia", *The Guardian* Nov 6 2019

[1503] R Paul, "Leaked Media Defender e-mails reveal secret government project", *Ars Technica* Sep 16 2007

[1504] LC Paulson, "Inductive analysis of the Internet protocol TLS", in *Security Protocols 1998* and *ACM Transactions on Computer and System Security* v 2 no 3 (1999) pp 332–351

[1505] V Paxson, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", in *Computer Communication Review* v 31 no 3, July 2001

[1506] M Payer, *'Software Security – Principles, Policies and Protection'* 2019

[1507] S Pearman, J Thomas, P Emani Naeini, H Habib, L Bauer, N Christin, L Faith Cranor, S Egelman, A Forget, "Let's go in for a closer look: Observing passwords in their natural habitat", *CCS 2017*

[1508] J Pearson 2020, "Exclusive: Facebook agreed to censor posts after Vietnam slowed traffic – sources", *Thnomson Reuters* Apr 21 2020

[1509] PeckShield, "bZx Hack Full Disclosure (With Detailed Profit Analysis)", *Medium* Feb 17 2020

[1510] C Percival, "Cache Missing for Fun and Profit", *BSDCan* 2005

[1511] J Pereira, "Breaking the Code: How Credit-Card Data Went Out Wireless Door", in *The Wall Street Journal*, May 4 2007, p A1

[1512] N Perlroth, S Shane, "In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc", in *New York Times* May 25 2019

[1513] A Perrig, *'A Copyright Protection Environment for Digital Images'*, Diploma thesis, École Polytechnique Fédérale de Lausanne (1997)

[1514] T Perrin, M Marlinspike, "The Double Ratchet Algorithm", `https://signal.org/docs/specifications/` Nov 20 2016

[1515] 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

[1516] M Peters, "MTN moves to prevent SIM card swap fraud", *IOL*, Dec 30 2007

[1517] I Peterson, "From Counting to Writing", MathLand Archives, `http://www.maa.org/mathland/mathland_2_24.html`

[1518] FAP Petitcolas, RJ Anderson, MG Kuhn, "Attacks on Copyright Marking Systems", in *Information Hiding* (1998) Springer LNCS v 1525 pp 219–239

[1519] FAP Petitcolas, RJ Anderson, MG Kuhn, "Information Hiding – A Survey", in *Proceedings of the IEEE* v 87 no 7 (July 1999) pp 1062–1078

[1520] H Petroski, *'To Engineer is Human'*, Barnes and Noble Books (1994)

[1521] A Peyton, "Ethereum Classic hit by another 51% hack", *Fintech Direct*, Aug 6 2020

[1522] A Pfitzmann, *Proceedings of the Third International Workshop on Information Hiding* (1999), Springer LNCS v 1768

[1523] B Pfitzmann, "Information Hiding Terminology", in *Information Hiding* (1996) Springer LNCS v 1174 pp 347–350

[1524] T Philippon, *'The Great Reversal – How America Gave up on Free Markets'*, Harvard 2019

[1525] PJ Phillips, AN Yates, Y Hu, CA Hahn, E Noyes, K Jackson, JG Cavazos, G Jeckeln, R Ranjan, S Sankaranarayanan, JC Chen, CD Castillo, R Chellappa, D White, AJ O'Toole, "Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms", *PNAS* June 12 2018 v 115 no 24 pp 6171–6176

[1526] Z Phillips, "Security Theater", in *Government Executive* Aug 1, 2007, at `http://www.govexec.com/features/0807-01/0807-01s3.htm`

[1527] 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

[1528] 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

[1529] RL Pickholtz, DB Newman, YQ Zhang, M Tatebayashi, "Security Analysis of the INTELSAT VI and VII Command Network", in *IEEE Proceedings on Selected Areas in Communications* v 11 no 5 (June 1993) pp 663–672

[1530] L Pinault, *'Consulting Demons'*, Collins 2000

[1531] S Pinto, N Santos, "Demystifying Arm TrustZone: A Comprehensive Survey", *ACM Computing Surveys* v 51 no 6 (Feb 2019)

[1532] JC Plantin, G de Seta, "WeChat as infrastructure: the techno-nationalist shaping of Chinese digital platforms", *Chinese Journal of Communication* v 12 no 3 (2019) pp 257–273

[1533] RA Poisel, *'Modern Communications Jamming Principles and Techniques'*, Artech House 2003

[1534] *Politech* mailing list, was at `http://www.politechbot.com/`

[1535] GJ Popek, RP Goldberg, "Formal Requirements for Virtualizable Third Generation Architectures", in *Communications of the ACM* v 17 no 7 (July 1974) pp 412–421

[1536] E Porter, "The Facebook Fallacy: Privacy Is Up to You", *New York Times* Apr 24 2018

[1537] R Porter, "Google fined €50 million for GDPR violation in France", *The Verge* Jan 21 2019

[1538] B Poser, "The Provenzano Code", in *Language Log*, Apr 21, 2006; at `http://itre.cis.upenn.edu/~myl/languagelog/archives/003049.html`

[1539] Richard Posner, "An Economic Theory of Privacy", in *Regulation* (1978) pp 19–26

[1540] Richard Posner, "Privacy, Secrecy and Reputation", in *Buffalo Law Review* v 28 no 1 (1979)

[1541] F Postma, "Military And Intelligence Personnel Can Be Tracked With The Untappd Beer App", *Bellingcat* May 18, 2020

[1542] K Poulsen, "ATM Reprogramming Caper Hits Pennsylvania", in *Wired*, July 12 2007

[1543] S Poulter, "Phone firm's whistleblower says his life has been made a misery", in *The Daily Mail* Jun 21 2007

[1544] J Powles, "DeepMind's Latest A.I. Health Breakthrough Has Some Problems", *Medium* Aug 8 2019

[1545] J Powles, H Hodson, "Google DeepMind and healthcare in an age of algorithms", *Health and Technology* v 7 no 4 (Dec 2017) pp 351–367

[1546] S Prasad, E Bouma-Sims, AK Mylappan, B Reaves, "Who's Calling? Characterising Robocalls thorugh Audio and Metadata Analysis", *Usenix Security 2020*

[1547] J Preece, H Sharp, Y Rogers, *'Interaction design: beyond human-computer interaction'*, Wiley 2002

[1548] 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

[1549] President's Council of Advisers on Science and Technology, *'Big Data and Privacy: A technological perspective'*, May 1 2014

[1550] Press Association, "Hatton Garden ringleader 'Basil' found guilty over £14m heist", *The Guardian* Mar 15 2019

[1551] L Presser, M Hruskova, H Rowbottom, J Kancir, "Care.data and access to UK health records: patient privacy and public trust", *Journal of Technology Science* Aug 8 2015

[1552] RS Pressman, *'Software Engineering: A Practitioner's Approach'*, McGraw-Hill 2000

[1553] V Prevelakis, D Spinellis, "The Athens Affair", *IEEE Spectrum*, July 2007

[1554] H Pringle, "The Cradle of Cash", in *Discover* v 19 no 10 (Oct 1998)

[1555] C Prins, "Biometric Technology Law", in *The Computer Law and Security Report* v 14 no 3 (May/Jun 98) pp 159–165

[1556] W Pritchard, "Lockdown was a boon for Spotify. Now musicians are fighting back", *Wired*, Jul 19 2020

[1557] Privacy International, *'Who's That Knocking at My Door? Understanding Surveillance in Thailand'*, 2017

[1558] Privacy International, *'A technical look at Phone Extraction'* 2019

[1559] S Proctor, EY Wassermann, J Hatcliff, "SAFE and Secure: Deeply Integrating Security in a New Hazard Analysis", *SAW 2017*

[1560] S Protière, A Boudaoud, Y Couder, "Particle-wave association on a fluid interface", in *Journal of Fluid Mechanics* v 554 no 10 (2006) pp 85–108

[1561] A Pruneda, "Windows Media Technologies: Using Windows Media Rights Manager to Protect and Distribute Digital Media", *MSDN Magazine*, Dec 2001, at `http://msdn.microsoft.com/msdnmag/issues/01/12/DRM/`

[1562] Public Accounts Committee, *'Public Accounts Committee – Nineteenth Report: The dismantled National Programme for IT in the NHS'*, July 2013

[1563] Public Accounts Committee, *'Ministry of Defence nuclear programme'*, Sep 2018

[1564] *Public Lending Right* (PLR), at `http://www.writers.org.uk/guild/Crafts/Books/PLRBody.html`

[1565] Public Record Office, *'Functional Requirements for Electronic Record Management Systems'*, November 1999

[1566] RD Putnam, *'Bowling Alone: the Collapse and Revival of American Community'*, Simon & Schuster, 2000

[1567] T Pyszczynski, S Solomon, J Greenberg, *'In the Wake of 9/11 – the Psychology of Terror'*, American Psychological Association 2003

[1568] Quality Control Systems Corporation, *'NHTSA's Implausible Safety Claim for Tesla's Autosteer Driver Assistance System'*, Feb 8 2019

[1569] B Quinn, J Ball, Rushe, "GCHQ chief accuses US tech giants of becoming terrorists' 'networks of choice' ", *The Guardian* Nov 3 2014

[1570] Z Quinn, *'Crash Override'*, Hachette 2017

[1571] JJ Quisquater, D Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards", in *International Conference on Research in Smart Cards*, Springer LNCS v 2140 pp 200–210

[1572] R v Paul Matthew Stubbs, [2006] EWCA Crim 2312 (12 October 2006), at `http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWCA/Crim/2006/2312.html`

[1573] H Ragab, A Milburn, K Razavi, H Bos, C Giuffrida, "CrossTalk: Speculative Data Leaks Across Cores Are Real", *IEEE symposium on Security & Privacy* (2021)

[1574] M Raghavan, S Barocas, J Kleinberg, K Levy, "Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices", *arXiv:1906.09208* Jun 21 2019

[1575] Rain Forest Puppy, "Issue disclosure policy v1.1", at `http://www.wiretrip.net/rfp/policy.html`

[1576] R Ramesh, "NHS England patient data 'uploaded to Google servers', Tory MP says" *The Guardian* Mar 3 2014

[1577] R Ramesh, "Online tool could be used to identify public figures' medical care, say critics" *The Guardian* Mar 17 2014

[1578] A Randal, "The Ideal Versus the Real: Revisiting the History of Virtual Machines and Containers", arXiv:1904.12226, Apr 27 2019

[1579] M Randolph, W Diehl, "Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman", *Cryptography* v 4 no 15 (2020)

[1580] J Rankin, "EU says China behind 'huge wave' of Covid-19 disinformation", *The Guardian* Jun 10 2020

[1581] W Rankl, W Effing, *'Smartcard Handbook'*, Wiley (1997); translated from *'Handbuch der Chpkarten'*, Carl Hanser Verlag (1995)

