Bibliography


[34] J Alfke, “Facebook and Decentralized Identifiers”, in Thought Palace Dec 2 2007


Security Engineering 894 Ross Anderson
BIBLIOGRAPHY


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


Security Engineering 895 Ross Anderson


Security Engineering 897

Ross Anderson


Security Engineering 898 Ross Anderson


[120] 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/


[124] I Arghire, “Hardware-based Password Managers Store Credentials in Plain-text” Security Week Dec 9 2019

[125] Arm Inc., ‘Cache Speculation Side-channels’ v 2.4, Oct 2018


[133] 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/2008027220904/http://smallwarsjournal.com/blog/2007/09/print/weapon-of-choice/

Security Engineering 899 Ross Anderson

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


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


[166] 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


[168] B Barrow, B Quinn, “Millions in danger from chip and pin fraudsters” in Daily Mail June 5th 2006


[197] 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


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


Security Engineering 904 Ross Anderson


[237] 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


[249] 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


BIBLIOGRAPHY


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


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


[286] E Bovenlander, invited talk on smartcard security, Eurocrypt 97, reported in [102]


[288] O Bowcott, “UK-US surveillance regime was unlawful ‘for seven years’ ” The Guardian Feb 6 2015


[293] M Brader, “How to lose 10,000,000 pounds”, in comp.risks v 24 no 25, Apr 19 2006


[296] L Brandimarte, A Acquisti, G Loewenstein, “Misplaced Confidences: Privacy and the Control Paradox”, WEIS 2010
[297] R Brandom, “Your phone’s biggest vulnerability is your fingerprint”, The Verge May 2, 2016


[300] H Bray, “'Face testing' at Logan is found lacking”, in Boston Globe July 17 2002

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


[309] J Brodkin, “FCC requires anti-robocall tech after Â‘AIJvoluntaryÂ‘ÂI plan didn’t work out”, Ars Technica Apr 1 2020


[317] 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


[329] M Burgess, “North Korea’s elite hackers are funding nukes with crypto raids”, Wired Apr 3 2019


[332] T Burt, “New action to disrupt world’s largest online criminal network”, Microsoft on the issues, Mar 10 2020

[333] 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

[334] 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


[340] G Burton “Equifax used default ’admin’ user name and password to secure hacked portal”, Computing Oct 21 2019


[344] ‘A Comparative Introduction to 4G and 5G Authentication’, Cable Labs, Winter 2019

[345] C Cadwalladr, “Facebook’s role in brexit – and the threat to democracy”, TED2019


[358] D Campbell, “Operation Ore Exposed”, *PC Pro*, Jul 2005, archived at [https://www.duncancampbell.org/content/operation-ore](https://www.duncancampbell.org/content/operation-ore)


[367] “German A555 takes its toll”, in Card World International (12/94-1/95) p 6

[368] 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

[369] “High tech helps card fraud decline” in Cards International no 117 (29 Sep 94)

[370] “Visa beefs up its anti-fraud technology”, in Cards International no 189 (12/12/97) p 5


[379] E Cebuc, “How are we doing with Android’s overlay attacks in 2020?”, F-secure Labs Mar 27 2020


[381] L Cerulus, “EU Commission to staff: Switch to Signal messaging app”, Politico Pro Feb 20 2020


[395] 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*


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


[399] K Chiu, “The world’s biggest online population is staying home and China’s internet can’t cope”, *Abacus News* Feb 17 2020

[400] “‘Trial by Internet’ Casts Spotlight on Korean Cyber Mobs” *Chosun Ilbo* July 8 2005


[402] 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

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


[408] C Cimpanu, “Newer Diameter Telephony Protocol Just As Vulnerable As SS7”, Bleeping Computer July 2 2018

[409] C Cimpanu, “Backdoor found in Ruby library for checking for strong passwords”, ZDNet July 8 2019

[410] C Cimpanu, “DNS-over-HTTPS causes more problems than it solves, experts say”, ZDNet Oct 6 2019

[411] C Cimpanu, “Major vulnerability patched in the EU’s eIDAS authentication system”, ZDNet Oct 29 2019

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

[413] C Cimpanu, “Android malware can steal Google Authenticator 2FA codes”, ZDNet Feb 27 2020

[414] J Cipriani, “iOS 13: Top 5 new security and privacy features for your iPhone”, CNet Sep 22 2019


Security Engineering 915 Ross Anderson


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


*Security Engineering* 916 Ross Anderson

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


[447] E Constable, “American Express to reduce the risk of online fraud”


