Bibliography


951


Security Engineering 952 Ross Anderson


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


Security Engineering 953 Ross Anderson


BIBLIOGRAPHY


Security Engineering 955 Ross Anderson
BIBLIOGRAPHY


Security Engineering 956 Ross Anderson
BIBLIOGRAPHY


[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


Security Engineering 960 Ross Anderson


[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


BIBLIOGRAPHY


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


Security Engineering 962 Ross Anderson

Security Engineering 963 Ross Anderson
BIBLIOGRAPHY


[252] 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


BIBLIOGRAPHY


[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

[299] N Borisov, I Goldberg, D Wagner, “Intercepting Mobile Communications:
The Insecurity of 802.11”, at Mobicom 2001

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

[301] P Boulot, P Gaudry, A Guillevic, N Heninger, E Thomé, P Zimmermann,
“Factorization of RSA-250”, Cado-nfs-discuss mailing list Feb 28 2020

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

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

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

[305] C Bowden, Y Akdeniz, “Cryptography and Democracy: Dilemmas of Free-
dom”, in Liberating Cyberspace: Civil Liberties, Human Rights, and the

elections/elections_var.htm

[307] J Bowen, “Expulsion of diplomat sends a strong signal to Israel”, BBC
News, Mar 23 2011

[308] M Brader, “Car-door lock remote control activates another car’s alarm”, in
comp.risks 21.56 (Jul 2001)

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

Nov 25 2019

1502.05926 Feb 20 2015

[312] RM Brady, RJ Anderson, RC Ball, ‘Murphy’s law, the fitness of evolving
species, and the limits of software reliability’, Cambridge University Com-

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

[314] S Brands, ‘Rethinking Public Key Infrastructures and Digital Certificates –

[315] JT Brassil, S Low, NF Maxemchuk, “Copyright Protection for the Elec-
tronic 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 “AIJvoluntaryâ€œAI plan didn’t work out”, *Ars Technica* Apr 1 2020


[334] 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


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


Security Engineering 970 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 971 Ross Anderson


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

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

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


R Carter, “What You Are ... Not What You Have”, in International Security Review Access Control Special Issue (Winter 93/94) pp 14-16

A Case, M Meltzer, S Adair, “Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs”, Volexity Sep 2 2019


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


Center for Democracy and Technology, http://www.cdt.org/

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


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 Kohno, 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, “ Travelling 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-åÁZs homegrown tracing app”, Financial Times Jun 26 2020


[444] R Clayton, private conversation, 2006


[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


[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


[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 978 Ross Anderson
[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


[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 982 Ross Anderson
BIBLIOGRAPHY


[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


[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


[611] The Economist, “After rigging an election, Belarusâ€™s regime beats protesters” Aug 16 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/


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


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


Security Engineering 986 Ross Anderson
BIBLIOGRAPHY

[647] 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


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

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


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


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

[661] 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 987 Ross Anderson


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

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


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


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

Security Engineering 989 Ross Anderson


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


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


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

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

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

Security Engineering 990 Ross Anderson
“Finger minutiae system leaps the 1:100,000 false refusal barrier”, in *Fraud Watch* (1996) no 2 pp 6–9

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

SJ Freedberg, “Army Awards Lockheed $75M For AI Cyber/Jamming Pod”, *Breaking Defense* Apr 29 2020


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

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


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


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


*Security Engineering* 991 Ross Anderson


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


[758] 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


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

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


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


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

[791] D Goodin, “Police decrypt 258,000 messages after breaking pricey IronChat crypto app”, Ars Technica, Jul 11 2018

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

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


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

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

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


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


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

[823] 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


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


Security Engineering 996 Ross Anderson


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


[847] 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


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


[872] Health and Human Services, ‘Standards for Privacy of Individually Identifiable Health Information’, HHS 45 CFR parts 160â§164. 65 Federal Register at 82461â§82,510; see also 82,777–82,779

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


[884] ER Henry, ‘Classification and Uses of Finger Prints’ George Rutledge & Sons, London, 1900

[885] I Herbert, “No evidence against man in child porn inquiry who ’killed himself’ ”, in The Independent Oct 1 2005

Security Engineering 999 Ross Anderson
[888] Herodotus, 'Histories'; Book 1 123.4, Book 5 35.3 and Book 7 239.3

