Bibliography


912


[115] 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

**Security Engineering** 918 Ross Anderson


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


[131] 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/


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

Security Engineering 919 Ross Anderson


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


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


[152] E Bangeman, “The insanity of France’s anti-file-sharing plan: L’État, c’est IFPI”, in *Ars Technica* Nov 25 2007

**Security Engineering**

920

Ross Anderson
BIBLIOGRAPHY


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


Security Engineering 921 Ross Anderson
BIBLIOGRAPHY


BIBLIOGRAPHY


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


Security Engineering 923 Ross Anderson


BIBLIOGRAPHY


[231] 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


Security Engineering 925 Ross Anderson

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.


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/


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

Security Engineering 927 Ross Anderson
[277] N Borisov, I Goldberg, D Wagner, “Intercepting Mobile Communications: The Insecurity of 802.11”, at *Mobicom 2001*

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


[280] E Bovenlander, invited talk on smartcard security, *Eurocrypt 97*, reported in [100]


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


[290] L Brandimarte, A Acquisti, G Loewenstein, “Misplaced Confidences: Privacy and the Control Paradox”, *WEIS 2010*

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


[293] 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

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

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


[303] J Brodkin, “FCC requires anti-robo call tech after “voluntary” plan didn’t work out”, Ars Technica Apr 1 2020


[311] 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


Security Engineering 929 Ross Anderson


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


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

Security Engineering 930 Ross Anderson
[328] 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

[329] 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


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


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


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

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


Security Engineering 931 Ross Anderson


[359] “Dark horse in lead for fingerprint ID card”, Card World Independent (May 94) p 2

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

[361] 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

[362] “High tech helps card fraud decline” in Cards International no 117 (29 Sep 94)
[363] “Visa beefs up its anti-fraud technology”, in Cards International no 189 (12/12/97) p 5


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


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


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

[385] D Chaum, “Blind signatures for untraceable payments”, in Crypto 82,

75

'88, Springer LNCS v 403 pp 319–327

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

Facebook Feed”, Wired Oct 23 2014

Cameras via Smartphones” AsiaCCS 2018

[391] R Chesney, “Telephony Metadata: Is the Contact-Chaining Program Un-
salvageable?” Lawfare Blog March 6 2019

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

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

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

[395] 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

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

[397] KH Chuang, E Bury, R Degraeve, B Kaczer, G Groeseneken, I Ver-
bauwhede, D Linten, “Physically unclonable function using CMOS break-
down position”, IEEE International Reliability Physics Symposium (IRPS)
(2017)

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


pp 70–75

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

[402] C Cimpanu, “Backdoor found in Ruby library for checking for strong pass-
words”, ZDNet July 8 2019

Security Engineering 934 Ross Anderson
[403] C Cimpanu, “DNS-over-HTTPS causes more problems than it solves, experts say”, ZDNet Oct 6 2019
[404] C Cimpanu, “Major vulnerability patched in the EU’s eIDAS authentication system”, ZDNet Oct 29 2019
[405] C Cimpanu, “Average tenure of a CISO is just 26 months due to high stress and burnout”, ZDNet Feb 12 2020
[407] J Cipriani, “iOS 13: Top 5 new security and privacy features for your iPhone”, CNet Sep 22 2019
[415] R Clayton, private conversation, 2006


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


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

[430] “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


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


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


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


Security Engineering 936 Ross Anderson
BIBLIOGRAPHY


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


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


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

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


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


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


[464] H Crouch, “Two NHS trusts sign agreements with Sensyne Health”, *DigitalHealth* Feb 4 2019


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


[479] 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


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


BIBLIOGRAPHY


[496] 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


[512] 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
[513] 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

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


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


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


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


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


[531] 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


[535] 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


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


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

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


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

[560] 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

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

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

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


[567] 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

Security Engineering 943 Ross Anderson
BIBLIOGRAPHY


Security Engineering 944 Ross Anderson
[586] J Epstein, R Pascale, “User Interface for a High Assurance Windowing Sys-


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


[593] European Parliament, ‘Development of surveillance technology and risk of

mon rules for the internal market in electricity and repealing Directive

[595] European Union, ‘Directive on the protection of individuals with regard to
the processing of personal data and on the free movement of such data’, Di-
rective 95/46/EC, at http://www.privacy.org/pi/intl_orgs/ec/eudp. html

