Bibliography


[35] M Alagappan, JV Rajendran, M Doroslovački, G Venkataramani, “DFS Covert Channels on Multi-Core Platforms”, Visisoc 2017


Security Engineering 955 Ross Anderson


Security Engineering 956 Ross Anderson


Security Engineering 957 Ross Anderson


[123] 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


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

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


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


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


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


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


[194] BBC News Online, “Citizenship Amendment Bill: India’s new ‘anti-Muslim’ law explained”, Dec 11 2019


Security Engineering 964 Ross Anderson


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


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


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


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


[302] E Bovenlander, invited talk on smartcard security, Eurocrypt 97, reported in [107]


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


[313] R Brandom, “Your phone’s biggest vulnerability is your fingerprint”, The Verge May 2, 2016


[315] 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

[316] H Bray, “ ‘Face testing’ at Logan is found lacking”, in *Boston Globe* July 17 2002
[317] M Brelis, “Patients’ files allegedly used for obscene calls”, in *Boston Globe* April 11, 1995; also in *comp.risks* v 17 no 7


[326] J Brodkin, “FCC requires anti-robocall tech after ‘voluntary’ plan didn’t work out”, *Ars Technica* Apr 1 2020


[334] RT Buchanan, “Stag party member claims he was â€˜grossly exploitedâ€™ by lap dancing club Spearmint Rhino after spending third of his salary in single evening”, *The Independent* Nov 11 2014


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


Security Engineering 971 Ross Anderson
[349] T Burt, “New action to disrupt world’s largest online criminal network”, Microsoft on the issues, Mar 10 2020

[350] 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

[351] 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


[354] L Butler, “Post Office boss receives 7% pay rise as postmaster salaries cut”, The Guardian Oct 19 2018


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


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


Security Engineering 972 Ross Anderson


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

[385] 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

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

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


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


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


[404] P Chain, F Filloux, “Code, on wheels: Reinventing the car, episode 5” Mondaynote, Aug 9 2020


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


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


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

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


[420] 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

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


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

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

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

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

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

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


[433] C Cimpanu, “China is now blocking all encrypted HTTPS traffic that uses TLS 1.3 and ESNI”, ZDNet Aug 8 2020

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


[437] P Clark, H Warrell, T Bradshaw, S Neville “The rise and fall of Hancock’s homegrown tracing app”, Financial Times Jun 26 2020


[444] R Clayton, private conversation, 2006

Security Engineering 976 Ross Anderson
[455] A Collins, “Court decides software time-locks are illegal”, in Computer Weekly (19 August 93) p 1
[457] D Coldewey, “Uber in fatal crash detected pedestrian but had emergency braking disabled”, TechCrunch May 24 2018
[460] “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

Security Engineering 977 Ross Anderson


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


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


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


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


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


BIBLIOGRAPHY

[482] G Corfield, “I helped catch Silk Road boss Ross Ulbricht: Undercover agent tells all” The Register Jan 29 2019


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

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


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


Security Engineering 979 Ross Anderson
BIBLIOGRAPHY

[500] H Crouch, “Two NHS trusts sign agreements with Sensyne Health”, DigitalHealth Feb 4 2019
[509] G Danezis, “Distributed Ledgers: what is so interesting about them?” Conspicuous Chatter Sep 27 2018
[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

Security Engineering 980 Ross Anderson


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


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


[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


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


[561] R Dingleline, “Tor security advisory: ”relay early” traffic confirmation attack”, Tor Blog, July 30 2014


[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


[574] 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

Security Engineering 983 Ross Anderson


[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


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


[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


BIBLIOGRAPHY


[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


[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


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


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


[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


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

[655] 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


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


[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


Security Engineering 989  Ross Anderson


[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


[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


Security Engineering 990 Ross Anderson
BIBLIOGRAPHY


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


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


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


Security Engineering 991 Ross Anderson
[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
[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

Security Engineering 992 Ross Anderson
[735] R Gallagher, “How U.K. Spies Hacked a European Ally and Got Away With It” The Intercept Feb 17 2018


