Curriculum Vitae – Ross Anderson

I am Professor of Security Engineering at Cambridge University and also at Edinburgh University. Security Engineering is about building systems to remain dependable in the face of malice, error or mischance. As a discipline, it focuses on the tools, processes and methods needed to design, implement and test complete systems, and to adapt existing systems as their environment evolves.

My mission has been building security engineering into a discipline. Thirty years ago, some parts of it – cryptography, protocols and operating system security – had some solid theory, but the experts mostly didn't talk to each other. Other aspects, such as software security, were a practitioners' art, while yet other aspects such as hardware security were just black magic.

Since 1992 I've started research programs in neglected areas, ranging from hardware security through API security and signal processing to security economics. I've worked on applications from payments through online medical records to curfew tags, and documented their failure modes so that engineers can learn from them. I wrote the standard textbook, *'Security Engineering – A Guide to Building Dependable Distributed Systems'* of which the first edition came out in 2001, the second in 2008 and the third in 2020 [272]. Along the way I've contributed to the design of a number of widely-deployed systems, from the STS specification for prepayment utility meters (with over 400 million in over 100 countries) through the HomePlug standard for power-line communications (widely used to extend wifi) to the design of Android Pay which enables hundreds of millions of people to make credit card payments with their mobile phones. This work has been recognised by the Lovelace Medal, the UK's top award in computing.

Sustainability is a growing theme as security engineering merges with safety and becomes essential to the next generation of cars, medical devices and much else. Regular security patches for durable goods will make security a larger part of the total lifecycle cost. A law that my work helped the EU to develop (2019/771) requires firms selling consumer goods with software components to patch them for the length of time the customer can reasonably expect; another (the Cyber Resilience Act) will extend this to other goods such as routers.

Our Cambridge Cybercrime Centre collects and curates data about online wickedness, from spam and phish to underground crime forums; this is now used by over 300 researchers in over 80 universities worldwide. Now that most acquisitive crime is online, security engineering is moving steadily up the political agenda; our work spills over into the study of violent online political extremism, and it informs a number of policy areas including privacy, surveillance, competition and artificial intelligence.

My university duties at Cambridge include teaching an undergraduate course in security and software engineering, and graduate courses in security and cybercrime. At Edinburgh, where I hold a 20% appointment, I teach a security engineering course.

Ross Anderson FRS FREng
September 2023

1 Research

1.1 Machine learning and signal processing

Our most recent technical research topic is adversarial machine learning. The revolution in neural networks since 2012 has let us build better pattern-recognition systems, but they are fragile in that an adversary can usually find inputs that look the same to humans but very different to classifiers. We invented a mechanism to diversify neural networks with a key, so that adversarial images will only fool the specific instance of the classifier against which they were trained, and otherwise raise an alarm [257, 259, 261, 268]. We've extended adversarial attacks to the kind of models that play games [267] and the kind that deal with 3-d images [271]. We've also worked out how to poison or backdoor machine-learning systems by manipulating the order in which training samples are presented, rather than by changing the samples or their labels [274]. We explained why training machine-learning models on the outputs of other models is dangerous and can lead to model collapse [299]. We also discovered how to develop inputs that take classifiers a lot of time or energy to process, leading to service-denial attacks [269]. This led to the discovery of attacks on almost all large NLP systems based on manipulating Unicode inputs [277], to the 'Trojan source' attack which broke almost all compilers using similar techniques [280, 288] and to a variety of attacks on search engines [297]. We have also shown how randomness tests that were standardised as being good enough for cryptographic key generation aren't enough for some machine learning applications [**?**].

In earlier work, we applied machine learning to improve side-channel attacks based on signal processing. We can work out what PIN you put in your phone by watching the camera wobble or listening to the taps on the screen; we can do the listening either with the phone's own microphones, or those on a nearby smart speaker [210, 262, 273].

We started applying signal-processing ideas to computer security back in the 1990s. We showed that 'Tempest' attacks on computers, which exploit stray RF emissions, could be mitigated by software as well as by hardware shielding [51, 75]. We also broke almost all the copyright marking schemes in use at the time [50]; our 'Stirmark' software became the industry standard for testing them [73, 72]. We returned to that topic in 2021 with a new way of embedding copyright marks in images which are extremely hard for inpainters based on machine learning to remove [276].