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

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

[598] Eurosma, ‘Protection Profile – Smart Card Integrated Circuit With Em-

setting up a Community regime for the control of exports of dual-use items
and technology’

sures to prevent and detect manipulation of records of tachographs’ Jan 23
2009

[601] R Evans, D Leigh, “GM subsidiary paid conman for ‘blagged’ private data, court
told”, The Guardian Apr 24, 2007; at http://www.guardian.co.uk/
crime/article/0,,2064180,00.html

[602] R Evans, “Trade unionist was refused job after police gave details to black-
list” The Guardian Mar 7 2019
[603] M Fairhurst, “Signature verification revisited: promoting practical exploita-
tion of biometric technology”, in Electronics and Communication Engineer-
ing Journal v 9 no 6 (Dec 97) pp 273–280

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

[605] 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


[607] Federal Committee on Statistical Methodology, ‘Statistical Policy Work-
ing Paper 22 (Revised 2005) – Report on Statistical Disclosure Limitation Methodology’


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


[623] A Fiat, M Naor, ”Broadcast Encryption”, in Crypto ’93, Springer LNCS v 773 pp 480–491


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

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

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


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


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

[647] B Fox, “The pirate’s tale”, in New Scientist 18 Dec 1999


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


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

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

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

Security Engineering 948 Ross Anderson
[657] “Finger minutiae system leaps the 1:100,000 false refusal barrier”, in Fraud Watch (1996) no 2 pp 6–9

[658] “Widespread card skimming causes European concern”, in Fraud Watch (1997) v 3 pp 1–2


[669] 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 950  Ross Anderson

[694] 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


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

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


Security Engineering 951 Ross Anderson


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


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

[726] D Goodin, “Developer of Checkm8 explains why iDevice jailbreak exploit is a game changer”, Ars Technica Sep 28 2019

[727] D Goodin, ‘Five months after returning rental car, man still has remote control’, Ars Technica, Oct 28 2019

[728] D Goodin, “Forum cracks the vintage passwords of Ken Thompson and other Unix pioneers”, Ars Technica Oct 10 2019

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

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


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


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

[758] 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


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


Security Engineering 954 Ross Anderson


[775] 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


[782] 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


Security Engineering 955 Ross Anderson
[785] JA Halderman, “Amazon’s MP3 Store Wisely Forgoes Watermarks”, Oct 2

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


Battlefield Weapons Systems and Technology Series (v 9), ISBN 0-08-037711-4

Keith.HallOfShame; see also http://www.threatcode.com/admin_rights.
htm

[790] M Hamburg, “Understanding Intel’s Ivy Bridge Random Number Genera-
tor”, Electronic Design Dec 11 2012


[792] H Handschu, P Paillier, J Stern, “Probing attacks on tamper-resistant
devices”, in Cryptographic Hardware and Embedded Systems – CHES 99,
Springer LNCS v 1717 pp 303–315

[793] R Hanley, “Millions in thefts plague New Jersey area”, in New York Times,
Feb 9, 1981, lc A; p 1

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

[795] C Harper, “How the PlusToken Scam Absconded With Over 1 Percent of
the Bitcoin Supply”, Bitcoin Magazine Aug 19 2019

[796] V Harrington, P Mayhew, ‘Mobile Phone Theft’, UK Home Office Research
Study 235, January 2002

[797] K Harris, ‘The State of Human Trafficking in California’, California De-
partment of Justice, 2012

[798] T Harris, “How Technology is Hijacking Your Mind – from a Magician and
Google Design Ethicist”, Medium May 18 2016

[799] MA Harrison, ML Ruzzo, JD Ullman, “Protection in Operating Systems”,

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

Policy and Guidelines”, in [57] pp 79–94

cessing Feb 2006

[803] Health and Human Services, ‘Standards for Privacy of Individually Iden-
tifiable Health Information’, HHS 45 CFR parts 160aÂ§164, 65 Federal
Register at 82461Â§82,510; see also 82,777–82,779

Security Engineering 956 Ross Anderson
BIBLIOGRAPHY


[813] Sir ER Henry, ‘Classification and Uses of Fingerprint’ George Rutledge & Sons, London, 1900