Security Engineering 1000 Ross Anderson


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


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


BIBLIOGRAPHY


[928] Q Hu, JY Yang, Q Zhang, K Liu, XJ Shen, “An automatic seal imprint verification approach”, in Pattern Recognition v 28 no 8 (Aug 95) pp 251–266


[932] 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


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

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

Security Engineering 1002 Ross Anderson
“Pink Death Strikes at US West Cellular”, in Information Security Monitor
v 9 no 2 (Jan 94) pp 1–2

Independent Security Evaluators Inc., “Content Protection for Optical Media”, May 2005

Information Systems Audit and Control Association, ‘Control Objectives for

Information Systems Audit and Control Association, ‘Exam Preparation
Materials available from ISACA’, at http://www.isaca.org/certi.htm

“Feds Praise Open Data Health Cloud Launch”, InformationWeek Nov 12
2013

International Atomic Energy Authority (IAEA), ‘The Physical Protection

International Standard on Auditing 315 (Revised 2019), International Au-
diting and Assurance Standard Board, Dec 2019

IBM, ‘IBM 4758 PCI Cryptographic Coprocessor – CCA Basic Services
Reference and Guide’, Release 1.31 for the IBM 4758-001


IEEE Spectrum, special issue on nuclear safekeeping, v 37 no 3 (Mar 2000)

CC Ife, Y Shen, SJ Murdoch, G Stringhini, “Waves of Malice: A Longitu-
dinal Measurement of the Malicious File Delivery Ecosystem on the Web”,
AsiaCCS 2019

I Ilves, “Why are Google and Apple dictating how European democracies
fight coronavirus?” The Guardian June 16 2020

“Ex-radio chief ‘masterminded’ TV cards scam”, in The Independent Feb 17
1998; see also “The Sinking of a Pirate”, Sunday Independent, Mar 1 1998

Information Commissioner’s Office, ‘Investigation into the use of data an-
alytics in political campaigns’, July 11 2018

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

Intel Corporation, ‘Intel Architecture Software Developer’s Manual – Vol-
ume 1: Basic Architecture’, Order number 243190 (1997)

Intel Corporation and others, ‘Advanced Access Content System (AACS) –
Technical Overview (informative)’, July 21 2004

60958, Geneva, February 1989

International Organization for Standardization, ‘Road Vehicles – Cyberson-
try Engineering’, ISO/SAE DIS 21434, 2020

M Isaac, K Conger, “Google, Facebook and Others Broaden Group to Se-

Security Engineering 1003 Ross Anderson


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


[967] I Jackson, personal communication


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


Security Engineering 1004 Ross Anderson


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

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


[1005] L Kahn, “The FBI Wanted a Backdoor to the iPhone. Tim Cook Said No”, *Wired* Apr 16 2019


[1023] A Katwala, “The race to create a perfect lie detector – and the dangers of succeeding” The Guardian Sep 5 2019

J Ross Anderson

Security Engineering 1007


[1048] T Kinder, “Regulator outlines plans to break up Big Four accounting firms”, Financial Times Feb 27 2020

[1049] T Kinder, “Big Four told to outline plans for audit split by October”, Financial Times Jul 6 2020

[1050] T Kinder, D McCrum, “EY fights fires on three audit cases that threaten its global reputation”, Financial Times Jun 8 2020

[1051] J King, “Bolero — a practical application of trusted third party services”, in Computer Fraud and Security Bulletin (July 95) pp 12–15


[1080] MR Koot, “After Ennetcom, Dutch police makes arrests re: PGP Safe, another Dutch company, for allegedly providing crypto phones to (primarily?) the underworld”, Mattij R. Koot’s Notebook, May 14 2017


[1083] K Korosec, “VW fires jailed Audi CEO Rupert Stadler” Techcrunch Oct 2 2018


BIBLIOGRAPHY


[1096] HM Kriz, “Phreaking recognised by Directorate General of France Telecom”, in Chaos Digest 1.03 (Jan 93)


[1099] H Kuchler, “Can we ever trust Google with our health data?”, Financial Times Jan 20 2020


[1108] D Kundaliya, “‘Android devices are being increasingly targeted by undeletable adware, researchers warn’, Computing July 7 2020

[1109] L Kuo, “Chinese surveillance company tracking 2.5m Xinjiang residents”, in The Guardian Feb 18 2019