1.2 Economics and security

If Alice guards a system but Bob pays the cost of failure, you can expect trouble. We now know that many real-world security problems can be best explained using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection and the tragedy of the commons. This field took off since I wrote about it in 2001 in an award-winning paper [90] and in my Security Engineering textbook [88]; it now has over 100 active researchers. We have helped drive policy via studies for the European Commission of the security economics of cyber-crime [154, 160], the resilience of the Internet [187] and what happens to safety regulation once there's software in everything [246, 247]; and via studies of the costs of cybercrime in 2011 [196] and 2018 [265].

I have spent about a decade building up the Cambridge Cybercrime Centre, which collects lots of data on malware, spam, phish and other online bad things as a service to the research community; over 300 researchers in over 80 universities now license our data. For surveys, see [134, 145, 171] and [188]. We have other papers on attitudes to online crime [217], the security economics of critical national infrastructure [170, 175] and surveillance [216], the ways in which financial regulators ignore abuses [255], and the economics of the business of cybercrime [278]. Our most recent initiative has been to extend our collection to online extremism [281], which is making novel data collections available to scholars of topics from misogyny to terrorism. Our data are also helping us in a long-term project to extend our security economics work through behavioural economics into psychology [179, 188, 192, 193, 211, 217, 218, 220, 221, 229, 231, 235, 254, 263, 286, 296].

1.3 What goes wrong with real systems

Engineers learn much more from the bridge that falls down than from the hundred that remain standing. I therefore study the failure modes of a number of critical systems including payment card systems [10, 12, 17, 113, 120, 142, 125, 139, 143, 153, 159, 165, 177, 180, 181, 192, 195, 201, 202, 213, 219, 225, 231, 232, 237], prepayment utility meters [18, 30], medical record systems [23, 29, 61, 68, 69, 129, 136, 151, 222] and vehicle systems [56]. Our laboratory's maxim is that 'good research comes from real problems'. From these case studies, I try to distil the essence of good security design [6, 14, 16, 21, 25, 31, 36, 47]. One piece of work led to the cancellation of badly-designed databases intended to support child protection [135]; another was an investigation into how Chinese agents compromised the Dalai Lama's office computers [167]; another work stream tackled smart grids and smart meters [170, 175, 182, 184, 203]. Recently we've been looking at security vulnerabilities in mobile phones [210, 226, 227, 234], at ways of extending mobile payments offline [233, 245], and at protecting data about wildlife from poachers [256].

Since 2016 we've also been working on the engineering and incentives necessary to maintain the software in durable safety-critical goods like cars and medical devices [246, 247, 251]. Research funded by Bosch (because of their interest in robust machine vision) led to much of the work on machine learning desrcirbed above; it also led to work on more sustainable toolchains [253].

1.4 Cryptographic protocols and APIs

Many of the interesting technical failures in security systems are where the wrong things are encrypted, or the right things are encrypted in the wrong way. Over the years I have discovered many protocol attacks [5, 14, 21, 33, 40, 41, 43]. I was the first to use formal methods to verify the crypto protocols underlying a real banking system [6, 16, 45]. I have also designed a number of protocols [13, 28, 46, 58, 62, 70, 93, 233], was one of the inventors of micropayments [28], and of the idea of making files sufficiently invisible that their existence can be plausibly denied even in the face of compulsion (the 'Steganographic File System' [52]). I've also worked on protocols in industrial control systems [183, 184], the interaction between protocols and economics [115, 186], with psychology [179, 192] and the effects on innovation [178, 185, 186, 187, 243].

I designed the trust-on-first-use key-management protocols for HomePlug, now deployed in millions of consumer electronic devices [128, 138]. I also pioneered API attacks, which extend protocol analysis to the application programming interfaces of cryptographic processors [80, 89, 102, 142, 125, 126]. Our work forced most manufacturers of hardware security modules to redesign their products [122].

1.5 Hardware reverse engineering

In 1996, we opened up the field of semiconductor security with a paper on the tamper-resistance of smartcards [37]. Our biggest contribution was probably in [95, 97] where we pioneered semi-invasive semiconductor testing: the idea is to use lasers to read out memory contents by inducing photocurrents and also to induce revealing faults. We then showed that common PIN entry devices could be hacked, explaining a number of payment frauds [153, 201]. We've also shown that you can recast decompilation as a search problem [209], which helps the analysis of large malware families that differ from each other by small tweaks.