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


Security Engineering 957 Ross Anderson


BIBLIOGRAPHY


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


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


Security Engineering 959 Ross Anderson


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

[866] “New England shopping mall ATM scam copied in UK”, in Information Security Monitor v 9 no 7 (June 94) pp 1–2

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


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


[885] I Jackson, personal communication


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


BIBLIOGRAPHY


[900] R Jenkins, “Hole-in-wall thief used MP3 player”, in The Times Nov 15 2006; at http://www.timesonline.co.uk/article/0,,29389-2453590,00.html


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


Security Engineering 962 Ross Anderson


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


**Security Engineering** 963 Ross Anderson
BIBLIOGRAPHY


[938] A Katwala, “The race to create a perfect lie detector – and the dangers of succeeding” The Guardian Sep 5 2019


Security Engineering 964 Ross Anderson
BIBLIOGRAPHY


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


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


[991] 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


[1001] HM Kriz, “Phreaking recognised by Directorate General of France Telecom”, in Chaos Digest 1.03 (Jan 93)


[1003] H Kuchler, “Can we ever trust Google with our health data?”, Financial Times Jan 20 2020


[1012] L Kuo, “Chinese surveillance company tracking 2.5m Xinjiang residents”, in The Guardian Feb 18 2019


[1017] ‘L0phtCrack 2.52 for Win95/NT’, at http://www.l0pht.com/l0phtcrack/


[1021] L Lamont, “And the real Lotto winner is ... that man at the cash register”, Sydney Morning Herald, May 3 2007


BIBLIOGRAPHY

[1041] 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 970 Ross Anderson
BIBLIOGRAPHY


[1064] S Liao “Spyware app abused iOS enterprise certificate to track targets” *The Verge*, Apr 8 2019


[1073] N Lomas, “Targeted ads offer little extra value for online publishers, study suggests”, *Techcrunch* May 31 2019


Security Engineering 971 Ross Anderson


[1087] 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 972 Ross Anderson


[1099] F Main, “Your phone records are for sale”, Chicago Sun-Times, Jan 5 2006


Security Engineering 973 Ross Anderson


[1121] AG Martínez, “How Trump Conquered Facebook—Without Russian Ads”, Wired Feb 23 2018


[1124] S Matala, T Nyman, N Asokan, “Historical insight into the development of Mobile TEEs”, Aalto University Secure Systems Group blog, June 20 2019


Security Engineering 974 Ross Anderson


[1134] V Mavroudis, P Svenda, “JavaCard: The execution environment you didn’t know you were using”, Software Sustainability Institute July 13 2018


[1138] 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


[1148] E McGaughey, “The extent of Russian-backed fraud means the referendum is invalid”, LSE Nov 14 2018


[1176] M Mesa, “Phish Scales: Malicious Actor Combines Personalized Email, Variety of Malware To Target Execs”, ProofPoint Apr 5 2016


Security Engineering 977 Ross Anderson
BIBLIOGRAPHY


[1194] 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


[1200] “BBC fined £400,000 by Ofcom for fake competitions”, Daily Mirror July 30 2008


[1208] “Card fraud nets Esc6 billion’, F Mollet, Cards International (22/9/95) p 3


[1219] B Morgan, “Strip club which gave client £50k bill loses license” Evening Standard Jan 31 2020

[1221] R Morris, Invited talk, Crypto 95


[1228] S Mukherjee, “What the Coronavirus Crisis Reveals About American Medicine”, New Yorker 27 April 2020


[1231] E Munro, “Munro review of child protection: final report – a child-centred system” Department for Education May 10 2011


[1261] National Audit Office, *‘Minister of Defence: Combat Identification’*, 2002


[1263] National Audit Office, *‘Rolling out smart meters’*, Nov 23 2018

[1264] National Audit Office, *‘Investigation into Verify’*, Mar 5 2019

[1265] National Cyber Security Centre, *‘Annual Review 2019’* 2019


[1268] National Institute of Standards and Technology, *‘Data Encryption Standard (DES)’*, FIPS 46-3, Nov 1999 incorporating upgrade to triple DES