[1582] S Ransbotham, "An Empirical Analysis of Exploitation Attempts based on Vulnerabilities in Open Source Software", WEIS 2010

[1583] S Rashid, "Breaking the Ledger Security Model", *https://saleemrashid.com/* Mar 20, 2018

[1584] FY Rashid, "Proposal to make https certificate expire yearly back on the table", *Decipher* Aug 15 2019

[1585] B Ray, "How I hacked SIM cards with a single text – and the networks DON'T CARE", *The Register* Sep 23 2013

[1586] ES Raymond, "The Case of the Quake Cheats", 27/12/1999, at `http://www.catb.org/~esr/writings/quake-cheats.html`

[1587] ES Raymond, *'The Cathedral and the Bazaar'*, at `http://www.catb.org/~esr/writings/cathedral-bazaar/`

[1588] ES Raymond, *'The Magic Cauldron'*, June 1999, at `http://www.catb.org/~esr/writings/magic-cauldron/magic-cauldron.html`

[1589] A Razaghpanah, R Nithyanand, N Vallina-Rodriguez, S Sundaresan, M Allman, C Kreibich, P Gill, "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem", *NDSS 2018*

[1590] K Razavi, B Gras, E Bosman, B Preneel, C Giuffrida, H Bos, "Flip Feng Shui: Hammering a Needle in the Software Stack", *USENIX Security* 2016

[1591] J Reardon, Á Feal, AE Bar On, N Valina-Rodriguez, S Egelman, "50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System", *Usenix Security 2019*

[1592] J Reason, *'Human Error'*, Cambridge University Press 1990

[1593] MG Reed, PF Syverson, DM Goldschlag, "Anonymous Connections and Onion Routing", in *IEEE Journal on Special Areas in Communications* v 16 no 4 (May 98) pp 482–494

[1594] EM Redmiles, "Quality and Inequity in Digital Security Education", PhD Thesis, University of Maryland, 2019

[1595] J Rees, "Facial recognition use by South Wales Police ruled unlawful", *BBC News*, Aug 11 2020

[1596] P Reidy, "MH17: five of the most bizarre conspiracy theories", *The Guardian* Jul 22 2014

[1597] Reporters without Borders, *'Handbook for Bloggers and Cyber-dissidents'*, 2005, at `http://www.rsf.org/rubrique.php3?id_rubrique=542`

[1598] E Rescorla, *'SSL and TLS – Designing and Building Secure Systems'*, Addison-Wesley 2000

[1599] E Rescorla, "Is Finding Security Holes a Good Idea?", *Third Workshop on the Economics of Information Security* (2004)

[1600] *Reuters*, "No Surveillance Tech for Tampa", in *Wired* Aug 21 2003, at `http://www.wired.com/politics/law/news/2003/08/60140`

[1601] M Reynolds, "The strange story of Section 230, the obscure law that created our flawed, broken internet", *Wired* Mar 24 2019

[1602] I Reyes, P Wijesekera, J Reardon, A Elazari Bar On, A Razaghpanah, N Vallina-Rodriguez, S Egelman, " 'Won't Somebody Think of the Children?' Examining COPPA Compliance at Scale", *Proceedings on Privacy Enhancing Technologies* (2018) pp 63–83

[1603] M Richards, R Anderson, S Hinde, J Kaye, A Lucassen, P Matthews, M Parker, M Shotter, G Watts, S Wallace, J Wise, *'The collection, linking and use of data in biomedical research and health care: ethical issues'*, Nuffield Bioethics Council, Feb 2015

[1604] D Richardson, *'Techniques and Equipment of Electronic Warfare'*, Salamander Books 1985

[1605] T Richter, S Escher, D Schönfeld, T Strufe, "Forensic Analysis and Anonymisation of Printed Documents", *IH&MMSec '18* pp 127–138

[1606] LW Ricketts, JE Bridges, J Miletta, *'EMP Radiation and Protection Techniques'*, Wiley 1975

[1607] M Ridley, *'The Red Queen: Sex and the Evolution of Human Nature'*, Viking Books 1993

[1608] G Rippon, *'The Gendered Brain'*, Bodley Head 2019

[1609] J Risen, E Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts", *New York Times* Dec 16, 2005

[1610] 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

[1611] RL Rivest, J Wack, "On the notion of 'software independence' in voting systems", *Philosophical Transactions of The Royal Society A* v 366 no 1881 pp 3759–67 (Nov 2008)

[1612] MB Robinson, "The Theoretical Development of 'CPTED': 25 years of Responses to C. Ray Jeffery", in *Advances in Criminological Theory* v 8; at `http://www.acs.appstate.edu/dept/ps-cj/vitacpted2.html`

[1613] AR Roddy, JD Stosz, "Fingerprint Features – Statistical Analysis and System Performance Estimates", in *Proceedings of the IEEE* v 85 no 9 (Sep 97) pp 1390–1421

[1614] J Rogers, "FAKE FIVER: Shopper's warning after being handed this fake £5 note – but is it counterfeit?", *The Sun* May 13 2018

[1615] WP Rogers, NA Armstrong, DC Acheson, EE Covert, RP Feynman, RB Hotz, DJ Kutyna, SK Ride, RW Rummel, JF Sutter, ABC Walker, AD Wheelon, CB Yeager, AG Keel, *'Report to the President by the Presidential Commission on the Space Shuttle Challenger Accident'* June 6 1986

[1616] R Rohozinski, M Mambetalieva, "Election Monitoring in Kyrgyzstan", 2005, *Open Net Initiative*, at `http://opennet.net/special/kg/`

[1617] E Ronen, C O'Flynn, A Shamir, AO Weingarten, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction", *IACR Eprint 1047* (2016)

[1618] K Rooney, "Majority of bitcoin trading is a hoax, new study finds" *CNBC* Mar 22 2019

[1619] SJ Root, *'Beyond COSO – Internal Control to Enhance Corporate Governance'*, Wiley 1998

[1620] N Rosasco, D Larochelle, "How and Why More Secure Technologies Succeed in Legacy Markets: Lessons from the Success of SSH", in *WEIS 2003*

[1621] S Rose, O Borchert, S Mitchell, S Connelly, "Zero Trust Architecture (2nd Draft)", *SP 800-207(Draft)*, Feb 2020

[1622] M Rosenberg, JE Barnes, "A Bible Burning, a Russian News Agency and a Story Too Good to Check Out", *New York Times*, Aug 11 2020

[1623] B Ross, C Jackson, N Miyake, D Boneh, JC Mitchell, "Stronger Password Authentication Using Browser Extensions", in *Usenix Security 2005*; at `http://crypto.stanford.edu/PwdHash/`

[1624] DE Ross, "Two Signatures", in `comp.risks` v 20.81: `http://catless.ncl.ac.uk/Risks/20.81.html`

[1625] A Roth, "US charges Russian 'Evil Corp' hackers with $100m banking scheme", *The Guardian* Dec 5 2019

[1626] "Card fraud plummets in France", M Rowe, *Banking Technology* (May 94) p 10

[1627] T Rowland, "Ringing up the wrong numbers", in *The Guardian* May 18 2006; at `http://www.guardian.co.uk/media/2006/may/18/newmedia.technology`

[1628] A Roy, N Memon, A Ross "MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems", *IEEE Transactions on Information Forensics and Security* v 12 no 9 (Sep 2017) 2013–25

[1629] The Royal Society, *'Strategy options for the UK's separated plutonium'*, Sep 27 2007

[1630] The Royal Society, *'Science as an open enterprise'* June 21 2012

[1631] WW Royce, "Managing the development of Large Software Systems: Concepts and Techniques", in *Proceedings IEEE WESCON* (1970) pp 1–9

[1632] HH Rubinovitz, "Issues Associated with Porting Applications to the Compartmented Mode Workstation", in *ACM SIGSAC* v 12 no 4 (Oct 94) pp 2–5

[1633] RA Rueppel, *'Analysis and Design of Stream Ciphers'*, Springer-Verlag 1986

[1634] RA Rueppel, "Criticism of ISO CD 11166 Banking: Key Management by Means of Asymmetric Algorithms", in *Proceedings of 3rd Symposium of State and Progress of Research in Cryptography*, Fondazione Ugo Bordoni, Rome 1993, pp 191–198

[1635] J Rushby, B Randell, "A Distributed Secure System", in *IEEE Computer* v 16 no 7 (July 83) pp 55–67

[1636] B Russell, Answer to parliamentary question, *Hansard* 10 Jun 2003 column 762W

[1637] J Rutkowska, "Running Vista Every Day!", *Invisible Things Blog*, Feb 2007

[1638] M Ryan, "The NSA Playset: Bluetooth Smart Attack Tools", at *Bluetooth Smart Security*, `http://lacklustre.net/bluetooth/`, 2015

[1639] DR Safford, DL Schales, DK Hess, "The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment", in *Usenix Security* (1993) pp 91–118

[1640] M Safi, "India's ruling party ordered online abuse of opponents, claims book", *The Guardian* Dec 27 2016

[1641] MJ Salganik, I Lundberg, AT Kindel and others, "Measuring the predictability of life outcomes with a scientific mass collaboration", *Proceedings of the National Academy of Sciences* v 117 no 15 pp 8398–8403, Mar 30 2020

[1642] JH Saltzer, MD Schroeder, "The Protection of Information in Computer Systems", in *Proceedings of the IEEE* v 63 no 9 (Mar 1975) pp 1278–1308

[1643] JH Saltzer, MF Kaashoek, *'Principles of Computer System Design'*, Morgan Kaufman 2009

[1644] RG Saltman, *'Accuracy, Integrity and Security in Computerized Vote-Tallying'*, NBS Special Publication 500–158 (1988)

[1645] J Saltzman, M Daniel, "Man freed in 1997 shooting of officer – Judge gives ruling after fingerprint revelation", in *The Boston Globe* Jan 24 2004

[1646] P Samarati, L Sweeney, "Protecting Privacy when Disclosing Information: k-Anonymity and its Enforcement through Generalization and Suppression", *SRI Tech Report SRI-CSL-98-04* (1998)

[1647] T Sammes, B Jenkinson, *'Forensic Computing – A Practitioner's Guide'*, Springer 2007

[1648] I Sample, "NHS patient records to revolutionise medical research in Britain" *The Guardian* Aug 28 2012

[1649] P Samuelson, "Intellectual Property Rights and the Global Information Economy", in *Communications of the ACM* v 39 no 1 (Jan 96) pp 23–28

[1650] P Samuelson, S Scotchmer, "The Law and Economics of Reverse Engineering", *Yale Law Journal* (2002)

[1651] D Samyde, SP Skorobogatov, RJ Anderson, JJ Quisquater, "On a New Way to Read Data from Memory", in *IEEE Security in Storage Workshop* (2002) pp 65–69