1.6 Peer-to-Peer systems and networks

I wrote one of the seminal papers on peer-to-peer systems when I proposed the Eternity Service [35]; the ideas were taken up by Freenet, Gnutella, Publius, Kazaa and others. We also developed mechanisms for authenticating distributed content using hash trees and hash chains [58, 62]. Further papers include [70, 71, 76, 82, 84, 105, 106, 108, 121, 229].

We later found that the topology of insurgent networks shapes, and is shaped by, strategies of attack and defence; our models can explain why insurgents form cells, and the circumstances under which suicide attacks are rational strategy. This led us to develop metrics and other analysis techiques for both static and dynamic networks [118, 121, 144, 155, 148, 202, 190, 191, 207]. We also looked at the privacy problems of social networks [161, 168].

1.7 Analysis and design of ciphers

Breaking ciphers was my introduction to information security in the mid-1980's when I found a number of attacks on the stream ciphers then in use [3, 4] and proposed improved versions [1]. Further work on stream ciphers [7, 15, 19] led to work on hash functions [11, 26] and to ways of constructing block ciphers from hash functions and stream ciphers [27]. My big project was 'Serpent', a block cipher which was a finalist in the Advanced Encryption Standard contest [54, 59, 60]. The winner, Rijndael, got 87 votes at the final AES conference while Serpent with 59 votes was second.

1.8 Physics and security

We used ideas from statistical physics to model why the reliability growth of large systems in response to testing is as poor as can possibly be: a software version of 'Murphy's Law' [74]. One consequence is that, under standard assumptions, open-source and proprietary systems are equivalent – in the sense that opening up the design helps the attacker and the defender to exactly the same extent [96]. If you want to know whether one or the other is better, you need to look at which of our model's assumptions are violated.

We have also been working to show that many of the claims made on behalf of quantum systems hinge on a particular interpretation of the Bell tests, which is not the only one [205, 208, 212, 223], raising issues with the security proofs offered for quantum crypto based on entanglement [298].

1.9 Policy

The 1990s brought the 'Crypto wars'. The Clinton government claimed that they needed to control cryptography; I was one of the authors of the most widely-cited paper rebutting this claim [44]. Further writings on crypto policy and technology policy followed [22, 43, 48, 53, 65, 87, 100, 101, 103, 110, 130, 131, 132, 133, 140, 172, 173, 197, 198]).

In 1998, I was one of the founders of the Foundation for Information Policy Research, a think-tank. We secured amendments to various laws including the RIP Act and the Export Control Act in the UK and the IPR Enforcement Directive in Brussels. We also worked with other NGOs to set up European Digital Rights (EDRi) in Brussels. I was on the UK GCSA's Blackett Review of Cyber Security, which led in 2011 to an extra £640m being spent on cyber security over the period 2011–5.

After Ed Snowden disclosed large-scale lawbreaking by the signals intelligence agencies in 2013, crypto controls were brought back on the agenda by UK Prime Minister David Cameron and FBI Director James Comey; we updated our classic paper on the costs and risks of government-mandated exceptional access to systems [230]. Most recently, following the push by the intelligence community and the European Commission for client-side scanning and the announcement by Apple of such a product, we wrote a third paper explaining why this exposes democracy and the rule of law to unacceptable risks [280]. As the intelligence agencies were working to push the Online Safety Bill through the UK Parliament and the Child Sex Abuse Regulation through the European Parliament, I followed up with critiques of the Bill [289] and the agencies' arguments around child protection [291]. I also analysed the effects of the mandate for interoperability in the EU Digital Markets Act which is also clearly designed to undermine end-to-end encryption [294], and the likely effectiveness of the Online Safety Act's censorship powers [296].

Other papers with impact on UK policy include a 2006 report for the Information Commissioner on children's databases [135], and a 2009 report published by the Joseph Rowntree Reform Trust entitled *'Database State'* on the safety, privacy and legality of large UK public-sector databases [166]; this was adopted by both Conservative and

Liberal Democrat parties before the 2010 election, which they won – leading to the abandonment of two children's databases.

Papers with impact in the EU include a 2008 study of the security economics and policy options in cybercrime [154]; a 2011 study for ENISA of the resilience of the Internet [187]; and a 2016 report on what happens to safety regulation in a world full of Internet-connected things [246, 247, 251]. This led to the Sales of Goods directive 2019/771 which mandates software maintenance among other things.