[450] D Coppersmith, ‘The Data Encryption Standard (DES) and its Strength Against Attacks’, IBM report RC 18613 (81421)


[455] S Cordier, “Bracelet électronique, ordonnance de protection, TGD... Ce que contient la loi sur les violences conjugales”, Le Monde Dec 18 2019


[458] J Cox, “Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years” Motherboard Feb 6 2019


[461] J Cox, “Criminals Are Tapping into the Phone Network Backbone to Empty Bank Accounts”, Vice Jan 31 2019

[462] J Cox, “Hackers Are Breaking Directly Into Telecom Companies to Take Over Customer Phone Numbers”, Vice Jan 10 2020


[468] L Cranor, “Time to rethink mandatory password changes”, Tech@FTC blog Mar 2 2016


[483] G Danezis, “Distributed Ledgers: what is so interesting about them?” Conspicuous Chatter Sep 27 2018


[490] Two statements, made by the Data Protection Commissioners of EU and EE5 countries and Switzerland, 20th International Conference on Data Protection, Santiago de Compostela, 16-18 September 1998


BIBLIOGRAPHY


[500] D Deahl, “This 10-year-old was able to unlock his mom’s iPhone using Face ID”, *The Verge* Nov 14 2017


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


Security Engineering 920 Ross Anderson


[524] 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

[525] 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

[526] Department of Justice, “Ohio Resident Charged with Operating Darknet-Based Bitcoin ‘Mixer,’ which Laundered Over $300 Million” Feb 13 2020


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


[534] R Dingledine, “Tor security advisory: "relay early" traffic confirmation attack”, Tor Blog, July 30 2014


[537] ‘The Annual Bullying Survey 2018’, Ditch the Label


[542] C Doctorow, “SAMBA versus SMB: Adversarial interoperability is judo for network effects”, Boing Boing July 17 2019


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


[548] 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


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


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

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


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

[573] 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

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

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

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


[581] 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


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


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


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


[611] 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


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

[618] 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


[620] R Evans, “Trade unionist was refused job after police gave details to blacklist” The Guardian Mar 7 2019


[622] C Farivar, “Russian man pleads guilty, admits he ran notorious Kelihos botnet” Ars Technica Sep 13 2018

Security Engineering 926 Ross Anderson
[623] 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


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


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

[645] “FCA fines RBS, NatWest and Ulster Bank Ltd £42 million for IT failures”, Financial Conduct Authority, Nov 20 2014

[646] “Final Notice, Tesco Personal Finance plc, Reference Number 186022”, Financial Conduct Authority, Oct 1 2018


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


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


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


*Security Engineering* 929 Ross Anderson
BIBLIOGRAPHY

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

[676] “Chip cards reduce fraud in France”, in *Fraud Watch* (1996) no 1 p 8

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

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


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


Security Engineering 930 Ross Anderson
[693] R Gallagher, “How U.K. Spies Hacked a European Ally and Got Away With It” The Intercept Feb 17 2018


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


Security Engineering 931 Ross Anderson
BIBLIOGRAPHY


[717] J Germain, “And we return to Munich’s migration back to Windows â€” it’s going to cost what now?! €100m!!” The Register Jan 4 2018


Security Engineering 932 Ross Anderson
BIBLIOGRAPHY


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

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


[745] D Goodin, “TJX agrees to pay banks $41m to cover Visa losses”, in The Channel Register, Dec 3 2007


[748] D Goodin, “How 3ve’s BGP hijackers eluded the Internet—and made $29M”, Ars Technica Dec 21 2018

Security Engineering 933 Ross Anderson
[749] D Goodin, “Developer of Checkm8 explains why iDevice jailbreak exploit is a game changer”, Ars Technica Sep 28 2019

[750] D Goodin, “Five months after returning rental car, man still has remote control”, Ars Technica, Oct 28 2019


[752] D Goodin, “Google Play app with 100 million downloads executed secret payloads”, Ars Technica Aug 27 2019

[753] D Goodin, “Kingpin of Evil Corp lived large. Now there’s a $5 million bounty on his head”, Ars Technica Dec 5 2019

[754] D Goodin, “What the newly released Checkra1n jailbreak means for iDevice security”, Ars Technica Nov 15 2019


[769] A Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History”, Wired Aug 22 2018


[780] H Griffiths, “Car crime rises again with 113,000 vehicles stolen last year”, Auto Express Apr 25 2019