[1652] RS Sandhu, S Jajodia, "Polyinstantiation for Cover Stories", in *Computer Security — ESORICS 92*, LNCS v 648 pp 307–328

[1653] G Sandoval, "Glitches let Net shoppers get free goods", in *CNET News.com*, July 5 2000

[1654] P Sankar, S Mora, JF Merz, NL Jones, "Patient Perspectives of Medical Confidentiality – A Review of the Literature", *J Gen Intern Med* 2003 August vol 18 no 8 pp 659–669

[1655] SANS Institute, "Consensus List of The Top Ten Internet Security Threats", at `http://www.sans.org/`, Version 1.22 June 19, 2000

[1656] DE Sanger, K Benner, "U.S. Accuses North Korea of Plot to Hurt Economy as Spy Is Charged in Sony Hack" *New York Times* Sep 6 2018

[1657] PF Sass, L Gorr, "Communications for the Digitized Battlefield of the 21st Century", in *IEEE Communications* v 33 no 10 (Oct 95) pp 86–95

[1658] E Van der Sar, "BitTorrent 'Copyright Troll' Lawsuits Skyrocket In Sweden", *Torrentfreak* Feb 14 2020

[1659] C Savage, "N.S.A. Phone Program Cost $100 Million, but Produced Only Two Unique Leads", *New York Times* Feb 25 2020

[1660] S Saulny, "118 Charged in A.T.M. Thefts After 9/11", *New York Times*, June 19 2003

[1661] J Scahill, J Begley, "How spies stole the keys to the encryption castle", *The Intercept* Feb 15 2015

[1662] W Schachtman, "How Technology Almost Lost the War: In Iraq, the Critical Networks Are Social – Not Electronic", in *Wired*, Dec 15 2007, at `http://www.wired.com/politics/security/magazine/15-12/ff_futurewar?currentPage=all`

[1663] M Schaefer, "Symbol Security Condition Considered Harmful", in *Proceedings of the 1989 IEEE Symposium on Security and Privacy*, pp 20–46

[1664] DL Schilling, *'Meteor Burst Communications: Theory and Practice'*, Wiley 1993

[1665] DC Schleher, *'Electronic Warfare in the Information Age'*, Artech House 1999

[1666] D Schmandt-Besserat, *'How Writing Came About'*, University of Texas Press 1996

[1667] MN Schmitt, *'Tallinn Manual on the International Law Applicable to Cyber Warfare'*, Cambridge University Press, first edition 2013; second edition 2017

[1668] ZE Schnabel, "The estimation of the total fish population in a lake", in *American Mathematical Monthly* v 45 (1938) pp 348–352

[1669] PM Schneider, "Datenbanken mit genetischen Merkmalen von Straftätern", in *Datenschutz und Datensicherheit* v 22 (6/1998) pp 330–333

[1670] B Schneier, *'Applied Cryptography'*, Wiley (1996)

[1671] B Schneier, "Why Computers are Insecure", in `comp.risks` v 20.67

[1672] B Schneier, *'Secrets and Lies : Digital Security in a Networked World'*, Wiley 2000

[1673] B Schneier, "Semantic Attacks: The Third Wave of Network Attacks", in *Crypto-Gram Newsletter* October 15 2000

[1674] B Schneier, *'Beyond Fear: Thinking Sensibly about Security in an Uncertain World'*, Copernicus Books (2003)

[1675] B Schneier, "Real-World Passwords", in *Crypto-Gram Newsletter* Dec 14, 2006

[1676] B Schneier, "Choosing Secure Passwords", in *Crypto-Gram Newsletter* Aug 7 2007

[1677] B Schneier, "Secure Passwords Keep You Safer, in *Crypto-Gram Newsletter* Jan 11, 2007

[1678] B Schneier, "The Psychology of Security", *RSA Conference* (2007), at `http://www.schneier.com/essay-155.html`

[1679] B Schneier, "Random Number Bug in Debian Linux", May 19 2020

[1680] B Schneier, “Excess Automobile Deaths as a Result of 9/11”, Sep 9 2013

[1681] B Schneier, “Evaluating the GCHQ Exceptional Access Proposal”, *Lawfare Blog* Jan 17 2019

[1682] B Schneier, *‘The Originality Engine – How Hacking Changes the World, for Better and for Worse’*, to appear in 2021; Bruce announced this book at the 2020 Workshop on Security and Human Behaviour, liveblogged at `https://www.lightbluetouchpaper.org/2020/06/18/security-and-human-behaviour-2020/`

[1683] B Schneier, A Shostack, “Breaking up is Hard to Do: Modeling Security Threats for Smart Cards,” in *USENIX Workshop on Smart Card Technology* 1999, pp 175–185

[1684] M Schnyder, “Datenfluesse im Gesundheitswesen”, in *in Symposium für Datenschutz und Informationssicherheit*, Zuerich, Oct 98

[1685] RA Scholtz, “Origins of Spread-Spectrum Communications”, in *IEEE Transactions on Communications* v TC-30 no 5 (May 1982) pp 822–854

[1686] M Schrems, “CJEU Judgment – First Statement”, `https://noyb.eu` July 16 2020

[1687] MD Schroeder, *‘Cooperation of Mutually Suspicious Subsystems in a Computer Utility’*, MIT PhD Thesis, September 1972, Project MAC Technical Report MAC TR-104 `http://hdl.handle.net/ncstrl.mit_lcs/MIT/LCS/TR-104`

[1688] Schumpeter, “Live-streaming will change rock ’n’ roll for the better”, *The Economist*, Jun 17 2020

[1689] Schumpeter, “Why companies struggle with recalcitrant IT”, *The Economist*, Jul 18 2020

[1690] K Schwab, “How googly eyes solved one of today’s trickiest UX problems” *Fast Company* Aug 27 2019

[1691] M Schwarz, S Weiser, D Gruss, “Practical Enclave Malware with Intel SGX”, *arXiv:1902.03256* Feb 8, 2019

[1692] M Schwarz, S Weiser, D Gruss, C Maurice, S Mangard, “Malware Guard Extension: abusing Intel SGX to conceal cache attacks”, *Cybersecurity* v 3 (2020)

[1693] N Scola. “Kamala Harris’ Crusade Against ‘Revenge Porn’ ”, *Politico* Feb 1 2019

[1694] M Scorgie, “Untapped sources for accountants” in *Genizah Fragments* (The Newsletter of Cambridge University’s Taylor-Schechter Genizah Research Unit) no 29 (April 1995), at `http://www.lib.cam.ac.uk/Taylor-Schechter/GF/GF29.html`

[1695] J Scott-Railton, A Hulcoop, B Abdul Razzak, B Marczak, S Anstis, R Deibert, “Dark Basin – Uncovering a Massive Hack-For-Hire Operation”, *Citizen Lab* June 9 2020

[1696] Beale Screamer, “Microsoft DRM – Technical description” and supporting documents, on *Cryptome.org*, Oct 23 2001; at `http://cryptome.org/beale-sci-crypt.htm`

[1697] M Seaborn, T Dullien, “Exploiting the DRAM rowhammer bug to gain kernel privileges”, *Google project zero blog* Mar 9 2015

[1698] T Seals 2020, “70 Percent of Mobile, Desktop Apps Contain Open-Source Bugs”, *Threatpost* May 25 2020

[1699] “New RCS technology exposes most mobile users to hacking”, Security Research Labs, Nov 29 2019, `https://www.srlanbs.de/bites/rcs-hacking/`

[1700] E Selleck, “Apple’s App Store is Populated With Gambling and Other Apps That Abuse Enterprise Certificates”, *iPhone Hacks*, Feb 12 2019

[1701] L Seltzer, “New Intel tech protects point-of-sale data”, *ZDNet* Oct 15 2014

[1702] W Seltzer, M Anderson, “Census Confidentiality under the Second War Powers Act (1942-1947),” Annual Meeting of the Population Association of America, Mar 30 2007, New York; at *Official Statistics and Statistical Confidentiality: Recent Writings and Essential Documents*, at `http://www.uwm.edu/~margo/govstat/integrity.htm`

[1703] R Senderek, *‘Key-Experiments – How PGP Deals With Manipulated Keys’*, 2000, at `http://senderek.de/security/key-experiments.html`

[1704] Chandak Sengoopta, *‘Imprint of the Raj’*, Pan Macmillan 2004

[1705] R Severo, “Hedy Lamarr, Sultry Star Who Reigned in Hollywood Of 30’s and 40’s, Dies at 86”, *New York Times* Jan 20 2000; US patent no 2,292,387 (HK Markey et al., Aug 11 1942)

[1706] A Shamir, “How to share a secret”, in *Communications of the ACM* v 22 no 11 (Nov 1979) pp 612–613

[1707] A Shamir, “Identity-based cryptosystems and signature schemes”, in *Proceedings of Crypto 1984*, Springer LNCS v 196, pp 47–53

[1708] A Shamir, “Research Announcement: Microprocessor Bugs Can Be Security Disasters”, Nov 2007, at `http://cryptome.org/bug-attack.htm`

[1709] A Shamir, I Safran, E Ronen, O Dunkelman, “A Simple Explanation for the Existence of Adversarial Examples with Small Hamming Distance”, *arXiv 1901.10861*, Jan 30 2019

[1710] M Sherr, E Cronin, S Clark, M Blaze, “Signaling vulnerabilities in wiretapping systems”, *IEEE Security and Privacy* v 3 no 6 (Nov/Dec 2005) pp 13–25

[1711] H Shacham, “The geometry of innocent flesh on the bone: return-into-libc without function calls (on the x86)” *ACM CCS* 2007 pp 552–561.