Other policy topics include tracing stolen bitcoin [252, 255, 260] and what tracing tools say about financial regulation; a 2010 report on the costs of cybercrime, commissioned by the Ministry of Defence, and repeated in 2017 [196, 265]; and a Nuffield Bioethics Council report on what happens to medical ethics in a world of cloud-based medical records and pervasive genomics [222].

1.10 Research mentoring and management

I advise four Cambridge research students (David Khachaturov, Nicholas Boucher, Jenny Blessing and Anh Vu). Ten former students are professors (George Danezis and Steven Murdoch at UCL, Robert Watson, Frank Stajano and Markus Kuhn at Cambridge, Jeff Yan at Strathclyde, Feng Hao at Warwick, Shishir Nagaraja at Newcastle, Tyler Moore at Tulsa and Hyoungshick Kim at Sungkyunkwan), along with three former postdocs (Alice Hutchings at Cambridge, Vasek Matyas at Brno and Sophie van der Zee at Rotterdam). Thirty of my former research students have earned PhDs (Jong-Hyeon Lee, Fabien Petitcolas, Frank Stajano, Harry Manifavas, Markus Kuhn, Ulrich Lang, Jeff Yan, Susan Pancho, Mike Bond, George Danezis, Sergei Skorobogatov, Hyun-Jin Choi, Richard Clayton, Jolyon Clulow, Feng Hao, Andy Ozment, Tyler Moore, Shishir Nagaraja, Robert Watson, Hyoungshick Kim, Shailendra Fuloria, Joe Bonneau, Wei-Ming Khoo, Rubin Xu, Kumar Sharad, Laurent Simon, Dongting Yu, Shehar Bano, Khaled Baqer, Alexander Vetterl, Mansoor Ahmed and Ilia Shumailov).

I have started four conference series (Fast Software Encryption in 1993 [9], Information Hiding [38] in 1996, the Workshop on Economics and Information Security in 2002 and the Workshop on Security and Human Behaviour in 2008), as well as one journal (Computer and Communications Security Reviews). I helped Sophie van der Zee start Decepticon.

I am a special adviser on information security to the risk committee of the board of Infosys. Other consultancy clients over the last twenty years include Google Deepmind, Raspberry Pi, RealVNC, Alcatel-Lucent, Qualcomm, Samsung, Actel, Securicor, Lehman Brothers, Kudelski, Matsushita, Microsoft, Intel, VISA, the UK Department of Transport, the British and Icelandic Medical Associations, the Government of Singapore and the Electricity Supply Commission of South Africa. Many of these assignments led to research papers.

2 Teaching and other activities

My teaching responsibilities at Cambridge have covered those areas of the curriculum that have to do with the dependability of computer systems. My lecture courses in 2022–23 are in Software and Security Engineering (for first-year undergraduates), on Computer Security and on Cybercrime (both MPhil). I've served on numerous committees having been elected to the University's governing body, Council, for 2003–2006, 2007–10, and 2015–18.

Since February 2021 I have also been appointed to a chair at Edinburgh one day per week. In 2021–22 I taught a new masters-level course in Security Engineering which continues in 2022–23.

3 Work history

2021–present: Edinburgh University School of Informatics. Professor of Security Engineering.

1992–present: Cambridge University Computer Laboratory. Professor of Security Engineering since October 2003; Reader in Security Engineering 2000–3; University Lecturer 1995-2000; Senior Research Associate 1995; research student 1992–4.

2011: Visiting scientist, Google; visiting professor, CMU

1984–1991: Self employed consultant working mostly in projects related to computer security.

1981–83: worked on multilingual typesetting

1979–80: gap-year travel in Europe, Africa, and the Middle East

1974–5: worked for Ferranti as a development engineer on inertial navigation

4 Education, qualifications and awards

2022: Doctor Honoris Causa, Masaryk University, Brno

2021: Kristian Beckman award, IFIP

2016: Lovelace medal (the top UK award in computing)

2016: Electronic Frontier Foundation Pioneer Award

2015: ACM SIGSAC Outstanding Innovation Award

2012: Louis D. Brandeis Privacy Award

2009: Fellow, Royal Society

2009: Fellow, Royal Academy of Engineering

2009: Fellow, Institute of Physics

2000: Fellow, IEE (now IET)