[1274] National Institute of Standards and Technology, *‘Digital Signature Standard (DSS)’*, FIPS 186-3, draft, Mar 2006


*Security Engineering* 982 Ross Anderson
BIBLIOGRAPHY


[1278] 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


[1288] J Naughton, “Facebook’s Vassal State”, in Memex 1.1 March 5, 2019


Security Engineering 983

Ross Anderson


[1309] C Newton, “The Trauma Floor”, The Verge, Feb 25, 2019

[1310] C Newton, “Mark Zuckerberg says Facebook will shift to emphasize encrypted ephemeral messages”, The Verge, Mar 6 2019

[1311] J Newton, “Countering the counterfeiters”, in Cards International (21/12/94) p 12


[1314] Andrew Ng, “How the Equifax hack happened, and what still needs to be done”, *Cnet* Sep 7 2018


[1316] 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


[1324] ‘White Paper – 5g Evolution and 6g’, NTT Docomo, January 2020


Security Engineering 985 Ross Anderson


[1336] “Nicht nachmachen: Dieser Vignetten-Trick kostet Sie 300 Euro”, Online Focus, June 12 2015


[1344] A Orlowski, “UK spy agency warns Brit telcos to flee from ZTE gear”, The Register April 16 2018


[1348] B Osborn, J McWilliams, B Beyer, M Saltonstall, “BeyondCorp – Design to Deployment at Google”, ;login: (Spring 2016) v 41 no 1
BIBLIOGRAPHY


Security Engineering 987 Ross Anderson


[1374] PeckShield, “bZx Hack Full Disclosure (With Detailed Profit Analysis)”, Medium Feb 17 2020


[1390] 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


[1397] Politech mailing list, was at http://www.politechbot.com/


[1400] R Porter, “Google fined €50 million for GDPR violation in France” The Verge Jan 21 2019


[1404] F Postma, “Military And Intelligence Personnel Can Be Tracked With The Untappd Beer App”, Bellingcat May 18, 2020


Security Engineering 989 Ross Anderson
[1406] S Poulter, “Phone firm’s whistleblower says his life has been made a misery”, in *The Daily Mail* Jun 21 2007


[1411] President’s Council of Advisers on Science and Technology, *Big Data and Privacy: A technological perspective*, May 1 2014


[1423] Public Accounts Committee, ‘Ministry of Defence nuclear programme’, Sep 2018


*Security Engineering* 990 Ross Anderson
BIBLIOGRAPHY


[1429] Z Quinn, ‘Crash Override’, Hachette 2017


[1434] R Ramesh, “Online tool could be used to identify public figures’ medical care, say critics” The Guardian Mar 17 2014


Security Engineering 991 Ross Anderson


[1457] M Reynolds, “The strange story of Section 230, the obscure law that created our flawed, broken internet”, Wired Mar 24 2019


BIBLIOGRAPHY


[1466] J Rogers, “FAKE FIVER: Shopper’s warning after being handed this fake £5 note ndash; but is it counterfeit?”, The Sun May 13 2018

[1467] 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


[1470] K Rooney, “Majority of bitcoin trading is a hoax, new study finds” CNBC Mar 22 2019


[1477] “Card fraud plummets in France”, M Rowe, Banking Technology (May 94) p 10

[1478] 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


Security Engineering 993 Ross Anderson


[1487] B Russell, Answer to parliamentary question, Hansard 10 Jun 2003 column 762W


[1498] I Sample, “NHS patient records to revolutionise medical research in Britain” The Guardian Aug 28 2012

Security Engineering 994 Ross Anderson
[1499] P Samuelson, “Copyright and digital libraries”, in Communications of the ACM v 38 no 4, April 1995


BIBLIOGRAPHY


[1540] N Scola. “Kamala Harris’ Crusade Against ‘Revenge Porn’ ”, Politico Feb 1 2019


[1545] E Selleck, “Apple’s App Store is Populated With Gambling and Other Apps That Abuse Enterprise Certificates”, iPhone Hacks, Feb 12 2019


[1581] N Silvester, “Doctor who hacked into Prime Minister’s health records escapes prosecution”, Daily Record Jan 10 2012

[1582] 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

[1583] Luther Simjian – Inventor of the Week, at https://lemelson.mit.edu/resources/luther-george-simjian