Security Engineering 1011 Ross Anderson


[1114] ‘L0phtCrack 2.52 for Win95/NT’, at http://www.l0pht.com/l0phtcrack/


[1118] L Lamont, “And the real Lotto winner is ... that man at the cash register”, Sydney Morning Herald, May 3 2007


[1120] 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 1012 Ross Anderson
BIBLIOGRAPHY


[1136] D Leloup, M Untersinger, “Comment les services de renseignement font la chasse aux employés des télécoms”, Le Monde Dec 8 2016

[1137] AK Lenstra, JP Hughes, M Augier, JW Bos, T Kleinjung, C Wachter, “Ron was wrong, Whit is right” IACR ePrint 2012/064


[1143] 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 1013 Ross Anderson


[1167] S Liao “Spyware app abused iOS enterprise certificate to track targets” The Verge, Apr 8 2019
[1170] A Liptak, “Hackers reportedly used a tool developed by the NSA to attack Baltimore’s computer systems”, The Verge May 25 2019
[1173] FF Liu, Y Yarom, Q Ge, G Heiser, RB Lee, “Last-Level Cache Side-Channel Attacks are Practical” IEEE Symposium on Security and Privacy 2015
[1178] N Lomas, “Targeted ads offer little extra value for online publishers, study suggests”, Techcrunch May 31 2019


[1187] B Lovejoy, “Apple being sued for refusing to help iTunes gift card scam victims”, *9to5Mac* Jul 20 2020


[1190] I Lunden, “Apple fined record $1.2B in France over anti-competitive sales practices” *TechCrunch* Mar 16 2020


[1196] 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


[1200] B Macq, ‘Special Issue – Identification and protection of Multimedia Information’, *Proceedings of the IEEE* v 87 no 7 (July 1999)


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


[1209] 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


[1231] AG Martínez, “How Trump Conquered Facebook—Without Russian Ads”, Wired Feb 23 2018


[1236] S Matala, T Nyman, N Asokan, “Historical insight into the development of Mobile TEEs ”, Aalto University Secure Systems Group blog, June 20 2019

[1238] SA Mathieson. “Gone phishing in Halifax – UK bank sends out market-


[1247] V Mavroudis, P Svenda, “JavaCard: The execution environment you didn’t know you were using”, Software Sustainability Institute July 13 2018


[1250] 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


BIBLIOGRAPHY


[1262] E McGaughey, “The extent of Russian-backed fraud means the referendum is invalid”, LSE Nov 14 2018


[1271] J McLaughlin, Z Dorfman, “‘Shattered’: Inside the secret battle to save America’s undercover spies in the digital age”, Yahoo News Dec 30 2019


Security Engineering 1020 Ross Anderson


[1289] 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


Security Engineering 1021 Ross Anderson
BIBLIOGRAPHY


[1294] M Mesa, “Phish Scales: Malicious Actor Combines Personalized Email, Variety of Malware To Target Execs”, ProofPoint Apr 5 2016


Security Engineering 1022

Ross Anderson


[1314] GA Miller, “The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information”, in *Psychological Review* v 63 (1956) pp 81-97


[1320] “BBC fined £400,000 by Ofcom for fake competitions”, *Daily Mirror* July 30 2008


[1327] “Card fraud nets Esc6 billion”, F Mollet, *Cards International* (22/9/95) p 3


[1338] B Morgan, “Strip club which gave client £50k bill loses license” Evening Standard Jan 31 2020


[1340] R Morris, Invited talk, Crypto 95


[1348] S Mukherjee, “What the Coronavirus Crisis Reveals About American Medicine”, New Yorker 27 April 2020


[1379] A Narayanan, “How to recognize AI snake oil” Arthur Miller lecture on science and ethics, Massachusetts Institute of Technology, Nov 18 2019


BIBLIOGRAPHY


[1388] National Audit Office, ‘Rolling out smart meters’, Nov 23 2018


Security Engineering 1027 Ross Anderson
[1404] 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


[1415] J Naughton, “Facebook’s Vassal State”, in Memex 1.1 March 5, 2019


[1421] RM Needham, “Naming”, in [1350], pp 318–127


Security Engineering 1028 Ross Anderson


[1435] C Newton, “The Trauma Floor”, *The Verge*, Feb 25, 2019

[1436] C Newton, “Mark Zuckerberg says Facebook will shift to emphasize encrypted ephemeral messages”, *The Verge*, Mar 6 2019