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


Security Engineering 993 Ross Anderson


[759] 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


Security Engineering 994 Ross Anderson


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


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


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

[792] D Goodin, “Police decrypt 258,000 messages after breaking pricey IronChat crypto app”, Ars Technica, Jul 11 2018
[793] D Goodin, “Developer of Checkm8 explains why iDevice jailbreak exploit is a game changer”, Ars Technica Sep 28 2019
[794] D Goodin, “Five months after returning rental car, man still has remote control”, Ars Technica, Oct 28 2019
[796] D Goodin, “Google Play app with 100 million downloads executed secret payloads”, Ars Technica Aug 27 2019
[797] D Goodin, “Kingpin of Evil Corp lived large. Now there’s a $5 million bounty on his head”, Ars Technica Dec 5 2019
[798] D Goodin, “What the newly released Checkra1n jailbreak means for iDevice security”, Ars Technica Nov 15 2019

Security Engineering 996 Ross Anderson


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


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

[824] 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


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


[841] P Gutmann, “Invalid banking cert spooks only one user in 300”, *Cryptography List* May 16 2005


[848] 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


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


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


[873] 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

[874] ‘HSE Team Inspection of the Control and Supervision of Operations at BNFL’s Sellafield Site’, Health and Safety Executive, 2000


Security Engineering 1000 Ross Anderson
[885] ER Henry, ‘Classification and Uses of Finger Prints’ George Rutledge & Sons, London, 1900


[889] Herodotus, ‘Histories’; Book 1 123.4, Book 5 35.3 and Book 7 239.3


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


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


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


Security Engineering 1002 Ross Anderson


[933] 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


Security Engineering 1003 Ross Anderson
[942] “Role of Communications in Operation Desert Storm”, in *IEEE Communications Magazine* (Special Issue) v 30 no 1 (Jan 92)


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

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


[966] R Iyengar, “Apple will pay up to $500 million to settle lawsuit over slowing down older iPhones”, CNN Mar 2 2020


[968] I Jackson, personal communication

[969] L Jackson, “BT forced to pay out refunds after free calls fraud”, in The Sunday Telegraph Feb 9 1997

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


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


[999] P Kafka, “Facebook’s political ad problem, explained by an expert” Vox, Dec 10 2019

[1000] B Kahle, “Libraries have been bringing older books to digital learners: Four publishers sue to stop it”, Internet Archive Blogs, July 22 2020

BIBLIOGRAPHY


[1006] L Kahney, “The FBI Wanted a Backdoor to the iPhone. Tim Cook Said No”, Wired Apr 16 2019


Security Engineering 1007  Ross Anderson


Security Engineering 1008 Ross Anderson
BIBLIOGRAPHY


[1049] T Kinder, “Regulator outlines plans to break up Big Four accounting firms”, Financial Times Feb 27 2020

[1050] T Kinder, “Big Four told to outline plans for audit split by October”, Financial Times Jul 6 2020

[1051] T Kinder, D McCrum, “EY fights fires on three audit cases that threaten its global reputation”, Financial Times Jun 8 2020


Security Engineering 1009 Ross Anderson
[1056] DV Klein, “Fooling the Cracker; A Survey of, and Improvements to Unix 

Economics’, Princeton 2004; at http://www.nuffield.ox.ac.uk/users/
klemperer/VirtualBook/VBCrevisedv2.asp


curity for Interconnected Signaling System # 7 Telecommunications Net-
works”, in First ACM CCS (1993) pp 195–212; later version in IEEE Com-
munications Magazine v 32 no 9 (Sep 94) pp 82–89

Texts in Mathematics no 114 (1987)


no 1 pp 1–15

[1064] 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

99 Springer LNCS v 1666 pp 388–397

[1066] P Kocher, “Design and Validation Strategies for Obtaining Assurance in 
Countermeasures to Power Analysis and Related Attacks”, at FIPS Physical 
cmvp/documents/fips140-3/physsec/papers/physsecpaper09.pdf

[1067] P Kocher, J Jaffe, B Jun, P Rohatgi, “Introduction to differential power 

[1068] 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

[1069] 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 At-
tacks: Exploiting Speculative Execution”, IEEE Symposium on Security 
and Privacy 2019

[1070] J Koebler, “Why American Farmers Are Hacking Their Tractors With 
Ukrainian Firmware”, Vice, Mar 21 2017

12 2020

[1072] BI Koerner, “Inside the Cyberattack That Shocked the US Government”, 
Wired Oct 23 2016

Into Upheaval”, Forbes Jun 24 2020

Security Engineering 1010 Ross Anderson


[1081] 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] K Korosec, “VW fires jailed Audi CEO Rupert Stadler” Techcrunch Oct 2 2018