[1712] Y Shachmurove, G Fishman, S Hakim, “The burglar as a rational economic agent”, Technical Report CARESS Working Paper 97-07, U Penn University of Pennsylvania Center for Analytic Research in Economics and the Social Sciences, June 1997

[1713] J Shafer, “Trump’s Daily Dose of Distraction”, *Politico* May 19 2020

[1714] G Shah, A Molina, M Blaze, “Keyboards and Covert Channels”, in *15th USENIX Security Symposium* 2006, at `http://www.crypto.com/papers/`

[1715] A Shaik, R Borgaonkar, SJ Park, JP Seifert, “New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities”, *WiSec 2019* pp 221–231

[1716] Y Shaked, A Wool, “Cracking the Bluetooth PIN”, *Mobisys 2005*

[1717] CE Shannon, “A Mathematical Theory of Communication”, in *Bell Systems Technical Journal* v 27 (1948) pp 379–423, 623–656

[1718] CE Shannon, “Communication theory of secrecy systems”, in *Bell Systems Technical Journal* v 28 (1949) pp 656–715

[1719] C Shapiro, “Antitrust in a time of populism”, *SSRN 3058345*, 2017

[1720] C Shapiro, “Protecting Competition in the American Economy: Merger Control, Tech Titans, Labor Markets”, *Journal of Economic Perspectives* v 33 no 3 (2019) pp 69–93

[1721] C Shapiro, H Varian, *‘Information Rules’*, Harvard Business School Press 1998

[1722] K Sharad, G Danezis, “An Automated Social Graph De-anonymization Technique”, *WPES ’14 – Workshop on Privacy in the Electronic Society* (2014) pp 47–58

[1723] M Sharif, S Bhagavatula, L Bauer, M Reiter, “Accessorize to a Crime: Real and Stealthy Attacks on State-Of-The-Art Face Recognition”, *ACM CCS* (2016)

[1724] D Sherwin, “Fraud – the Unmanaged Risk”, in *Financial Crime Review* v 1 no 1 (Fall 2000) pp 67–69

[1725] S Sheye, “SSL Client Certificates – Not Securing the Web”, in *Cryptomathic NewsOnInk Quarterly Newsletter* (Nov 2006)

[1726] B Shneiderman, “Human-Centred Artificial Intelligence: Reliable, Safe and Trustworthy”, *International Journal of Computer-Human Interaction* v 36 no 6 (2020) pp 495–504

[1727] JF Shoch, JA Hupp, “The ‘Worm’ Programs – Early Experience with a Distributed Computation”, *Comm ACM* v 25 no 3 (1982) pp 172–180

[1728] PW Shor, “Algorithms for Quantum Computers”, in *35th FOCS* (1994), IEEE, pp 124–134

[1729] A Short, *‘Response to FOI request to Driver and vehicle Standards Agency’*, Jan 13 2020, at `https://www.whatdotheyknow.com/request/tachograph_offence_statistics`

[1730] A Shostack, P Syverson, "What Price Privacy? (and why identity theft is about neither identity nor theft)", in *Economics of Information Security*, Kluwer Academic Publishers, 2004, Chapter 11

[1731] V Shoup, "OAEP Reconsidered", IBM Zürich, Switzerland, September 18, 2001

[1732] JL Shreeve, "Chip and Pain: A Financial Fiasco", *The Independent* April 22 2009

[1733] I Shumailov, YR Zhao, D Bates, N Papernot, R Mullins, R Anderson, "Sponge Examples: Energy-Latency Attacks on Neural Networks", *arXiv 2006.03463* Jun 5 2020

[1734] I Shumailov, L Simon, J Yan, R Anderson, "Hearing your touch: A new acoustic side channel on smartphones", *arXiv:1903.11137* (2019), based on first author's MPhil thesis of 2017

[1735] I Shumailov, YR Zhao, R Mullins, R Anderson, "The taboo trap: Behavioural detection of adversarial samples", *arXiv:1811.07375* Nov 18 2018

[1736] I Shumailov, YR Zhao, R Mullins, R Anderson, "Towards Certifiable Adversarial Sample Detection", *arXiv:2002.08740*, Feb 20 2020

[1737] D Shumow, N Ferguson, "On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng", *Crypto rump session* (2007)

[1738] O Sibert, D Bernstein, D Van Wie, "The DigiBox: A Self-Protecting Container for Information Commerce", *Usenix Security* (1995)

[1739] O Sibert, PA Porras, R Lindell, "An Analysis of the Intel 80x86 Security Architecture and Implementations", in *IEEE Transactions on Software Engineering* v 22 no 5 (May 96) pp 283–293

[1740] D Silver, A Huang, CJ Maddison, A Guez, L Sifre, G van den Driessche, J Schrittwieser, I Antonoglou, V Panneershelvam, M Lanctot, S Dieleman, D Grewe, J Nham, N Kalchbrenner, I Sutskever, T Lillicrap, M Leach, K Kavukcuoglu, T Graepel, D Hassabis, "Mastering the game of Go with deep neural networks and tree search" *Nature* v 529 (2016) pp 484–489

[1741] C Silverman, "Apps Installed On Millions Of Android Phones Tracked User Behavior To Execute A Multimillion-Dollar Ad Fraud Scheme", *BuzzFeed News*, Oct 23 2018

[1742] C Silverman, "Popular VPN And Ad-Blocking Apps Are Secretly Harvesting User Data", *BuzzFeed News*, Mar 9 2020

[1743] C Silverman, R Mac, "Facebook Fired An Employee Who Collected Evidence Of Right-Wing Pages Getting Preferential Treatment", *BuzzFeed News*, Aug 6 2020

[1744] C Silverman, R Mac, P Dixit, " 'I Have Blood on My Hands': A Whistleblower Says Facebook Ignored Global Political Manipulation", *BuzzFeed News*, Sep 14 2020

[1745] N Silvester, "Doctor who hacked into Prime Minister's health records escapes prosecution", *Daily Record* Jan 10 2012

[1746] C Simoiu, C Gates, J Bonneau, S Goel, " 'I was told to buy a software or lose my computer. I ignored it': A study of ransomware", *SOUPS 2019*

[1747] *Luther Simjian – Inventor of the Week*, at `https://lemelson.mit.edu/resources/luther-george-simjian`

[1748] D Simmons, "BBC fools HSBC voice recognition security system", *BBC* May 19 2017

[1749] GJ Simmons, "The Prisoners' Problem and the Subliminal Channel", in *Proceedings of CRYPTO '83*, Plenum Press (1984) pp 51–67

[1750] GJ Simmons, "A system for verifying user identity and authorization at the point-of sale or access," *Cryptologia* v 8 no 1 (1984) pp 1–21

[1751] GJ Simmons, "How to Insure that Data Acquired to Verify Treaty Compliance are Trustworthy", GJ Simmons, *Proceedings of the IEEE* v 76 no 5 (1988; reprinted as a chapter in [1752])

[1752] GJ Simmons (ed) *'Contemporary Cryptology – The Science of Information Integrity'*, IEEE Press (1992)

[1753] GJ Simmons, "A Survey of Information Authentication", in [1752] pp 379–439

[1754] GJ Simmons, "An Introduction to Shared Secret and/or Shared Control Schemes and Their Application", in [1752] pp 441–497

[1755] GJ Simmons, invited talk at the *1993 ACM Conference on Computer and Communications Security*, Fairfax, Virginia, Nov 3–5, 1993

[1756] GJ Simmons, "Subliminal Channels; Past and Present", *European Transactions on Telecommunications* v 5 no 4 (Jul/Aug 94) pp 459–473

[1757] GJ Simmons, "The History of Subliminal Channels", in *IEEE Journal on Selcted Areas in Communications* v 16 no 4 (April 1998) pp 452–462

[1758] H Simon, *'Administrative Behavior'*, 4th ed., Free Press 1997

[1759] H Simon, *'The Sciences of the Artificial'*, 3rd ed., MIT Press 1996

[1760] L Simon, RJ Anderson, "PIN Skimmer: Inferring PINs Through The Camera and Microphone", *Third ACM workshop on Security and Privacy in Smartphones & mobile devices (SPSM 2013)* pp 67–78

[1761] L Simon, RJ Anderson, "Security Analysis of Android Factory Resets", *Mobile Security Technologies (MoST) 2015*

[1762] L Simon, D Chisnall, RJ Anderson, "What you get is what you C: Controlling side effects in mainstream C compilers", *IEEE European Symposium on Security and Privacy (EUro S&P)* 2018, `https://sites.google.com/view/laurent-simon`

[1763] L Simon, WD Xu, RJ Anderson, "Don't interrupt me while I type: Inferring text entered through gesture typing on android keyboards", *PoPETs* 2016 v 3 pp 136–154

[1764] R Singel, "Yahoo Outed Chinese Dissident Knowing Investigation Was Political, Documents Show – UPDATED", in *Wired* July 31 2007

[1765] R Singel, "Point, Click … Eavesdrop: How the FBI Wiretap Net Operates", in *Wired* Aug 29 2007

[1766] N Singer, A Krolik, "Grindr and OkCupid Spread Personal Details, Study Says", *EarthInfo Now* Jan 14 2019

[1767] N Singer, N Perlroth, A Krolik, "Zoom Rushes to Improve Privacy for Consumers Flooding Its Service", *New York Times* Apr 8 2020

[1768] M Singh, P Leu, S Capkun, "UWB with Pulse reordering: Securing Ranging Against Relay and Physical-Layer Attacks", *NDSS 2019*

[1769] A Sipress, "Tracking Traffic by Cell Phone; Md., Va. to Use Transmissions to Pinpoint Congestion", in *Washington Post* (22/12/1999) p A01

[1770] KS Siyan, J Casad, J Millecan, D Yarashus, P Tso, J Shoults, *'Windows NT Server 4 – Professional Reference'*, New Riders Publishing (1996)

[1771] SP Skorobogatov, "Copy Protection in Modern Microcontrollers", at `http://www.cl.cam.ac.uk/~sps32/mcu_lock.html`

[1772] SP Skorobogatov, *'Low temperature data remanence in static RAM'*, Cambridge University Technical Report UCAM-CL-TR-536 (June 2002)

[1773] SP Skorobogatov, *'Semi-invasive attacks – A new approach to hardware security analysis'*, PhD Thesis, 2004; University of Cambridge Technical Report 630, 2005

[1774] SP Skorobogatov, "Data Remanence in Flash Memory Devices", in *CHES 2005* pp 339–353

[1775] SP Skorobogatov, "Optically Enhanced Position-Locked Power Analysis", in *CHES 2006* pp 61–75

[1776] SP Skorobogatov, "Tamper resistance and physical attacks", at *Summer School on Cryptographic Hardware, Side-Channel and Fault Attacks*, June 12–15, 2006, Louvain-la-Neuve, Belgium; slides at `http://www.cl.cam.ac.uk/~sps32`

[1777] SP Skorobogatov, "Optical surveillance on silicon chips: your crypto keys are visible", Security group seminar Oct 13 2009, slides at `https://www.cl.cam.ac.uk/~sps32/`

[1778] SP Skorobogatov, "Flash Memory 'Bumping' Attacks", *CHES 2010*

[1779] SP Skorobogatov, C Woods, "Breakthrough silicon scanning discovers backdoors in military chip", *CHES 2012*

[1780] SP Skorobogatov, "Security, reliability and back doors", Security group seminar May 13 2013, slides at `https://www.cl.cam.ac.uk/~sps32/`

[1781] SP Skorobogatov, "The bumpy road towards iPhone 5c NAND mirroring", arXiv:1609.04327, Sep 14 2016; project page at `https://www.cl.cam.ac.uk/~sps32/5c_proj.html`

[1782] SP Skorobogatov, "Deep dip teardown of tubeless insulin pump", *arXiv:1709.06026*, Sep 18 2017

[1783] SP Skorobogatov, "How microprobing can attack encrypted memory", *Proceedings of Euromicro Conference on Digital System Design, AHSA 2017 Special Session* (2017)