1995: PhD, University of Cambridge

1994: Member, IEE; Chartered Engineer

1993: Fellow, IMA; Chartered Mathematician

1987: Member, Institute of Bankers (lapsed)

1974–8: BA, Trinity College, Cambridge; part II Mathematics, part II History and Philosophy of Science (converted to MA, 1982)

1976: CEI part II in computer engineering; AMIEE

1973: Higher grade maths, physics, chemistry, biology, geography, english, french, german, latin; High School of Glasgow

5 Appointments and editorships

Foundation for Information Policy Research, *Chair*, since 1998; `http://www.fipr.org`

Chair: Workshop on Security and Human Behaviour 2008–2010 and 2013–4, 2017 and 2020–21; Workshop on Economics and Information Security, 2002 and 2006; Computer Security Applications Conference (European Co-Chair), 2000 and 2001; Eurocrypt 99 (rump session); Scrambling for Safety, 1998; Workshop on Personal Information, Isaac Newton Institute, Cambridge, June 1996 [38]; Workshop on Information Hiding, Isaac Newton Institute, Cambridge, May-June 1996 [39]; Workshop on Fast Software Encryption, Cambridge, December 1993 [9]

Program Committee Member: SaTML 23-4; Workshop on Economics and Information Security, 2002–24; SHB 2008–24; Usenix Sexurity 2023; Financial Cryptography 2009–2021; GameSec 2012–6; Decepticon 2015; WISCS 2015; ACM CCS 2014; USEC 2014; SOUPS 2006, 2011 and 2013; NDSS 2012; Laser 2012; Information Hiding 1996–2012; FOCI 2011; ACM Electronic Commerce 2000, 2004, 2006 and 2010; Oakland (IEEE Computer Society Symposium on Security and Privacy), 1994–5, 2002 and 2009; ESORICS 2002, 2005 and 2007; ESCAR 2005–7; USEC 2007; Workshop on the Economics of Securing the Information Infrastructure 2006; CHES 2001, 2003 and 2005; SIGCOMM 2003; Fast Software Encryption 1993–2007; IPT-PWS 2002; RSA 2001; ACISP 2001; Asiacrypt 1996 and 2000; ICICS 99; EICAR 99; Usenix Electronic Commerce 96–8; Mednet 97; Crypto 95; Cryptography Policy and Algorithms 95; Cardis 94.

World Economic Forum: Member, Global Agenda Council on the Future of the Internet (2008–2012)

Visiting Professor: CMU Cylab; 2011; Rukmini Gopalakrishnan Chair, India Institute of Science, 2009; UC Berkeley, 2001–2; MIT, 2002; Queensland University of Technology, July 1995

Distinguished / Keynote / Invited Speaker: NATO CyCon 23; Ruhrsec 23; Cybersecurity@CEPS Summit 2022; Digitalize 2022; LangSec 22; DLD Summer 22; ICISC 2022; USEC 2022; IFIP SEC 2021; ACNS 2021; MIT Dertouzos Lecture, 2021; Remote Chaos Experience 2020; Chaos Communications Congress 2019; Safecomp 2019; 2018; Information Hiding 2018; CCS Asia 2017; ACM CCS 2016; Royal