[1086] 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


BIBLIOGRAPHY


[1097] HM Kriz, “Phreaking recognised by Directorate General of France Telecom”, in Chaos Digest 1.03 (Jan 93)


[1100] H Kuchler, “Can we ever trust Google with our health data?”, Financial Times Jan 20 2020


[1109] D Kundaliya, “Android devices are being increasingly targeted by undeletable adware, researchers warn”, Computing July 7 2020
[1110] L Kuo, “Chinese surveillance company tracking 2.5m Xinjiang residents”, in The Guardian Feb 18 2019


[1115] ‘L0phtCrack 2.52 for Win95/NT’, at http://www.10hht.com/10phtcrack/


[1118] F Lambert, “Tesla driver on Autopilot admits to watching a movie when crashing into police car” Elektrek, Aug 26 2020

[1119] F Lambert, “The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately heâ€™s a good guy” Elektrek, Aug 27 2020


[1121] L Lamont, “And the real Lotto winner is ... that man at the cash register”, Sydney Morning Herald, May 3 2007


[1123] L Lamport, Email message sent to a DEC SRC bulletin board at 12:23:29 PDT on 28 May 1987. Link No. 75,


Security Engineering 1013 Ross Anderson
BIBLIOGRAPHY


[1139] D Leloup, M Untersinger, “Comment les services de renseignement font la chasse aux employés des télécoms”, Le Monde Dec 8 2016

[1140] AK Lenstra, JP Hughes, M Augier, JW Bos, T Kleinjung, C Wachter, “Ron was wrong, Whit is right” IACR ePrint 2012/064


[1146] 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

Security Engineering 1014 Ross Anderson


[1170] S Liao “Spyware app abused iOS enterprise certificate to track targets” The Verge, Apr 8 2019
[1173] A Liptak, “Hackers reportedly used a tool developed by the NSA to attack Baltimore’s computer systems”, The Verge May 25 2019
[1181] N Lomas, “Targeted ads offer little extra value for online publishers, study suggests”, Techcrunch May 31 2019


[1190] B Lovejoy, “Apple being sued for refusing to help iTunes gift card scam victims”, 9to5Mac Jul 20 2020


[1193] I Lunden, “Apple fined record $1.2B in France over anti-competitive sales practices” TechCrunch Mar 16 2020


[1199] 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


Security Engineering 1017 Ross Anderson


[1207] M Magree, “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] F Main, “Your phone records are for sale”, Chicago Sun-Times, Jan 5 2006


[1212] 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


BIBLIOGRAPHY


[1234] AG Martínez, “How Trump Conquered Facebook—Without Russian Ads”, Wired Feb 23 2018


[1239] S Matala, T Nyman, N Asokan, “Historical insight into the development of Mobile TEEs ”, Aalto University Secure Systems Group blog, June 20 2019


[1250] V Mavroidis, P Svenda, “JavaCard: The execution environment you didn’t know you were using”, Software Sustainability Institute July 13 2018


Security Engineering 1020 Ross Anderson
[1253] 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


[1265] E McGaughey, “The extent of Russian-backed fraud means the referendum is invalid”, LSE Nov 14 2018


BIBLIOGRAPHY


Security Engineering 1022 Ross Anderson
BIBLIOGRAPHY


[1292] 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


[1297] M Mesa, “Phish Scales: Malicious Actor Combines Personalized Email, Variety of Malware To Target Execs”, ProofPoint Apr 5 2016


[1317] 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
[1323] “BBC fined £400,000 by Ofcom for fake competitions”, Daily Mirror July 30 2008


[1330] “Card fraud nets Esc6 billion’, F Mollet, Cards International (22/9/95) p 3


[1341] B Morgan, “Strip club which gave client £50k bill loses license” Evening Standard Jan 31 2020


[1343] R Morris, Invited talk, Crypto 95

BIBLIOGRAPHY


[1351] S Mukherjee, “What the Coronavirus Crisis Reveals About American Medicine”, New Yorker 27 April 2020


Security Engineering 1027 Ross Anderson

[1382] A Narayanan, “How to recognize AI snake oil” Arthur Miller lecture on science and ethics, Massachusetts Institute of Technology, Nov 18 2019


[1391] National Audit Office, ‘Rolling out smart meters’, Nov 23 2018


[1407] 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 1029 Ross Anderson
BIBLIOGRAPHY