[1784] SP Skorobogatov, "Hardware Security: Present challenges and Future directions", *IC Hardware Analysis Workshop, NTU, Singapore 2018* at `http://www.cl.cam.ac.uk/~sps32`

[1785] SP Skorobogatov, "Is Hardware Security prepared for unexpected discoveries?", *2018 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits* pp 1–4

[1786] SP Skorobogatov, RJ Anderson, "Optical Fault Induction Attacks", in *Cryptographic Hardware and Embedded Systems Workshop* (CHES 2002), Springer LNCS v 2523 pp 2–12

[1787] SP Skorobogatov, C Woods. "In the blink of an eye: There goes your AES key" *IACR Preprint 2012/296*

[1788] B Skyrms, *'Evolution of the Social Contract'*, Cambridge University Press (1996)

[1789] R Sleevi, "What's wrong with the ecosystem", *CA Browser Forum* (2014), `https://cabforum.org/wp-content/uploads/CABF45-Sleevi-Whats-Wrong-With-the-Ecosystem.pdf`

[1790] R Sleevi, "Sustaining Digital Certificate Security", *Google Security Blog* Oct 28 2015

[1791] P Slovic, ML Finucane, E Peters, DG MacGregor, "Rational Actors or Rational Fools? Implications of the Affect Heuristic for Behavioral Economics"; revised version as "The Affect Heuristic" in *Heuristics and Biases: The Psychology of Intuitive Judgment*, CUP (2002) pp 397–420

[1792] A Smith, *'An Inquiry into the Nature and Causes of the Wealth of Nations'*, 1776

[1793] A Smith, "New fake £20 notes 'trick shop assistants then peel off within a week' ", *Metro* Nov 15 2018

[1794] B Smith, "What's Facebook's Deal With Donald Trump?" *New York Times* June 21 2020

[1795] B Smith, "The Week Old Hollywood Finally, Actually Died" *New York Times* Aug 16 2020

[1796] C Smith, *'The Car Hacker's Handbook'*, No Starch Press, 2016

[1797] E Smith, "The Incredibly Technical History of Digital Rights Management", *Vice* Oct 19 2017

[1798] RE Smith, "Constructing a high assurance mail guard", in *Seventeenth National Computer Security Conference* (1994) pp 247–253

[1799] SW Smith, SH Weingart, "Building a High-Performance, Programmable Secure Coprocessor", IBM Technical report RC 21102, also in *Computer Networks (Special Issue on Computer Network Security)* v 31 (Apr 1999) pp 831–860

[1800] P Smulders, "The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables", in *Computers & Security* v 9 (1990) pp 53–58

[1801] T Snoke, "Best Practices for NTP Services", *SEI Blog* April 3 2017

[1802] T Snyder, *'The Road to Unfreedom'*, Bodley Head 2018

[1803] O Solon, "NHS patient data made publicly available online", *Wired* Mar 3 2014

[1804] D Solove, "A Taxonomy of Privacy", in *University of Pennsylvania Law Review* v 154 no 3 (2006) pp 477–560; at `http://papers.ssrn.com/abstract_id=667622`

[1805] A Soltani, R Calo, C Bergstrom, "Contact-tracing apps are not a solution to the COVID-19 crisis", *TechStream* April 27, 2020

[1806] R Sommer, V Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection", *IEEE Symposium on Security and Privacy* (2010)

[1807] DX Song, D Wagner, XQ Tian, "Timing analysis of keystrokes and SSH timing attacks", in *Proceedings of 10th USENIX Security Symposium* (2001)

[1808] R v Department of Health, ex parte Source Informatics: [2000] 2 WLR 940

[1809] 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`

[1810] E Spafford, "The Internet worm program: an analysis", in *Computer Communications Review* v 19 no 1 (Jan 89) pp 17–57

[1811] A Sparrow, "NHS patient records may be shared with private companies", The Guardian Dec 4 2011

[1812] J Specht, "The price of plenty: how beef changed America", *The Guardian* 7 May 2019, and *'Red Meat Republic'*, Princeton University Press (2019)

[1813] M Specter, "Do fingerprints lie? The gold standard of forensic evidence is now being challenged", *New York Times*, May 27, 2002

[1814] MA Specter, J Koppel, D Weitzner, "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections", Feb 13 2020

[1815] R Spencer, S Smalley, P Loscocco, M Hibler, D Andersen, J Lepreau, "The Flask Security Architecture: System Support for Diverse Security Policies," in *Proceedings of the 8th USENIX Security Symposium* (1999) pp 123–139

[1816] C Spensky, J Stewart, A Yerukhimov, R Shay, A Trachtenberg, R Housley, RK Cunningham, "SoK: Privacy on Mobile Devices – It's Complicated", *Proceedings on Privacy Enhancing Technologies* vol 2016 no 3

[1817] "Tip von Urmel", in *Der Spiegel*, Sep 11 1995

[1818] N Springer, "When Apps Get Your Medical Data, Your Privacy May Go With It", *New York Times* Sep 3 2019

[1819] S Stamm, Z Ramzan, M Jakobsson, "Drive-By Pharming", *Indiana University Department of Computer Science Technical Report TR641*, 2006

[1820] M Stamp, RM Low, *'Applied Cryptanalysis'*, Wiley 2007

[1821] T Standage, *'The Victorian Internet'*, Phoenix Press 1999

[1822] F Stajano, RJ Anderson, "The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks", in *'Security Protocols – 7th International Workshop'*, Springer LNCS 1796 pp 172–182

[1823] F Stajano, P Wilson, "Understanding scam victims: seven principles for systems security", *Cambridge University Computer Lab tech report no 754* (2009)

[1824] S Staniford, D Moore, V Paxson, N Weaver, "The Top Speed of Flash Worms", in *WORM04*, 2004

[1825] "Computer Chip Usage in Toner Cartridges and Impact on the Aftermarket: Past, Current and Future", Static Control, Inc., formerly at `http://www.scc-inc.com/special/oemwarfare/whitepaper/default.htm`, retrieved via `www.archive.org`

[1826] N Statt, "Fortnite for Android will ditch Google Play Store for Epic's website", *The Verge* Aug 3 2018

[1827] WA Steer, "VideoDeCrypt", at `http://www.ucl.ac.uk/~ucapwas/vdc/`

[1828] P Stein, P Feaver, *'Assuring Control of Nuclear Weapons'*, CSIA occasional paper number 2, Harvard University 1987

[1829] 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)'*

[1830] N Stephenson, *'Snow Crash'*, Bantam Doubleday Dell (1992)

[1831] M Stevens, E Bursztein, P Karpman, A Albertini, Y Markov, A Petit Bianco, C Baisse, "Announcing the first SHA1 collision", Google security blog (Feb 23 2017)

[1832] DR Stinson, *'Cryptography – Theory and Practice'*, CRC Press 1995

[1833] M Stoller, “Absentee Ownership: How Amazon, Facebook, and Google Ruin Commerce Without Noticing”, *BIG by Matt Stoller* Jul 28 2020

[1834] M Stoller, “Warren Buffett: America’s Folksiest Predator”, *BIG by Matt Stoller* Aug 10 2020

[1835] B Stone, “Amazon Erases Orwell Books From Kindle”, *New York Times* Jul 17 2009

[1836] B Stone-Gross, T Holz, G Stringhini, G Vigna, “The Underground Economy of Spam: A Botmaster’s Perspective of Coordinating Large-Scale Spam Campaigns”, *USENIX Workshop on Large-Scale Exploits and Emerging Threats (LEET)* (2011)

[1837] PO Stoutland, S Pitts-Kiefer, *‘Nuclear Weapons in the New Cyber Age’*, Nuclear Threat Initiative 2018

[1838] O Storbeck, T Kinder, S Palma, “EY failed to check Wirecard bank statements for 3 years”, *Financial Times* Jun 26 2020

[1839] S Stover, D Dittrich, J Hernandez, S Dittrich, “Analysis of the Storm and Nugache trojans: P2P is here”, *;login* Dec 2007

[1840] J van der Straaten, “So You Think Digital is the Future? Your Internet Data is Rotting”, *Researchgate* May 2019

[1841] R Strehle, *‘Verschlüsselt – Der Fall Hans Bühler’*, Werd Verlag 1994

[1842] E Strickland, “Expert Questions Claim That St. Jude Pacemaker Was Hacked”, *IEEE Spectrum* Sep 2 2016

[1843] DH Strobel, B Driessen, T Kasper, G Leander, D Oswald, F Schellenberg, C Paar, “Fuming Acid and Cryptanalysis: Handy Tools for Overcoming a Digital Locking and Access Control System”, *Crypto 2013* pp 147–164

[1844] A Stubblefield, J Ioannidis, A Rubin, “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”, in *ISOC 2002*

[1845] C Stupp, “Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case”, *Wall Street Journal*, Aug 30 2019

[1846] G Suarez-Tanguil, G Stringhini, “Eight Years of Rider Measurement in the Android Malware Ecosystem”, *IEEE Transactions on Dependable and Secure Computing* (2018)

[1847] Suetonius (Gaius Suetonius Tranquillus), *‘Vitae XII Caesarum’*, translated into English as *‘History of twelve Caesars’* by Philemon Holland, 1606; Nutt 1899

[1848] T Sugawara, B Cyr, S Rampazzi, D Genkin, K Fu, “Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems”, at *https://lightcommands.com* Nov 11 2019

[1849] J Suler, “The Online Disinhibition Effect”, *CyberPsychology & Behavior* (July 2004)

[1850] SC Sundaramurthy, M Wesch, XM Ou, J McHugh, SR Rajagopalan, AG Bardas, “Humans Are Dynamic - Our Tools Should Be Too”, *IEEE Internet Computing* v 21 (May-June 2017) pp 40–46

[1851] D Sutherland, “A Model of Information”, in *9th National Computer Security Conference* (1986)

[1852] T Swarbrick, “Our National Security Council is a joke”, *Unherd* May 20 2020

[1853] L Sweeney, “Weaving Technology and Policy Together to Maintain Confidentiality”, in *Journal of Law, Medicine and Ethics* v 25 no 2–3 (1997) pp 98–110

[1854] L Sweeney, JS Yoo, L Perovich, KE Boronow, P Brown, JG Brody, “ Re-identification Risks in HIPAA Safe Harbor Data: A study of data from one environmental health study”, *Technology Science* 2017082801 (2017)

[1855] F Swiderski, W Snyder, *‘Threat Modeling’*, Microsoft Press 2004

[1856] P Swire, “Efficient Confidentiality for Privacy, Security, and Confidential Business Information”, Brookings-Wharton Papers on Financial Services (2003), at `http://ssrn.com/abstract=383180`

[1857] P Swire, “A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Agencies”, in *Houston Law Review* v 42 no 5 (Jan 2006) pp 101–148; at `http://ssrn.com/abstract_id=842228`