Institute of Navigation 2016; EISIC 2015; Information Security for the Public Sector, Stockholm 2015; Crossing 2015; eHelse 2015; Sackler Forum 2014; Black Hat 2014; Cathie Marsh Lecture, Royal Statistical Society, 2014; Annual Privacy Lecture, Berkeley Law School 2014; Financial Crypto 2014; ESSoS 2014; DIVMA 2014; Technion 2013; NADPO 2013; EST 2013; USEC/WESCSR 2012; ACSAC 2012; Amsterdam Privacy Conference 2012; Obradoiro de Criptografia, Privacidade e seguridade 2012; Payment Systems Economics 2012; Indocrypt 2011; Govcert 2011; ETAPS 2011; ESORICS 2011; AusCERT 2011; CMU Cylab 2011; DHS/SRI ITTC 2011; OII 2011; Visions of Computer Science, Academy of Computer Science, Edinburgh 2010; Plenary lecture, Federal Reserve Conference on the Economics of Payments, 2010; IET Prestige Lecture, 2010; Centenary lecture, India Institute of Science, Bangalore, 2009; OWASP 2009; De Montfort STRL Annual Distinguished Seminar 2009; Wisec 2009; UK Unix User Group 2009; International Symposium on Resilient Control Systems 2009; SCADA Security Scientific Symposium 2009; ITU Telecom World 2009; SOUPS 2008; DEON'08; All Hands e-Science Conference 2008; TTeC (Tromso Telemedicine and e-Health Conference) 2008; Gartner IT Security Summit 2008; Crypto 2007; IFIP SEC 2007; Federal Reserve Santa Fe Conference 2007; IDC Security Conference 2007; Softint 2007; University of Edinburgh 2006; Science, Technology and Society 2006; EMIS NUG 2006; Networkshop 2006; University of Washington 2005; ISSE 2005; Science and Society 2005; Body Sensor Networks 2005; 3rd DRM Conference, 2005; IST 2004; Wizards of OS 2004; NITES 2004; Principles of Distributed Computing, 2003; J. Barkley Rosser Memorial Lecture, University of Wisconsin, 2002; IFIP 2002; Economics of Open Source Software, 2002; Symposium on Operating System Principles, 2001; CHES 2001; MIT Distinguished Lecture Series, 2000; Carnegie Mellon University, 1999; Applications Security, 1999; Symposium für Datenschutz und Datensicherheit, 1998; ACM Conference on Computer and Communications Security, 1997; Royal Dutch Medical Association, 1997; HealthCare 96; Securicom 1995; and the Cryptography Policy and Algorithms Conference, Brisbane, 1995. Invited seminar talks include ETH Zürich and the Universities of Michigan, Frankfurt, Århus, Twente, York and Newcastle; the National Physical Laboratory; the Centrum voor Wiskunde en Informatik, Amsterdam; SRI, California; Microsoft Inc., Seattle; Dansk Dataforening, Copenhagen; and the Ecole Normale Supérieure, Paris.

Royal Society Committees: sectional committee 4, 2012–5

House of Commons: Special adviser to the Health Committee Inquiry into the Electronic Patient Record, 2007

Isaac Newton Institute: *Principal Organiser*, research programme on Computer Security, Cryptology and Coding Theory, January – June 1996

Computer and Communications Security Reviews, *Editor-in-Chief, 1998-9; Editor, 1992-98*. I founded this in 1992 and sold it in 1998

References

[1] "Fast cryptogenerator" (with K Lockstone), *UK patent application no. 8606842*, March 1986

[2] "Building a Mainframe Security Module", in *Proc. Infosec 89*, pp 75–87

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

[4] "Tree Functions and Cipher Systems", in *Cryptologia* vol XV no 3 (July 1991) pp 194–202

[5] "An Attack on Server Assisted Authentication Protocols" in *Electronics Letters* vol 28 (16 July 1992) p 1473

[6] "UEPS – a Second Generation Electronic Wallet" in *Computer Security – ESORICS 92*, Springer LNCS vol 648 pp 411–418

[7] "Fast Attack on Certain Stream Ciphers", *Electronics Letters* vol 29 (22 July 93) pp 1322–1323

[8] "A practical RSA trapdoor", in *Electronics Letters* vol 29 no 11 (1993) p 995

[9] *'Fast Software Encryption'* Springer LNCS vol 809, 1993 (*editor*)

[10] "Why Cryptosystems Fail", in *Proceedings of 1993 ACM Conference on Cryptology and Computer Security* pp 215–227

[11] "The Classification of Hash Functions", in *Codes and Cyphers – Cryptography and Coding 4* (Proceedings of IMA Conference on Cryptography and Coding, Cirencester 93), ed. P Farrell (IMA, 1995) pp 83–93

[12] "Why Cryptosystems Fail" in *Communications of the ACM* vol 37 no 11 (November 1994) pp 32–40

[13] "Fortifying key negotiation schemes with poorly chosen passwords" (with TMA Lomas), in *Electronics Letters* vol 30 (23 June 1994) pp 1040–1041

[14] "Robustness principles for public key protocols" (with RM Needham), in *Advances in Cryptology – Crypto 95* Springer LNCS vol 963 pp 236–247

[15] "Searching for the Optimum Correlation Attack", in *'Fast Software Encryption'* (1994), Springer LNCS vol 1008 pp 137–143

[16] "Making Smartcard Systems Robust", in *Proceedings of Cardis 94* (Lille, October 1994) pp 1–14

[17] "Liability and Computer Security – Nine Principles", in *Computer Security – ESORICS 94*, Springer LNCS vol 875 pp 231–245