[1418] J Naughton, “Facebook’s Vassal State”, in Memex 1.1 March 5, 2019


Security Engineering 1030 Ross Anderson
BIBLIOGRAPHY


[1438] C Newton, “The Trauma Floor”, The Verge, Feb 25, 2019

[1439] C Newton, “Mark Zuckerberg says Facebook will shift to emphasize encrypted ephemeral messages”, The Verge, Mar 6 2019

[1440] J Newton, “Countering the counterfeiters”, in Cards International (21/12/94) p 12


[1444] Andrew Ng, “How the Equifax hack happened, and what still needs to be done”, Cnet Sep 7 2018

[1445] S Nichols “Silence of the WANs: FBI DDoS-for-hire greaseball takedowns slash web flood attacks 'by 11%' ” The Register 19 Mar 2019

[1446] 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


[1454] ‘White Paper – 5g Evolution and 6g’, NTT Docomo, January 2020


Security Engineering 1031 Ross Anderson


[1466] S O’Kane, “Daimler fined nearly $1 billion for selling cars that cheated emissions tests”, The Verge, Sep 24 2019


[1468] “Nicht nachmachen: Dieser Vignetten-Trick kostet Sie 300 Euro”, Online Focus, June 12 2015


[1475] A Orlowski, “UK spy agency warns Brit telcos to flee from ZTE gear”, The Register April 16 2018


[1479] B Osborn, J McWilliams, B Beyer, M Saltonstall, “BeyondCorp – Design to Deployment at Google”, ;login: (Spring 2016) v 41 no 1

[1480] C Osborne, “University of California SF pays ransomware hackers $1.14 million to salvage research”, ZDNet, Jun 30 2020

[1481] C Osborne, “In one click: Amazon Alexa could be exploited for theft of voice history, PII, skill tampering”, ZDNet, Aug 13 2020


Security Engineering 1033 Ross Anderson


[1507] PeckShield, “bZx Hack Full Disclosure (With Detailed Profit Analysis)”, Medium Feb 17 2020


[1510] N Perlooth, S Shane, “In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc”, in New York Times May 25 2019


[1524] 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


Security Engineering 1035 Ross Anderson
BIBLIOGRAPHY


[1531] Politech mailing list, was at http://www.politechbot.com/


[1534] R Porter, “Google fined €50 million for GDPR violation in France” The Verge Jan 21 2019


[1538] F Postma, “Military And Intelligence Personnel Can Be Tracked With The Untappd Beer App”, Bellingcat May 18, 2020


[1540] S Poulter, “Phone firm’s whistleblower says his life has been made a misery”, in The Daily Mail Jun 21 2007


Security Engineering 1036 Ross Anderson
[1560] Public Accounts Committee, ‘Ministry of Defence nuclear programme’, Sep 2018
[1567] Z Quinn, ‘Crash Override’, Hachette 2017

Security Engineering 1037 Ross Anderson


[1574] R Ramesh, “Online tool could be used to identify public figures' medical care, say critics” The Guardian Mar 17 2014


Security Engineering 1038 Ross Anderson
BIBLIOGRAPHY


[1598] M Reynolds, “The strange story of Section 230, the obscure law that created our flawed, broken internet”, Wired Mar 24 2019


Security Engineering 1039 Ross Anderson


[1611] J Rogers, “FAKE FIVER: Shopper’s warning after being handed this fake £5 note – but is it counterfeit?”, The Sun May 13 2018

[1612] 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


[1615] K Rooney, “Majority of bitcoin trading is a hoax, new study finds” CNBC Mar 22 2019


[1623] “Card fraud plummets in France”, M Rowe, Banking Technology (May 94) p 10
[1624] 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


[1633] B Russell, Answer to parliamentary question, Hansard 10 Jun 2003 column 762W


[1645] I Sample, “NHS patient records to revolutionise medical research in Britain” The Guardian Aug 23 2012


[1655] E Van der Sar, “BitTorrent ‘Copyright Troll’ Lawsuits Skyrocket In Sweden”, Torrentfreak Feb 14 2020


BIBLIOGRAPHY


[1676] B Schneier, “Random Number Bug in Debian Linux”, May 19 2020


[1685] Schumpeter, “Live-streaming will change rock ‘n’ roll for the better”, The Economist, Jun 17 2020


[1690] N Scola, “Kamala Harris’ Crusade Against ‘Revenge Porn’ ”, Politico Feb 1 2019


BIBLIOGRAPHY

[1697] E Selleck, “Apple’s App Store is Populated With Gambling and Other Apps That Abuse Enterprise Certificates”, iPhone Hacks, Feb 12 2019