[1858] *Symposium On Usable Privacy and Security*, `http://cups.cs.cmu.edu/soups/2007/`

[1859] J Szczesny, "Daimler Agrees to Multi-Billion Dollar Diesel Settlement for U.S. Company paying out more than $2.2 billion", *The Detroit Bureau*, Aug 14 2020

[1860] C Szegedy, W Zaremba, I Sutskever, J Bruna, D Erhan, IJ Goodfellow, R Fergus, "Intriguing properties of neural networks", *arXiv 1312.6199* (2013)

[1861] A Tang, S Sethumadhavan, S Stolfo, "CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management", *Usenix Security* (2017)

[1862] S Tajik, F Ganji, JP Seifert, H Lohrke, C Boit, "Laser Fault Attack on Physically Unclonable Functions", *FDTC 2015*

[1863] AS Tanenbaum, M van Steen *'Distributed systems'*, Prentice Hall 2002

[1864] T Tanielian, LH Jaycox, "Invisible Wounds of War", *Rand Corporation*, 2008; p 128, 436

[1865] C Tarnovsky, "Sophisticated Million Dollar Hack To Discover Weaknesses In A Series Of Smartcards", `https://youtu.be/2td3-sWsiKg`; and "Exposing The Deep-Secure Elements Of Smartcards", `https://youtu.be/-vnik_iUuUs`, both at *hardwear.io* (2019)

[1866] C Tavris, E Aronson, *'Mistakes were made – but not by me'*, Harcourt 2007

[1867] J Taylor, "Major breach found in biometrics system used by banks, UK police and defence firms", *The Guardian* Aug 14 2019

[1868] J Taylor, MR Johnson, CG Crawford, *'DVD Demystified'*, Third edition, McGraw-Hill 2006

[1869] J Tehranian, "An Unhurried View of Copyright Reform: Bridging the Law/Norm Gap", *Utah Law Review* (2007)

[1870] J Temperton, "Inside Sellafield: how the UK's most dangerous nuclear site is cleaning up its act", *Wired*, 17 September 2016

[1871] S Tendler, N Nuttall, "Hackers run up £1m bill on Yard's phones", in *The Times*, 5 Aug 1996

[1872] T Tengs, M Adams, J Pliskin, D Safran, J Siegel, M Weinstein, J Graham, "Five-hundred life-saving interventions and their cost-effectiveness", *Risk Analysis* v 15 no 3 (1995) pp 369–390

[1873] *'Tesla deaths'*, at `https://www.tesladeaths.com/`, June 23 2020

[1874] E Tews, *'DECT Security Analysis'*, PhD Thesis, Darmstadt, 2012

[1875] E Tews, J Wälde, M Weiner, "Breaking DVB-CSA", in *Western European Workshop, WEWoRC 2011*

[1876] E Tews, RP Weinmann, A Pyshkin, "Breaking 104 bit WEP in less than 60 seconds", *Cryptology ePrint archive*, Apr 2007

[1877] RH Thaler, *'Misbehaving: The Making of Behavioural Economics'*, Penguin 2016

[1878] RH Thaler, "Nudge, not sludge", *Science* v 361 no 6401 (2018) p 431

[1879] R Thaler, C Sunstein, *'Nudge'*, Penguin 2009

[1880] L Thalheim, J Krissler, PM Ziegler, "Body Check – Biometric Access Protection Devices and their Programs Put to the Test", *c't magazine*, Nov 2002 p 114

[1881] H Thimbleby, "Improving safety in medical devices and systems", *IEEE International Conference on Healthcare Informatics* (2013)

[1882] H Thimbleby, "Safer user interfaces: A case study in improving number entry", *IEEE Transactions on Software Engineering* v 41 no 7 (2015) pp 711–729

[1883] DR Thomas, AR Beresford, A Rice, "Security Metrics for the Android Ecosystem", *Workshop on Security and Privacy in Smartphones and Mobile Devices, 2015* pp 87–98

[1884] TL Thomas, "Dragon Bytes: Chinese Information-War Theory and Practice", Foreign Military Studies Office, Fort Leavenworth, Kansas, 2004

[1885] K Thomas, A Moscicki, "New research: How effective is basic account hygiene at preventing hijacking", *Google Security Blog* May 17 2019

[1886] C Thompson, "YouTube's Plot to Silence Conspiracy Theories", *Wired* Sep 18 2020

[1887] K Thompson, "Reflections on Trusting Trust", in *Communications of the ACM* v 27 no 8 (Aug 84) pp 761–763

[1888] R Thompson, "Google Sponsored Links Not Safe", Exploit Prevention Labs Apr 24 2007, at `http://explabs.blogspot.com/2007/04/google-sponsored-links-not-safe.html`; see also J Richards, "Hackers hijack Google AdWords", *The Times*, Apr 27 2007

[1889] SA Thompson, C Warzel, "Twelve Million Phones, One Dataset, Zero Privacy", *New York Times* Dec 19, 2019

[1890] I Thomson, "Talk about unintended consequences: GDPR is an identity thief's dream ticket to Europeans' data", in *The Register* Aug 9 2019

[1891] S Thrun, M Montemerlo, H Dahlkamp, D Stavens, A Aron, J Diebel, P Fong, J Gale, M Halpenny, G Hoffmann, KL Oakley, M Palatucci, V Pratt, P Stang, S Strohband, C Dupont, LE Jendrossek, C Koelen, C Markey, C Rummel, J van Niekerk, E Jensen, P Alessandrini, G Bradski, B Davies, S Ettinger, A Kaehler, A Nefian, P Mahoney, "Stanley: The Robot That Won the DARPA Grand Challenge", *Journal of Field Robotics*, Springer Texts in Advanced Robotics v 36, pp 1–43; at `https://robots.stanford.edu/papers/thrun.stanley05.pdf`

[1892] Y Tian, C Herley, S Schechter, "StopGuessing: Using Guessed Passwords to Thwart Online Guessing", *EuroS&P* (2019)

[1893] TimeWarner, "Carmine Caridi, Motion Picture Academy Member Who Handed Over His Awards Screeners for Illegal Duplication, Ordered to Pay $300,000 to Warner Bros. Entertainment Inc.", Nov 23 2004, at `http://www.timewarner.com/corp/newsroom/pr/0,20812,832500,00.html`

[1894] 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

[1895] MW Tobias, *'Locks, Safes and Security – An International Police Reference'*, at `https://www.securitylaboratories.org/`

[1896] MW Tobias, "Opening locks by bumping in five seconds or less: is it really a threat to physical security?", 2006, at `https://www.securitylaboratories.org/`

[1897] MW Tobias, "Bumping of locks – legal issues in the United States", at `https://www.securitylaboratories.org/`

[1898] MW Tobias, "The Medeco M3 Meets the Paper Clip: Is the security of this lock at risk?" (2007), at `https://www.securitylaboratories.org/`

[1899] C Tomlinson, *'Rudimentary Treatise on the Construction of Locks'*, 1853 (excerpt), at `http://www.deter.com/unix/papers/treatise_locks.html`

[1900] TT Tool, *'The MIT Lock Picking Manual'*, 1991; at `http://people.csail.mit.edu/custo/MITLockGuide.pdf`

[1901] R Torrance, D James, "The State-of-the-Art in IC Reverse Engineering", *CHES 2009* pp 363–381; also at *DAC '11* pp 333–338

[1902] MA Toy, "Chinese hack into film festival site", *Sydney Morning Herald* July 26 2009

[1903] F Tramèr, P Dupré, G Rusak, G Pellegrino, D Boneh, "AdVersarial: Perceptual Ad Blocking Meets Adversarial Machine Learning", *arXiv:1811.03194*, Aug 26 2019

[1904] F Tramèr, N Papernot, I Goodfellow, D Boneh, P McDaniel, "The Space of Transferable Adversarial Examples", *arXiv 1704.03453* Apr 11 2017

[1905] F Tramèr, F Zhang, A Juels, MK Reiter, T Ristenpart, "Stealing Machine Learning Models via Prediction APIs", *arXiv 1609.02943* Oct 3 2016

[1906] A Travis, "Voice ID device to track failed asylum seekers", in *The Guardian* Mar 10 2006

[1907] A Travis, "Terror suspects cleared of tampering with 'faulty' tags", in *The Guardian* Nov 1 2013

[1908] A Travis, "Man who escaped mosque in burqa was under counter-terror restrictions", in *The Guardian* Nov 5 2013

[1909] I Traynor, “DNA database agreed for police across EU”, in *The Guardian*, Jun 13 2007

[1910] P Trimintzios, C Hall, R Clayton, R Anderson, E Ouzounis, *‘Resilience of the Internet Interconnection Ecosystem’*, ENISA, April 11 2011; abridged version published at WEIS 2011

[1911] A Troianovski, “Not Just a Crisis: Coronavirus Is a Test for Putin’s Security State”, *New York Times*, Mar 19 2020

[1912] E Tromer, *‘Hardware-Based Cryptanalysis’*, PhD Thesis, Weizmann Institute of Science (2007)

[1913] C Troncoso, G Danezis, E Kosta, B Preneel, “PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance”, in *Workshop on Privacy in the Electronic Society* (2007)

[1914] C Troncoso, M Isaakidis, G Danezis, H Halpin “Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments” *Proceedings of Privacy Enhancing Technologies* 2017 v 4 307–329

[1915] Z Tufekci, “Zuckerberg’s So-Called Shift Toward Privacy”, *New York Times* March 7 2019

[1916] JD Tygar, BS Yee, N Heintze, “Cryptographic Postage Indicia”, in *ASIAN 96* (Springer-Verlag LNCS v 1179) pp 378–391, CMU tech report CMU-CS-96-113

[1917] D Uberti, “Facebook Went to War Against White Supremacist Terror After Christchurch. Will It Work?” *Vice* Oct 3 2019

[1918] R Uhlig, “BT admits staff could have fiddled system to win Concorde trip”, in *The Daily Telegraph* July 23 1997

[1919] ukcrypto mailing list, at `http://www.chiark.greenend.org.uk/mailman/listinfo/ukcrypto`

[1920] Underwriters’ Laboratories company history, at `https://www.company-histories.com/`

[1921] N Unger, S Dechand, J Bonneau, S Fahl, Hg Perl, I Goldberg, M Smith, “SoK: Secure Messaging”, *IEEE Security & Privacy*, 2015

[1922] J Ungoed-Thomas, A Lorenz, “French play dirty for £1bn tank deal”, in *Sunday Times* Aug 6 2000

[1923] United Kingdom Government, *‘e-commerce@its.best.uk’*, 2000

[1924] United Kingdom Passport Service, *‘Biometrics Enrolment Trial Report’*, May 2005