[18] "Cryptographic Credit Control in Prepayment Metering Systems" (with SJ Bezuidenhout), in *Proceedings of the 1995 IEEE Symposium on Security and Privacy* pp 15–23

[19] "On Fibonacci Keystream Generators", in *'Fast Software Encryption'* (1994), Springer LNCS vol 1008 pp 346–352

[20] *'Robust Computer Security'*, PhD Thesis, University of Cambridge

[21] "Programming Satan's Computer" (with RM Needham) in *'Computer Science Today'*, commemorative issue of Springer Lecture Notes in Computer Science (vol 1000, 1995) pp 426–441

[22] "Crypto in Europe – Markets, Law and Policy", in *Cryptography: Policy and Algorithms* (1995), Springer LNCS vol 1029 pp 75–89

[23] "NHS-wide networking and patient confidentiality", in *British Medical Journal* vol 311 no 6996 (1 July 1995) pp 5–6

[24] "Clinical System Security – Interim Guidelines", in *British Medical Journal* vol 312 no 7023 (13th January 1996) pp 109–111

[25] *'Security in Clinical Information Systems'*, published by the BMA (11th January 1996)

[26] "Tiger: A Fast New Hash Function", (with E Biham) in *'Fast Software Encryption'* (1996), Springer LNCS vol 1039 pp 89–97

[27] "Two Practical and Provably Secure Block Ciphers: BEAR and LION", (with E Biham) in *'Fast Software Encryption'* (1996), Springer LNCS vol 1039 pp 113–120

[28] "NetCard - A Practical Electronic Cash Scheme" (with C Manifavas and C Sutherland), in *Security Protocols* (1996), Springer LNCS vol 1189 pp 49–57

[29] "Patient Confidentiality – At Risk from NHS Wide Networking", in *Proceedings of HealthCare 96*

[30] "On the Reliability of Electronic Payment Systems", (with SJ Bezuidenhoudt) in *IEEE Transactions on Software Engineering* vol 22 no 5 (May 1996) pp 294–301

[31] "A Security Policy Model for Clinical Information Systems", in *Proceedings of the 1996 IEEE Symposium on Security and Privacy* pp 30–43

[32] "Stretching the Limits of Steganography", in *Information Hiding – First International Workshop* (Cambridge, May/June 96), Springer LNCS vol 1174 pp 39–47

[33] "The Newton Channel" (with S Vaudenay, B Preneel and K Nyberg), in *Information Hiding – First International Workshop* (Cambridge, May/June 96), Springer LNCS vol 1174 pp 151–156

[34] "The design of future pre-payment systems" (with SJ Bezuidenhout, N Pattinson and D Taylor), in *Proceedings of 8th IEE Metering and Tariffs for Electricity Supply (MATES)*, Brighton, 3–5 July 1996; IEE Conference Publication No. 426 (ISSN 0537-9989) pp 119–123

[35] "The Eternity Service", in *Proceedings of Pragocrypt 96* (GC UCMP, ISBN 80-01-01502-5) pp 242–252

[36] "An Update on the BMA Security Policy", in *'Personal Medical Information – Security, Engineering and Ethics'* ([40] below) pp 233–250

[37] "Tamper Resistance – a Cautionary Note" (with MG Kuhn), in *Proceedings of the Second Usenix Workshop on Electronic Commerce* (Nov 96) pp 1–11 *best paper award*

[38] *'Information Hiding – First International Workshop'*, May 30 – June 1 1996; sponsored by the Isaac Newton Institute; proceedings published by Springer as LNCS vol 1174 (*editor*)

[39] *'Personal Medical Information – Security, Engineering and Ethics'*, June 21–22 1996; sponsored by the BMA and the Isaac Newton Institute; proceedings published by Springer in July 1997 as ISBN 3-540-63244-1 (*editor*)

[40] “Minding your p’s and q’s” (with S Vaudenay) in *Advances in Cryptology – Asiacrypt 96*, Springer LNCS vol 1163 pp 26–35

[41] “Low Cost Attacks on Tamper Resistant Devices” (with MG Kuhn) in *Security Protocols – Proceedings of the 5th International Workshop* (1997) Springer LNCS vol 1361 pp 125–136

[42] “Chameleon – A New Kind of Stream Cipher” (with C Manifavas) in *‘Fast Software Encryption’* (1997), Springer LNCS v 1267 pp 107–113