[1437] J Newton, “Countering the counterfeiter”, in *Cards International* (21/12/94) p 12


[1441] Andrew Ng, “How the Equifax hack happened, and what still needs to be done”, *Cnet* Sep 7 2018
[1442] S Nichols “Silence of the WANs: FBI DDoS-for-hire greaseball takedowns slash web flood attacks 'by 11%' ” The Register 19 Mar 2019

[1443] 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


[1451] ‘White Paper – 5g Evolution and 6g’, NTT Docomo, January 2020


Security Engineering 1030 Ross Anderson


[1463] S O’Kane, ‘Daimler fined nearly $1 billion for selling cars that cheated emissions tests’, The Verge, Sep 24 2019


[1465] “Nicht nachmachen: Dieser Vignetten-Trick kostet Sie 300 Euro”, Online Focus, June 12 2015


[1467] Open Net Initiative, ‘China (including Hong Kong)’, Country report 2006, at https://opennet.net/


[1472] A Orlowski, “UK spy agency warns Brit telcos to flee from ZTE gear”, The Register April 16 2018


[1476] B Osborn, J McWilliams, B Beyer, M Saltonstall, “BeyondCorp – Design to Deployment at Google”, ;login: (Spring 2016) v 41 no 1
BIBLIOGRAPHY

[1477] C Osborne, “University of California SF pays ransomware hackers $1.14 million to salvage research”, ZDNet, Jun 30 2020

[1478] C Osborne, “In one click: Amazon Alexa could be exploited for theft of voice history, PII, skill tampering”, ZDNet, Aug 13 2020


BIBLIOGRAPHY


[1504] PeckShield, “bZx Hack Full Disclosure (With Detailed Profit Analysis)”, Medium Feb 17 2020


A Peyton, “Ethereum Classic hit by another 51% hack”, Fintech Direct, Aug 6 2020

A Pfitzmann, Proceedings of the Third International Workshop on Information Hiding (1999), Springer LNCS v 1768


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


L Pinault, ‘Consulting Demons’, Collins 2000

S Pinto, N Santos, “Demystifying Arm TrustZone: A Comprehensive Survey”, ACM Computing Surveys v 51 no 6 (Feb 2019)


RA Poisel, ‘Modern Communications Jamming Principles and Techniques’, Artech House 2003

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


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


[1535] F Postma, “Military And Intelligence Personnel Can Be Tracked With The Untappd Beer App”, *Bellingcat* May 18, 2020


[1537] S Poulter, “Phone firm’s whistleblower says his life has been made a misery”, in *The Daily Mail* Jun 21 2007


[1557] Public Accounts Committee, ‘Ministry of Defence nuclear programme’, Sep 2018


[1564] Z Quinn, ‘Crash Override’, Hachette 2017


[1571] R Ramesh, “Online tool could be used to identify public figures’ medical care, say critics” The Guardian Mar 17 2014

Security Engineering 1036 Ross Anderson

Security Engineering 1037 Ross Anderson


[1595] M Reynolds, “The strange story of Section 230, the obscure law that created our flawed, broken internet”, Wired Mar 24 2019


[1608] J Rogers, “FAKE FIVER: Shopper’s warning after being handed this fake £5 note – but is it counterfeit?”, The Sun May 13 2018

Security Engineering 1038 Ross Anderson
[1609] 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


[1612] K Rooney, “Majority of bitcoin trading is a hoax, new study finds” CNBC Mar 22 2019


[1620] “Card fraud plummets in France”, M Rowe, Banking Technology (May 94) p 10

[1621] 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


[1630] B Russell, Answer to parliamentary question, Hansard 10 Jun 2003 column 762W


[1642] I Sample, “NHS patient records to revolutionise medical research in Britain” The Guardian Aug 28 2012


Security Engineering 1041 Ross Anderson
[1673] B Schneier, “Random Number Bug in Debian Linux”, May 19 2020
[1682] Schumpeter, “Live-streaming will change rock ‘n’ roll for the better”, The Economist, Jun 17 2020
[1687] N Scola. “Kamala Harris’ Crusade Against ‘Revenge Porn’ “, Politico Feb 1 2019
[1694] E Selleck, “Apple’s App Store is Populated With Gambling and Other Apps That Abuse Enterprise Certificates”, iPhone Hacks, Feb 12 2019
A Shamir, “How to share a secret”, in *Communications of the ACM* v 22 no 11 (Nov 1979) pp 612–613