[1925] United Nations Economic Commission for Europe, *‘Proposal for a new UN regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system’*, ECE/TRANS/WP.29/2020/REVISED

[1926] M Untersinger, J Follorou, “EncroChat, cette mystérieuse société technologique prisée par le crime organisé”, *Le Monde*, Aug 3 2020

[1927] UPI newswire item, Oklahoma distribution, November 26, 1983, Tulsa, Oklahoma

[1928] US Army, *‘TM 31-210 Improvised Munitions Handbook’*, 1969, at `http://cryptome.org/tm-31-210.htm`

[1929] *‘United States Code’* – online at `http://www4.law.cornell.edu/uscode/`

[1930] United States Court of Appeals, District of Columbia Circuit, *United States Telecom Association v. Federal Communications Commission and United States of America*, no 99-1442, 15/8/2000, at `http://pacer.cadc.uscourts.gov/common/opinions/200008/99-1442a.txt`

[1931] United States Courts, *‘Wiretap Report 2017’*, at `https://www.uscourts.gov/statistics-reports/wiretap-report-2017`

[1932] US Immigration and Customs Enforcement, *‘Russian national pleads guilty for role in transnational cybercrime organization responsible for more than $568 million in losses’*, Jun 29 2020

[1933] US Navy, “ Navy Releases Collision Report for USS Fitzgerald and USS John S McCain Collisions” NNS171101-07 Nov 1 2017

[1934] S Usborne, “How did Tesla make some of its cars travel further during Hurricane Irma?”, *The Guardian* Sep 11 2017

[1935] S Vaidhyanathan, "Facebook's new move isn't about privacy. It's about domination", *The Guardian* March 7 2019

[1936] J Valenti, "Anita Sarkeesian interview: 'The word "troll" feels too childish. This is abuse' ", The Guardian Aug 29 2015

[1937] L van Hove, "Electronic Purses: (Which) Way to Go?", in *First Monday* v 5 no 7 (June 2000)

[1938] P Van Oorschot, M Wiener, "Parallel Collision Search with Application to Hash Functions and Discrete Logarithms", *Second ACM Conference on Computer and Communications Security* pp 210–218

[1939] R van Renesse, *'Optical Document Security'* (second edition), Artech House 1997

[1940] 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, pp 71–85

[1941] H van Vliet, *'Software Engineering – Principles and Practice'*, Wiley (second edition), 2000

[1942] R van Voris, "Black Box Car Idea Opens Can of Worms", in *Law News Network* Jun 4 1999

[1943] 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

[1944] H Varian, "Economic Aspects of Personal Privacy", in *Privacy and Self-Regulation in the Information Age*, National Telecommunications and Information Administration report, 1996

[1945] HR Varian, *'Intermediate Microeconomics – A Modern Approach'*, Norton 1999

[1946] HR Varian, "New Chips Can Keep a Tight Rein on Customers", *The New York Times* July 4 2002

[1947] H Varian, "Managing Online Security Risks", Economic Science Column, The New York Times, June 1, 2000

[1948] H Varian, "New chips and keep a tight rein on consumers, even after they buy a product", New York Times, July 4 2002

[1949] H Varian, "System Reliability and Free Riding", in *Economics of Information Security*, Kluwer 2004 pp 1–15

[1950] H Varian, Keynote address to the Third Digital Rights Management Conference, Berlin, Germany, January 13, 2005

[1951] M Vasek, J Bonneau, R Castellucci, C Keith, T Moore, "The Bitcoin Brain Drain: Examining the Use and Abuse of Bitcoin Brain Wallets", *Financial Cryptography* (2016)

[1952] M Vass, " 'Spearmint Rhino took my teen son's money while he was at home in bed' – more complain about lap dancing club" *Bournemouth Daily Echo* Nov 15 2014

[1953] S Vaudenay, "Security Flaws Induced by CBC Padding", *Eurocrypt 2002*

[1954] A Vaughan, "UK launched passport photo checker it knew would fail with dark skin", *New Scientist* Oct 9 2019

[1955] W Venema, "Murphy's Law and Computer Security", in *Usenix Security 96* pp 187–193

[1956] R Verdult, F Garcia, B Ege, "Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer", *Usenix 2013*

[1957] R Verdult, F Garcia, "Cryptanalysis of the Megamos Crypto automotive immobilizer" *USENIX; login* v 40 no 6 pp 17–22

[1958] A Vetterl, "Three Paper Thursday: Will we ever get IoT security right?", `www.lightbluetouchpaper.org` May 14 2020

[1959] A Vetterl, R Clayton, "Honware: A Virtual Honeypot Framework for Capturing CPE and IoT Zero Days" *APWG Symposium on Electronic Crime Research (eCrime)*, Nov 2019

[1960] "Link 16/MIDS Frequently Asked Questions", *Viasat*, at `https://www.viasat.com/support/data-links/faq`

[1961] J Vijayan, "Retail group takes a swipe at PCI, puts card companies 'on notice' ", *Computerworld* Oct 4 2007

[1962] N Villeneuve, "DNS tampering in China", Jul 10 2007

[1963] N Villeneuve, "Breaching Trust: An analysis of surveillance and security practices on China's TOM-Skype platform", *Information Warfare Monitor* Oct 1 2008

[1964] J Vincent, "Forty percent of 'AI startups' in Europe don't actually use AI, claims report", *The Verge* Mar 5 2019

[1965] 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`

[1966] 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`

[1967] VISA International, *'Integrated Circuit Chip Card – Security Guidelines Summary*, version 2 draft 1, November 1997

[1968] A Viterbi, "Spread spectrum communications – myths and realities", in *IEEE Communications Magazine* v 17 no 3 (May 1979) pp 11–18

[1969] PR Vizcaya, LA Gerhardt, "A Nonlinear Orientation Model for Global Description of Fingerprints", in *Pattern Recognition* v 29 no 7 (July 96) pp 1221–1231

[1970] W Vogels, "Modern applications at AWS", *All Things Distributed*, Aug 28 2019

[1971] G Volovik, *'The Universe in a Helium Droplet'*, Clarendon Press, Oxford 2003

[1972] L von Ahn, *personal communication*, 2006

[1973] L von Ahn, M Blum, NJ Hopper, J Langford, "CAPTCHA: Using Hard AI Problems For Security", *Advances in Cryptology – Eurocrypt 2003*, Springer LNCS v 2656 pp 294–311

[1974] A Vrij, *'Detecting Lies and Deceit: Pitfalls and Opportunities'*, Wiley 2008

[1975] 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

[1976] 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/`

[1977] D Wagner, B Schneier, "Analysis of the SSL 3.0 Protocol", in *Second USENIX Workshop on Electronic Commerce* (1996), pp 29–40

[1978] 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

[1979] J Walker, "IC Surgery: getting to the heart of the problem with the smallest scalpel" *HardwearIO* (2019) at `https://youtu.be/o1We1o3tMWc`

[1980] 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`

[1981] E Waltz, *'Information Warfare – Principles and Operations'*, Artech House (1998)

[1982] XQ Wang, YQ Sun, S Nanda, XF Wang, "Looking from the Mirror: Evaluating IoT Device Security through Mobile Companion Apps" *Usenix 2019*

[1983] XY Wang, DG Feng, XJ Lai, HB Yu, "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD", *IACR Cryptology ePrint Archive* Report 2004/199

[1984] XY Wang, YQL Yin, HB Yu, " Collision Search Attacks on SHA1", Feb 13 2005; refined to "Finding Collisions in the Full SHA-1", *Crypto 2005*

[1985] XY Wang, HB Yu, "How to Break MD5 and Other Hash Functions", in *Advances in Cryptology – Eurocrypt 2005*

[1986] R Want, A Hopper, V Falcao, J Gibbons, "The Active Badge Location System", in *ACM Transactions on Information Systems* v 10 no 1 (Jan 92) pp 91–102; at `http://www.cl.cam.ac.uk/research/dtg/attarchive/ab.html`

[1987] D Ward, "JTRS: A Cautionary Tale For Today", *Mitre Disrupting Acquisition Blog* Apr 1, 2020

[1988] R Ward, B Beyer, "BeyondCorp: A New Approach to Enterprise Security" *;login:* v 39 no 6 (2014) pp 6–11

[1989] WH Ware, "Security and Privacy in Computer Systems", *Spring Joint Computer Conference, 1967* pp 279–282, at `https://www.rand.org/pubs/papers/P3544.html`

[1990] WH Ware, *'Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security'*, Rand Report R609-1 (Feb 1970), at `https://www.rand.org/pubs/reports/R609-1.html`

[1991] M Warner, "Machine Politics In the Digital Age", in *The New York Times* November 9, 2003

[1992] SD Warren, LD Brandeis, "The Right To Privacy", Harvard Law Review series 4 (1890) pp 193–195

[1993] *'Waste Electrical and Electronic Equipment (WEEE) regulations*, UK Health and Safety Executive 2006, updated 2014, transposing Directive 2012/19/EU

[1994] S Waterman, "Analysis: Russia-Georgia cyberwar doubted", *Space War* Aug 18 2008

[1995] M Watson, "Sat-nav 'jammer' threatens to sink road pricing scheme", in *Auto Express* Aug 8th 2007

[1996] RNM Watson, "Exploiting Concurrency Vulnerabilities in Kernel System Call Wrappers", in *First USENIX Workshop on Offensive Technologies* (WOOT 07), at `http://www.watson.org/~robert/2007woot/`

[1997] RNM Watson, "A decade of OS access-control extensibility", *Communications of the ACM* v 56 no 2 (Feb 2013)

[1998] DJ Watts, *'Six Degrees – The Science of a Connected Age'*, Heinemann 2003

[1999] N Weaver, "Our Government Has Weaponized the Internet. Here's How They Did It", *Wired* Nov 13 2013

[2000] W Webb, "High-tech Security: The Eyes Have It", in *EDN* (18/12/97) pp 75–78

[2001] S Weckert, "Google Maps Hacks – Performance & Installation, 2020", `http://www.simonweckert.com/googlemapshacks.html`, Feb 2020

[2002] SH Weingart, "Physical Security for the μABYSS System", in *Proceedings of the 1987 IEEE Symposium on Security and Privacy*, pp 52–58

[2003] SH Weingart, "A Survey of Attacks and Defenses", *CHES* 2000

[2004] SH Weingart, "Mind the Gap: Updating FIPS 140", at *FIPS Physical Security Workshop*, Hawaii 2005

[2005] 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* IEEE (1990) pp 232–243

[2006] L Weinstein, "IDs in Color Copies—A PRIVACY Forum Special Report" in *Privacy Forum Digest*, v 8 no 18 (6 Dec 1999), at `http://www.vortex.com/privacy/priv.08.18`

[2007] L Weinstein, "The Online Medical Records Trap", *Lauren Weinstein's Blog* Oct 4 2007, at `http://lauren.vortex.com/archive/000306.html`