[781] 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


[784] P Grother, M Ngan, K Hanaoka, ‘Face Recognition Vendor Test (FRVT)’ NIST IR 2871, Sep 11 2019


[798] P Gutmann, “Invalid banking cert spooks only one user in 300”, Cryptography List May 16 2005; at http://www.mail-archive.com/cryptography%40metzdowd.com/msg03852.html


[805] 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


[809] JA Halderman, N Heninger, “How is NSA breaking so much crypto?” Oct 14 2015, Freedom to Tinker


[818] R Hanson, “Can wiretaps remain cost-effective?”, in Communications of the ACM v 37 no 12 (Dec 94) pp 13–15


[824] D Harz, “Stealing All of Maker’s Collateral”, Medium Feb 20 2020


[827] Health and Human Services, ‘Standards for Privacy of Individually Identifiable Health Information’, HHS 45 CFR parts 160â§164, 65 Federal Register at 82461â§82510; see also 82,777–82,779


Security Engineering 938

Ross Anderson


[841] Herodotus, 'Histories'; Book 1 123.4, Book 5 35.3 and Book 7 239.3


Security Engineering 939 Ross Anderson


[860] I Hodson, “DeepMind and Google: the battle to control artificial intelligence”, The Economist 1848 April/May 2019


[867] C Holloway, “Controlling the Use of Cryptographic Keys”, in Computers and Security v 14 no 7 (95) pp 587–598


[869] BD Hong, SW Bae, YD Kim, “GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier” NDSS 2018


Security Engineering 940  Ross Anderson


[879] 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


[891] “Role of Communications in Operation Desert Storm”, in IEEE Communications Magazine (Special Issue) v 30 no 1 (Jan 92)


[893] “Pink Death Strikes at US West Cellular”, in Information Security Monitor v 9 no 2 (Jan 94) pp 1–2


[905] Information Commissioner’s Office, ‘Investigation into the use of data analytics in political campaigns’, July 11 2018

[906] Information Commissioner’s Office, ‘Mobile phone data extraction by police forces in England and Wales’, June 2020


[914] I Jackson, personal communication


[916] B Jacobs, “Maximator: European signals intelligence cooperation, from a Dutch perspective”, Journal of Intelligence and National Security Apr 7 2020


[929] R Jenkins, “Hole-in-wall thief used MP3 player”, in The Times Nov 15 2006; at http://www.timesonline.co.uk/article/0,,29389-2455890,00.html


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


[949] L Kahn, “The FBI Wanted a Backdoor to the iPhone. Tim Cook Said No”, Wired Apr 16 2019


Security Engineering 946 Ross Anderson


[990] YG Kim, R Daly, Jeremie Kim, C Fallin, JH Lee, DH Lee, C Wilkerson, K Lai O Muthu, “Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors”, *ISCA 2014*

[991] T Kinder, “Regulator outlines plans to break up Big Four accounting firms”, *Financial Times* Feb 27 2020

[992] T Kinder, “Big Four told to outline plans for audit split by October”, *Financial Times* Jul 6 2020

[993] T Kinder, D McCrum, “EY fights fires on three audit cases that threaten its global reputation”, *Financial Times* Jun 8 2020


Security Engineering 947 Ross Anderson


[1024] K Korosec, “VW fires jailed Audi CEO Rupert Stadler” Techcrunch Oct 2 2018


[1026] 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


[1037] HM Kriz, “Phreaking recognised by Directorate General of France Telecom”, in Chaos Digest 1.03 (Jan 93)


Security Engineering 949 Ross Anderson


[1048] D Kundaliya, “‘Android devices are being increasingly targeted by undeletable adware, researchers warn’, *Computing* July 7 2020

[1049] L Kuo, “Chinese surveillance company tracking 2.5m Xinjiang residents”, in *The Guardian* Feb 18 2019


[1054] ‘L0phtCrack 2.52 for Win95/NT’, at http://www.l0pht.com/10phtcrack/


[1058] L Lamont, “And the real Lotto winner is ... that man at the cash register”, *Sydney Morning Herald*, May 3 2007


Security Engineering 950 Ross Anderson
BIBLIOGRAPHY

[1060] L Lamport, Email message sent to a DEC SRC bulletin board at 12:23:29 PDT on 28 May 1987. Link No. 75.