C Shapiro, “Antitrust in a time of populism”, *SSRN 3058345*, 2017


Ilia Shumailov,


Security Engineering 1045 Ross Anderson
BIBLIOGRAPHY


[1738] N Silvester, “Doctor who hacked into Prime Minister’s health records escapes prosecution”, Daily Record Jan 10 2012

[1739] 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

[1740] Luther Simjian – Inventor of the Week, at https://lemelson.mit.edu/resources/luther-george-simjian

[1741] D Simmons, “BBC fools HSBC voice recognition security system”, BBC May 19 2017


[1743] 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

[1744] 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 [1745])


[1749] GJ Simmons, ‘Subliminal Channels; Past and Present’, European Transactions on Telecommunications v 5 no 4 (Jul/Aug 94) pp 459–473


[1756] 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


[1771] SP Skorobogatov, “Flash Memory ‘Bumping’ Attacks”, CHES 2010


[1774] 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


[1780] SP Skorobogatov, C Woods. “In the blink of an eye: There goes your AES key” IACR Preprint 2012/296


[1786] A Smith, “New fake £20 notes ‘trick shop assistants then peel off within a week’”, Metro Nov 15 2018


[1795] T Snyder, ‘The Road to Unfreedom’, Bodley Head 2018


BIBLIOGRAPHY


[1818] S Staniford, D Moore, V Paxson, N Weaver, “The Top Speed of Flash Worms”, in WORM04


[1820] N Statt, “Fortnite for Android will ditch Google Play Store for Epic’s website”, The Verge Aug 3 2018


BIBLIOGRAPHY

[1833] J van der Straaten, “So You Think Digital is the Future? Your Internet Data is Rotting”, Researchgate May 2019
[1840] Suetonius (Gaius Suetonius Tranquillus), ‘Vitae XII Caesarum’, translated into English as ‘History of twelve Caesars’ by Philemon Holland, 1606; Nutt (1899)

Security Engineering 1051 Ross Anderson


[1860] C Tavris, E Aronson, ‘Mistakes were made – but not by me’, Harcourt 2007


[1864] J Temperton, “Inside Sellafield: how the UK’s most dangerous nuclear site is cleaning up its act”, Wired, 17 September 2016

[1865] S Tendler, N Nuttall, “Hackers run up £1m bill on Yard’s phones”, in The Times, 5 Aug 1996


Security Engineering 1053 Ross Anderson

[1883] I Thomson, “Talk about unintended consequences: GDPR is an identity thief’s dream ticket to Europeans’ data”, in The Register Aug 9 2019


[1889] 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/


[1901] A Travis, “Man who escaped mosque in burqa was under counter-terror restrictions”, in The Guardian Nov 5 2013


[1908] Z Tufekci, “Zuckerberg’s So-Called Shift Toward Privacy”, New York Times March 7 2019

[1909] 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


[1911] R Uhlig, ‘BT admits staff could have fiddled system to win Concorde trip”, in The Daily Telegraph (23/7/1997)


Security Engineering 1055 Ross Anderson


[1919] UPI newswire item, Oklahoma distribution, November 26, 1983, Tulsa, Oklahoma


[1924] 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


[1927] S Vaidhyanathan, “Facebook’s new move isn’t about privacy. It’s about domination”, The Guardian March 7 2019


[1929] L van Hove, “Electronic Purses: (Which) Way to Go?”, in First Monday v 5 no 7 (June 2000)


[1932] 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


[1942] H Varian, Keynote address to the Third Digital Rights Management Conference, Berlin, Germany, January 13, 2005


[1944] 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


[1964] L von Ahn, personal communication, 2006


Security Engineering 1058 Ross Anderson
BIBLIOGRAPHY


Security Engineering 1060 Ross Anderson


[2013] Z Whittaker, “Hackers are stealing years of call records from hacked cell operators”, Techcrunch, June 25 2019


[2020] 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


[2026] D Winder, “How To Make $1 Million From Hacking: Meet Six Hacker Millionaires”, Forbes, Aug 29 2019


BIBLIOGRAPHY


[2040] 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


[2065] RS Zhang, XY Wang, XH Yan, XX Jiang, “Billing Attacks on SIP-Based VOIP Systems”, in *WOOT 2007*


Security Engineering 1064 Ross Anderson