[1584] D Simmons, “BBC fools HSBC voice recognition security system”, BBC May 19 2017


[1586] 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

[1587] 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 [1588])


[1592] GJ Simmons, ‘Subliminal Channels; Past and Present’, European Transactions on Telecommunications v 5 no 4 (Jul/Aug 94) pp 459–473


[1597] 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


[1599] R Singel, “Point, Click ... Eavesdrop: How the FBI Wiretap Net Operates”, in Wired Aug 29 2007


[1604] A Sipress, “Tracking Traffic by Cell Phone; Md., Va. to Use Transmissions to Pinpoint Congestion”, in Washington Post (22/12/1999) p A01


[1613] SP Skorobogatov, “Flash Memory ‘Bumping’ Attacks”, CHES 2010


[1622] SP Skorobogatov, C Woods. “In the blink of an eye: There goes your AES key” IACR Preprint 2012/296


[1628] A Smith, “New fake £20 notes ‘trick shop assistants then peel off within a week’”, Metro Nov 15 2018


[1633] T Snyder, ‘The Road to Unfreedom’, Bodley Head 2018


Security Engineering 1002 Ross Anderson
[1643] E Spaord, “The Internet worm program: an analysis”, in Computer Communications Review v 19 no 1 (Jan 89) pp 17–57


[1660] S Staniford, D Moore, V Paxson, N Weaver, “The Top Speed of Flash Worms”, in WORM04


Security Engineering 1003 Ross Anderson
BIBLIOGRAPHY


[1668] J van der Straaten, “So You Think Digital is the Future? Your Internet Data is Rotting”, Researchgate May 2019


[1678] Suetonius (Gaius Suetonius Tranquillus), ‘Vitae XII Caesarii’, translated into English as ‘History of twelve Caesars’ by Philemon Holland, 1606; Nutt (1899)


[1695] C Tavris, E Aronson, ‘Mistakes were made – but not by me’, Harcourt 2007


[1699] J Temperton, “Inside Sellafield: how the UK’s most dangerous nuclear site is cleaning up its act”, Wired, 17 September 2016
[1700] S Tendler, N Nuttall, “Hackers run up £1m bill on Yard’s phones”, in The Times, 5 Aug 1996


[1713] I Thomson, “Talk about unintended consequences: GDPR is an identity thief’s dream ticket to Europeans’ data”, in The Register Aug 9 2019


[1718] MW Tobias, “Opening locks by bumping in five seconds or less: is it really a threat to physical security?”, 2006, at www.security.org


[1734] 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

BIBLIOGRAPHY

[1736] R Uhlig, “BT admits staff could have fiddled system to win Concorde trip”, in The Daily Telegraph (23/7/1997)


[1746] UPI newswire item, Oklahoma distribution, November 26, 1983, Tulsa, Oklahoma

[1747] S Usborne, “How did Tesla make some of its cars travel further during Hurricane Irma?”, The Guardian Sep 11 2017

[1748] S Vaidhyanathan, “Facebook’s new move isn’t about privacy. It’s about domination”, The Guardian March 7 2019


[1751] L van Hove, “Electronic Purses: (Which) Way to Go?”, in First Monday v 5 no 7 (June 2000)


[1754] 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 1008 Ross Anderson
[1764] H Varian, Keynote address to the Third Digital Rights Management Conference, Berlin, Germany, January 13, 2005
[1766] 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
BIBLIOGRAPHY


[1781] 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

[1782] L von Ahn, personal communication, 2006


Security Engineering 1010 Ross Anderson


[1809] M Weaver, “Developer tortured by raiders with crowbars”, Daily Telegraph, 31 October 97

Security Engineering 1011 Ross Anderson
[1810] N Weaver, “Our Government Has Weaponized the Internet. Here’s How They Did It”, Wired Nov 13 2013


[1827] E Whitaker, “At SBC, It’s All About ‘Scale and Scope’”, in Business Week Nov 7 2005

Security Engineering 1012 Ross Anderson


[1830] Z Whittaker, “Hackers are stealing years of call records from hacked cell operators”, Techcrunch, June 25 2019


[1837] 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


[1854] 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


[1870] 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