[2008] K Weise, N Singer, "Amazon Pauses Police Use of Its Facial Recognition Software", *New York Times* Jun 10 2020

[2009] M Weiss, M Weiss, "An assessment of threats to the US power grid", *Energy, Sustainability and Society* v 9 no 18 (2019)

[2010] 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

[2011] G Welchman, *'The Hut Six Story'*, McGraw Hill 1982

[2012] B Wels, R Gonggrijp, "Bumping locks", 2006, at `http://www.toool.nl/bumping.pdf`

[2013] A Welz, "Unnatural Surveillance: How Online Data Is Putting Species at Risk," *Yale Environment 360,* Sep 6 2017

[2014] J Werner, J Mason, M Antonakakis, M Polychronakis, F Monrose, "The SEVerESt Of Them All: Inference Attacks Against Secure Virtual Enclaves," *ACM Asia CCS* July 2019

[2015] *'Smart Metering – Obtaining and Using Consumption Data Relating to Domestic Premises – Data Privacy Plan*, Western Power Distribution, May 2018

[2016] A Westfeld, A Pfitzmann, "Attacks on Steganographic Systems", in *Information Hiding* (1999), Springer LNCS v 1768 pp 61–76

[2017] L Whateley, "Somebody stole £16,000 from my account but Barclays won't refund me", *The Times* Aug 20 2011; see also comments at `https://www.lightbluetouchpaper.org/2011/12/25/bankers-christmas-present/`

[2018] E Whitaker, "At SBC, It's All About 'Scale and Scope' ", in *Business Week* Nov 7 2005

[2019] G White, "The 20-Year Hunt for the Man Behind the Love Bug Virus", *Wired* Sep 12 2020

[2020] Z Whittaker, "Meet 'Muscular': NSA accused of tapping links between Yahoo, Google datacenters", *ZDnet* Oct 30 2013

[2021] Z Whittaker, "Hackers are stealing years of call records from hacked cell operators", *Techcrunch*, June 25 2019

[2022] A Whitten, JD Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0", in *Eighth USENIX Security Symposium* (1999) pp 169–183

[2023] Wikileaks, *'Vault 7: CIA Hacking Tools Revealed'*, Mar 7 2017

[2024] MV Wilkes, RM Needham, *'The Cambridge CAP computer and its Operating System'*, Elsevier North Holland 1979

[2025] 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

[2026] L Wilson, "Understanding the Appeal of ISIS", *New England Journal of Public Policy* v 29 no 1 (2017)

[2027] C Williams, "Surge in encrypted torrents blindsides record biz", in *The Register* Nov 8 2007, at `http://www.theregister.co.uk/2007/11/08/bittorrent_encryption_explosion/`

[2028] TA Williams, "Peaceful left-wing activist, 94, with no criminal record wins eight-year battle to wipe details of his 66 anti-war, poll tax and tuition fees protests from police 'extremism' database", *Daily Mail* Jan 24 2019

[2029] E Williamson, AJ Walker, KJ Bhaskaran, S Bacon, Chris Bates, CE Morton, HJ Curtis, A Mehrkar, D Evans, P Inglesby, J Cockburn, HI Mcdonald, B MacKenna, L Tomlinson, IJ Douglas, CT Rentsch, R Mathur, A Wong, R Grieve, D Harrison, H Forbes, A Schultze, RT Croker, J Parry, F Hester, S Harper, R Perera, S Evans, L Smeeth, B Goldacre, "OpenSAFELY: factors associated with COVID-19-related hospital death in the linked electronic health records of 17 million adult NHS patients" *medRxiv* `https://doi.org/10.1101/2020.05.06.20092999` May 7 2020

[2030] B Wilson, J Hoffman, J Morgenstern, "Predictive Inequity in Object Detection", *arXiv 1902.11097* Feb 21 2019

[2031] CL Wilson, MD Garris and CI Watson, "Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints", NIST IR 7110 (May 2004)

[2032] H Wimmer, J Perner, "Beliefs about beliefs: representation and constraining function of wrong beliefs in young children's understanding of deception", *Cognition* v 13 no 1 (1983) pp 103–28

[2033] D Winder, "How To Make $1 Million From Hacking: Meet Six Hacker Millionaires", *Forbes*, Aug 29 2019

[2034] FW Winterbotham, *'The Ultra Secret'*, Harper & Row 1974

[2035] P Woit, *'Not Even Wrong: The Failure of String Theory and the Continuing Challenge to Unify the Laws of Physics'*, Vintage 2007

[2036] A Wolfson, "A hoax most cruel", in *The Courier-Journal* Oct 9, 2005

[2037] K Wong, "Mobile Phone Fraud – Are GSM Networks Secure?", in *Computer Fraud and Security Bulletin* (Nov 96) pp 11–18

[2038] N Wong, "Judge tells DoJ 'No' on search queries", Google blog Mar 17 2006

[2039] E Wood, *'Housing Design, A Social Theory'*, Citizens' Housing and Planning Council of New York, 1961

[2040] L Wood, "Global Biometric System Market Report 2019: Size is Expected to Grow from USD 33.0 Billion in 2019 to USD 65.3 Billion by 2024", *BusinessWire* Nov 7 2019

[2041] Z Wood, "Dixons Carphone fined £500,000 for massive data breach", *The Guardian* Jan 9 2020

[2042] 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)

[2043] "Automated teller machines (ATMs) (per 100,000 adults)", *World Bank*, `https://data.worldbank.org/indicator/FB.ATM.TOTL.P5`

[2044] B Wright, "The Verdict on Plaintext Signatures: They're Legal", in *Computer Law and Security Report* v 14 no 6 (Nov/Dec 94) pp 311–312

[2045] B Wright, *'The Law of Electronic Commerce: EDI, Fax and Email'*, Little, Brown 1994

[2046] DB Wright, AT McDaid, "Comparing system and estimator variables using data from real line-ups", in *Applied Cognitive Psychology* v 10 no 1 pp 75–84

[2047] JB Wright, *'Report of the Weaponization and Weapons Production and Military Use Working Group –Appendix F to the Report of the Fundamental Classification Policy Review Group'*, US Department of Energy Office of Scientific and Technical Information 1997

[2048] MA Wright, "Security Controls in ATM Systems", in *Computer Fraud and Security Bulletin*, November 1991, pp 11–14

[2049] P Wright, *'Spycatcher – The Candid Autobiography of a Senior Intelligence Officer'*, William Heinemann Australia, 1987

[2050] L Wouters, J Van den Herreweghen, FD Garcia, D Oswald, B Gierlichs, B Preneel, "Dismantling DST-80 Based Immobiliser Systems", *IACR Transactions on Cryptographic Hardware and Embedded Systems* v 2 (2020) pp 99–127

[2051] T Wu, *'The Master Switch: The Rise and Fall of Information Empires'*, Knopf 2010

[2052] T Wu, *'The Attention Merchants: The Epic Scramble to Get Inside Our Heads'*, Penguin Random House 2016

[2053] T Wu, *'The Curse of Bigness'*, Atlantic 2018

[2054] R Wyden, *Letter to John Ratcliffe*, June 16 2020; linked from S Nicholls, "If you're despairing at staff sharing admin passwords, look on the bright side. That's CIA-grade security", *The Register* June 16 2020

[2055] C Wylie, *'Mindf*ck'*, Profile Books 2019

[2056] K Xiao, D Forte, Y Jin, R Karri, S Bhunia, M Tehranipoor, "Hardware Trojans: Lessons Learned after One Decade of Research", *ACM Transactions on Design Automation of Electronic Systems* v 22 no 1 (May 2016)

[2057] JX Yan, *'Security for Online Games'*, PhD thesis, University of Cambridge 2003

[2058] 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; also in *IEEE Security & Privacy*, Sep–Oct 2004 pp 25–29

[2059] JX Yan, B Randell, *'Security in Computer Games: from Pong to Online Poker'*, University of Newcastle Tech Report CS-TR-889 (2005)

[2060] JX Yan, B Randell, "A systematic classification of cheating in online games", at *Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games* (2005)

[2061] T Ylönen, "SSH – Secure Login Connections over the Internet", in *Usenix Security 96* pp 37–42

[2062] G Yuval, "Reinventing the Travois: Encryption/MAC in 30 ROM Bytes", in *Fast Software Encryption* (1997), Springer LNCS v 1267 pp 205–209

[2063] R Zarnekow, W Brenner, "Distribution of cost over the application lifecycle – A multi-case study", *European Conference on Information Systems (ECIS)*, (2005)

[2064] *ZDnet*, “Software blocks images of money”, Jan 12 2004

[2065] S van der Zee, R Clayton, RJ Anderson, “The gift of the gab: Are rental scammers skilled at the art of persuasion?” *arXiv:1911.08253* Nov 19 2019

[2066] S van der Zee, R Poppe, PJ Taylor, RJ Anderson, “To freeze or not to freeze: A culture-sensitive motion capture approach to detecting deceit”, *PLOS One* April 12 2019

[2067] K Zetter, “From the Eye of a Legal Storm, Murdoch’s Satellite-TV Hacker Tells All”, in *Wired*, May 30 2008

[2068] K Zetter, “Report: NSA Exploited Heartbleed to Siphon Passwords for Two Years”, in *Wired*, Apr 11 2014

[2069] K Zetter, “Hacker Can Send Fatal Dose to Hospital Drug Pumps”, in *Wired*, Jun 8 2015

[2070] K Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”, in *Wired*, Mar 3 2016

[2071] K Zetter, “Researchers Uncover New Version of the Infamous Flame Malware”, in *Wired*, Apr 9 2019

[2072] RS Zhang, XY Wang, XH Yan, XX Jiang, “Billing Attacks on SIP-Based VOIP Systems”, in *WOOT 2007*

[2073] YQ Zhang, F Monrose, M Reiter, “The security of modern password expiration: An algorithmic framework and empirical analysis”, *ACM CCS* (2010)

[2074] YR Zhao, I Shumailov, H Cui, XT Gao, R Mullins, R Anderson, “Blackbox Attacks on Reinforcement Learning Agents Using Approximated Temporal Information”, *DSN-DSML* 2020; also *arXiv:1909.02918* (2019)

[2075] L Zhuang, F Zhou, JD Tygar, “Keyboard Acoustic Emanations Revisited” in *12th ACM CCS* (2005)

[2076] P Zimbardo, *‘The Lucifer Effect’*, Random House 2007

[2077] Ellie Zolfagharifard, “How poachers use INSTAGRAM to find their prey: Geo-tagged photos help hunters track and kill tigers and rhinos,” *Daily Mail* 8 May 2014

[2078] S Zuboff, *‘The Age of Surveillance Capitalism – The fight for a human future at the new frontier of power’*, Profile Books 2019

[2079] 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

Index