Security Engineering 1045 Ross Anderson
BIBLIOGRAPHY


[1741] N Silvester, “Doctor who hacked into Prime Minister’s health records escapes prosecution”, Daily Record Jan 10 2012

[1742] 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

[1743] Luther Simjian – Inventor of the Week, at https://lemelson.mit.edu/resources/luther-george-simjian

[1744] D Simmons, “BBC fools HSBC voice recognition security system”, BBC May 19 2017


[1746] 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

[1747] 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 [1748])


[1752] GJ Simmons, ‘Subliminal Channels; Past and Present’, European Transactions on Telecommunications v 5 no 4 (Jul/Aug 94) pp 459–473


[1759] 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


Security Engineering 1048 Ross Anderson
BIBLIOGRAPHY


[1774] SP Skorobogatov, “Flash Memory ‘Bumping’ Attacks”, CHES 2010


[1777] 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


[1783] SP Skorobogatov, C Woods. “In the blink of an eye: There goes your AES key” IACR Preprint 2012/296


Security Engineering 1049 Ross Anderson


[1789] A Smith, “New fake £20 notes ‘trick shop assistants then peel off within a week’ ”, Metro Nov 15 2018


[1798] T Snyder, ‘The Road to Unfreedom’, Bodley Head 2018


[1821] S Staniford, D Moore, V Paxson, N Weaver, “The Top Speed of Flash Worms”, in WORM04


Security Engineering 1051 Ross Anderson
BIBLIOGRAPHY

[1823] N Statt, “Fortnite for Android will ditch Google Play Store for Epic’s website”, The Verge Aug 3 2018


[1825] P Stein, P Feaver, ‘Assuring Control of Nuclear Weapons’, CSIA occasional paper number 2, Harvard University 1987


[1836] J van der Straaten, “So You Think Digital is the Future? Your Internet Data is Rotting”, Researchgate May 2019


Security Engineering 1052 Ross Anderson

[1843] Suetonius (Gaius Suetonius Tranquillus), ‘Vitae XII Caesarum’, translated into English as ‘History of twelve Caesars’ by Philemon Holland, 1606; Nutt (1899)


BIBLIOGRAPHY


[1863] C Tavris, E Aronson, ‘Mistakes were made – but not by me’, Harcourt 2007


[1867] J Temperton, “Inside Sellafield: how the UK’s most dangerous nuclear site is cleaning up its act”, *Wired*, 17 September 2016

[1868] S Tendler, N Nuttall, “Hackers run up £1m bill on Yard’s phones”, in *The Times*, 5 Aug 1996


[1876] R Thaler, C Sunnstein, *‘Nudge’*, Penguin 2009


[1886] I Thomson, “Talk about unintended consequences: GDPR is an identity thief’s dream ticket to Europeans’ data”, in *The Register* Aug 9 2019


[1892] 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/


[1904] A Travis, “Man who escaped mosque in burqa was under counter-terror restrictions”, in The Guardian Nov 5 2013


[1912] 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

[1913] D Uberti, “Facebook Went to War Against White Supremacist Terror After Christchurch. Will It Work?” Vice Oct 3 2019

[1914] R Uhlig, “BT admits staff could have fiddled system to win Concorde trip”, in The Daily Telegraph (23/7/1997)


[1923] UPI newswire item, Oklahoma distribution, November 26, 1983, Tulsa, Oklahoma


[1928] 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


[1931] S Vaidhyanathan, “Facebook’s new move isn’t about privacy. It’s about domination”, The Guardian March 7 2019


[1933] L van Hove, “Electronic Purses: (Which) Way to Go?”, in First Monday v 5 no 7 (June 2000)


[1936] 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


[1946] H Varian, Keynote address to the Third Digital Rights Management Conference, Berlin, Germany, January 13, 2005

[1948] 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


*Security Engineering* 1060 Ross Anderson


[1995] N Weaver, “Our Government Has Weaponized the Internet. Here’s How They Did It”, Wired Nov 13 2013


[2014] E Whitaker, “At SBC, It’s All About ‘Scale and Scope’ “, in Business Week Nov 7 2005


[2017] Z Whittaker, “Hackers are stealing years of call records from hacked cell operators”, Techcrunch, June 25 2019


[2024] 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


[2044] 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


Security Engineering 1064 Ross Anderson


[2063] 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