[1076] D Leloup, M Untersinger, “Comment les services de renseignement font la chasse aux employés des télécoms”, Le Monde Dec 8 2016


[1082] 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


[1096] J Leyden, “Feds told they need warrants for webmail”, in The Register
June 19 2007; at http://www.theregister.co.uk/2007/06/19/webmail_ 
wiretaps_appeal/

[1097] J Leyden, “MySpace phishing scam targets music fans”, in The Register, 
Oct 14 2006; at http://www.theregister.co.uk/2006/10/14/myspace_ 
phishing.scam/

[1098] 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

Current Evidence from CCTV-Captured Public Conflicts”, Discover Society 
June 5 2019

Over Information and Cyber Operations”, Lawfare Blog Mar 27 2020

AFIPS (1975) pp 361–368

[1102] David Lindemayer, Ben Scheele “Do Not Publish”, Science Magazine v 
356 no 6340 (May 26 2017) pp 800–801

[1103] JPMG Linnartz, “The ‘Ticket’ Concept for Copy Control Based on Embed- 
ded Signalling”, ESORICS 98, Springer LNCS 1485 pp 257–274

[1104] JPMG Linnartz, M van Dijk, “Analysis of the Sensitivity Attack Against 
Electronic Watermarks in Images”, in [135] pp 258–272

bluetooth.com

[1106] S Liao “Spyware app abused iOS enterprise certificate to track targets” The 
Verge, Apr 8 2019

[1107] SB Lipner, “The Birth and Death of the Orange Book”, Annals of the 

[1108] M Lipp, M Schwarz, D Gruss, T Prescher, W Haas, S Mangard, P Kocher, 
2018

[1109] A Liptak, “Hackers reportedly used a tool developed by the NSA to attack 
Baltimore’s computer systems”, The Verge May 25 2019

[1110] D Litchfield, C Anley, J Heasman, B Grindlay, ‘The Database Hacker’s 

[1111] B Littlewood, “Predicting software reliability”, in Philosophical 

[1112] 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

[1113] XY Liu, Z Zhou, WR Diao, Z Li, KH Zhang, “When good becomes evil: 
Keystroke inference with smartwatch, ACM CCS 2015 pp 1273–1285

Security Engineering 953 Ross Anderson


[1117] N Lomas, “Targeted ads offer little extra value for online publishers, study suggests”, Techcrunch May 31 2019


[1132] 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


[1144] F Main, “Your phone records are for sale”, Chicago Sun-Times, Jan 5 2006


Security Engineering

955

Ross Anderson
BIBLIOGRAPHY


BIBLIOGRAPHY


[1171] S Matala, T Nyman, N Asokan, “Historical insight into the development of Mobile TEEs ”, Aalto University Secure Systems Group blog, June 20 2019


[1181] V Mavroudis, P Svenda, “JavaCard: The execution environment you didn’t know you were using”, Software Sustainability Institute July 13 2018


[1185] 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


[1196] E McGaughey, “The extent of Russian-backed fraud means the referendum is invalid”, LSE Nov 14 2018


Security Engineering 958 Ross Anderson
BIBLIOGRAPHY


[1205] D McLeod, “FNB backs down on password decision after backlash”, *Tech Central* Aug 20 2019


Security Engineering 959 Ross Anderson


[1225] M Mesa, “Phish Scales: Malicious Actor Combines Personalized Email, Variety of Malware To Target Exces”, ProofPoint Apr 5 2016


[1243] 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


[1249] “BBC fined £400,000 by Ofcom for fake competitions”, Daily Mirror July 30 2008


[1257] “Card fraud nets Esc6 billion’, F Mollet, Cards International (22/9/95) p 3

Security Engineering 961 Ross Anderson


[1271] R Morris, Invited talk, Crypto 95


BIBLIOGRAPHY


National Audit Office, ‘Rolling out smart meters’, Nov 23 2018

National Audit Office, ‘Investigation into Verify’, Mar 5 2019


National Institute of Standards and Technology, ‘Data Encryption Standard (DES)’ FIPS 46-3, Nov 1999 incorporating upgrade to triple DES


National Institute of Standards and Technology, ‘Digital Signature Standard (DSS)’, FIPS 186-3, draft, Mar 2006


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

Security Engineering 965 Ross Anderson


[1340] J Naughton, “Facebook’s Vassal State”, in Memex 1.1 March 5, 2019


[1346] RM Needham, “Naming”, in [1280], pp 318–127


Security Engineering 966 Ross Anderson


[1361] C Newton, “The Trauma Floor”, *The Verge*, Feb 25, 2019

[1362] C Newton, “Mark Zuckerberg says Facebook will shift to emphasize encrypted ephemeral messages”, *The Verge*, Mar 6 2019

[1363] J Newton, “Countering the counterfeiters”, in *Cards International* (21/12/94) p 12


[1366] Andrew Ng, “How the Equifax hack happened, and what still needs to be done”, *Cnet* Sep 7 2018


[1368] 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

Security Engineering 967 Ross Anderson


[1376] ‘White Paper – 5g Evolution and 6g’, NTT Docomo, January 2020


BIBLIOGRAPHY


[1388] “Nicht nachmachen: Dieser Vignetten-Trick kostet Sie 300 Euro”, Online Focus, June 12 2015


[1393] A Orben, T Dienlin, AK Przybylski, “Social media’s enduring effect on adolescent life satisfaction”, PNAS April 16 2019


[1395] A Orlowski, “UK spy agency warns Brit telcos to flee from ZTE gear”, The Register April 16 2018


[1399] B Osborn, J McWilliams, B Beyer, M Saltonstall, “BeyondCorp – Design to Deployment at Google”, ;login: (Spring 2016) v 41 no 1

[1400] C Osborne, “University of California SF pays ransomware hackers $1.14 million to salvage research”, ZDNet, Jun 30 2020


[1416] J Pastor,”CRYPTOPOST – A cryptographic application to mail processing”, in Journal of Cryptology v 3 no 2 (Jan 1991) pp 137–146


Security Engineering 970  Ross Anderson


[1427] PeckShield, “bZx Hack Full Disclosure (With Detailed Profit Analysis)”, Medium Feb 17 2020


[1443] 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


[1446] L Pinault, *‘Consulting Demons’*, Collins 2000


[1449] RA Poisel, *‘Modern Communications Jamming Principles and Techniques’*, Artech House 2003

[1450] Politech mailing list, was at http://www.politechbot.com/


[1453] R Porter, “Google fined €50 million for GDPR violation in France” *The Verge* Jan 21 2019


[1457] F Postma, “Military And Intelligence Personnel Can Be Tracked With The Untappd Beer App”, *Bellingcat* May 18, 2020


[1459] S Poulter, “Phone firm’s whistleblower says his life has been made a misery”, in *The Daily Mail* Jun 21 2007


Security Engineering 972 Ross Anderson

[1463] 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


Security Engineering 973 Ross Anderson

[1482] Z Quinn, ‘Crash Override’, Hachette 2017


[1488] R Ramesh, “Online tool could be used to identify public figures’ medical care, say critics” The Guardian Mar 17 2014


BIBLIOGRAPHY


[1512] M Reynolds, “The strange story of Section 230, the obscure law that created our flawed, broken internet”, Wired Mar 24 2019


Security Engineering 975 Ross Anderson


[1522] J Rogers, “FAKE FIVER: Shopper’s warning after being handed this fake £5 note nudge; but is it counterfeit?”, The Sun May 13 2018

[1523] 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


[1526] K Rooney, “Majority of bitcoin trading is a hoax, new study finds” CNBC Mar 22 2019


[1533] “Card fraud plummets in France”, M Rowe, Banking Technology (May 94) p 10

[1534] 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


[1543] B Russell, Answer to parliamentary question, Hansard 10 Jun 2003 column 762W


[1554] I Sample, “NHS patient records to revolutionise medical research in Britain” The Guardian Aug 28 2012

[1555] P Samuelson, “Copyright and digital libraries”, in Communications of the ACM v 38 no 4, April 1995


[1603] E Selleck, “Apple’s App Store is Populated With Gambling and Other Apps That Abuse Enterprise Certificates”, iPhone Hacks, Feb 12 2019


[1639] N Silvester, “Doctor who hacked into Prime Minister’s health records escapes prosecution”, *Daily Record* Jan 10 2012

[1640] 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*

[1641] Luther Simjian – Inventor of the Week, at [https://lemelson.mit.edu/resources/luther-george-simjian](https://lemelson.mit.edu/resources/luther-george-simjian)

[1642] D Simmons, “BBC fools HSBC voice recognition security system”, *BBC* May 19 2017


[1645] 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 [1646])


[1650] GJ Simmons, ‘Subliminal Channels; Past and Present’, European Transactions on Telecommunications v 5 no 4 (Jul/Aug 94) pp 459–473


[1656] 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


[1672] SP Skorobogatov, “Flash Memory ‘Bumping’ Attacks”, CHES 2010


[1675] SP Skorobogatov, “The bumpy road towards iPhone 5c NAND mirroring”, arXiv:1609.04327, Sep 14 2016; and see project page at https://www.cl.cam.ac.uk/~sps32/5c_proj.html


[1681] SP Skorobogatov, C Woods. “In the blink of an eye: There goes your AES key” IACR Preprint 2012/296


[1687] A Smith, “New fake £20 notes ‘trick shop assistants then peel off within a week’”, Metro Nov 15 2018


[1693] T Snyder, ‘The Road to Unfreedom’, Bodley Head 2018


Security Engineering 985

Ross Anderson


[1703] E Spafford, “The Internet worm program: an analysis”, in Computer Communications Review v 19 no 1 (Jan 89) pp 17–57


[1720] S Staniford, D Moore, V Paxson, N Weaver, “The Top Speed of Flash Worms”, in WORM04


[1722] N Statt, “Fortnite for Android will ditch Google Play Store for Epic’s website”, The Verge Aug 3 2018


[1724] P Stein, P Feaver, ‘Assuring Control of Nuclear Weapons’, CSIA occasional paper number 2, Harvard University 1987


[1733] J van der Straaten, “So You Think Digital is the Future? Your Internet Data is Rotting”, Researchgate May 2019


Security Engineering 987  Ross Anderson


[1741] Suetonius (Gaius Suetonius Tranquillus), ‘Vitae XII Caesarum’, translated into English as ‘History of twelve Caesars’ by Philemon Holland, 1606; Nutt (1899)


[1759] C Tavris, E Aronson, ‘Mistakes were made – but not by me’, Harcourt 2007
[1763] J Temperton, “Inside Sellafield: how the UK’s most dangerous nuclear site is cleaning up its act”, Wired, 17 September 2016
[1764] S Tendler, N Nuttall, “Hackers run up £1m bill on Yard’s phones”, in The Times, 5 Aug 1996
BIBLIOGRAPHY


[1779] I Thomson, “Talk about unintended consequences: GDPR is an identity thief’s dream ticket to Europeans’ data”, in The Register Aug 9 2019


[1784] 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/


Security Engineering 990 Ross Anderson

[1793] A Travis, “Man who escaped mosque in burqa was under counter-terror restrictions”, in The Guardian Nov 5 2013


[1801] 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

[1802] D Uberti, “Facebook Went to War Against White Supremacist Terror After Christchurch. Will It Work?” Vice Oct 3 2019

[1803] R Uhlig, “BT admits sta↵ could have fiddled system to win Concorde trip”, in The Daily Telegraph (23/7/1997)


Security Engineering 991 Ross Anderson
[1809] UPI newswire item, Oklahoma distribution, November 26, 1983, Tulsa, Oklahoma


[1814] 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


[1816] S Osborne, “How did Tesla make some of its cars travel further during Hurricane Irma?”, The Guardian Sep 11 2017

[1817] S Vaidhyanathan, “Facebook’s new move isn’t about privacy. It’s about domination”, The Guardian March 7 2019

[1818] J Valenti, “Anita Sarkeesian interview: ’The word ”troll” feels too childish. This is abuse’ “, The Guardian Aug 29 2015


[1820] L van Hove, “Electronic Purses: (Which) Way to Go?”, in First Monday v 5 no 7 (June 2000)


[1823] 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


Security Engineering 992 Ross Anderson


[1833] H Varian, Keynote address to the Third Digital Rights Management Conference, Berlin, Germany, January 13, 2005


[1835] 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


[1850] 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


[1852] L von Ahn, personal communication, 2006


Security Engineering 994 Ross Anderson


[1879] M Weaver, “Developer tortured by raiders with crowbars”, Daily Telegraph, 31 October 97

[1880] N Weaver, “Our Government Has Weaponized the Internet. Here’s How They Did It”, Wired Nov 13 2013


[1898] E Whitaker, “At SBC, It’s All About ‘Scale and Scope’ ”, in Business Week Nov 7 2005

Security Engineering 996 Ross Anderson


[1901] Z Whittaker, “Hackers are stealing years of call records from hacked cell operators”, Techcrunch, June 25 2019


[1909] 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


[1914] D Winder, “How To Make $1 Million From Hacking: Meet Six Hacker Millionaires”, Forbes, Aug 29 2019

Security Engineering 997 Ross Anderson


[1927] 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