[43] “The GCHQ Protocol and Its Problems” (with MR Roe) in *Advances in Cryptology – Eurocrypt 97* Springer LNCS vol 1233 pp 134–148

[44] “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption” (with H Abelson, SM Bellovin, J Benaloh, M Blaze, W Diffie, J Gilmore, PG Neumann, RL Rivest, JI Schiller, B Schneier) in *World Wide Web Journal* v 2 no 3 (Summer 1997) pp 241–257; submitted as testimony to the US senate and to House of Commons Trade and Industry Select Committee

[45] “The Formal Verification of a Payment System”, chapter in *Industrial Strength Formal Methods*, edited by Mike Hinchey and Jonathan Bowen, Academic Press 1999 ISBN: 1-85233-640-4, pp 43-52

[46] “Secure Books: Protecting the Distribution of Knowledge” (with V Matyas, F Petitcolas, I Buchan and R Hanka), in *Security Protocols – Proceedings of the 5th International Workshop* (1997), Springer LNCS vol 1361 pp 1–11

[47] “Eine klare Sicherheitspolitik für klinische Informationssysteme” (with A von Heydwolff), in *Datenschutz und Datensicherheit* vol 21 no 10 (Oct 97) pp 569–574

[48] *‘The Global Trust Register’* (with B Crispo, JH Lee, C Manifavas, V Matyás and FAP Petitcolas), published by Northgate Consultants, February 1998 (ISBN 0-9532397-0-5); 1999 edition published by MIT Press (ISBN 0-262-51105-3)

[49] “On The Limits of Steganography” (with F Petitcolas), *in the IEEE Journal on Selected Areas in Communications, May 1998 – [57] below*, v 16 no 4, pp 474–481

[50] “Attacks on Copyright Marking Systems” (with F Petitcolas and MG Kuhn), in *Proceedings of the Second International Workshop on Information Hiding* (Portland, Apr 98), Springer LNCS vol 1525 pp 219–239

[51] “Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations”, (with MG Kuhn) in *Proceedings of the Second International Workshop on Information Hiding* (Portland, Apr 98), Springer LNCS vol 1525 pp 126–143

[52] “The Steganographic File System” (with RM Needham and A Shamir), in *Proceedings of the Second International Workshop on Information Hiding* (Portland, Apr 98) Springer LNCS vol 1525 pp 74–84

[53] “Safety and Privacy in Clinical Information Systems”, in *‘Rethinking IT and Health’*, J Lenaghan *(ed.)*, IPPR (Nov 98) (ISBN 1-86030-077-4) pp 140–160

[54] “Serpent: A New Block Cipher Proposal” (with E Biham and LR Knudsen), in *Fast Software Encryption – proceedings of fifth international workshop* (1998), Springer LNCS vol 1372 pp 222–238

[55] *'IEEE Journal on Selected Areas in Communications'*, v 16 no 4 (May 1998) *joint editor*

[56] "On the Security of Digital Tachographs", in *Computer Security – ESORICS 98*, Springer LNCS vol 1485 pp 111–125

[57] "The Systematic Construction of Secret Sharing Schemes with Sparse Access Structures" (with CS Ding, T Helleseth and T Kløve), *in 'Designs, Codes and Cryptography'* v 15 no 2 (Nov 1998) pp 111–124

[58] "A New Family of Authentication Protocols" (with F Bergadano, B Crispo, JH Lee, C Manifavas and R Needham), in *Operating Systems Review* v 32 no 4 (Oct 1998) pp 9–20

[59] "Serpent: A Proposal for the Advanced Encryption Standard" (with E Biham and LR Knudsen), submitted to NIST as an AES candidate; a short version of the paper appeared at the AES conference, August 1998; both papers available at `http://www.cl.cam.ac.uk/~rja14/serpent.html`

[60] "Serpent and Smartcards" (with E Biham and LR Knudsen), *in the pre-proceedings of Cardis 98*; available at `http://www.cl.cam.ac.uk/~rja14/serpent.html`

[61] "The DeCODE Proposal for an Icelandic Health Database", produced for the Icelandic Medical Association; part of this was published in *Læknablaðið (The Icelandic Medical Journal)* v 84 no 11 (Nov 98) pp 874–5; full text available from `http://www.cl.cam.ac.uk/users/rja14/#Med`

[62] "The Eternal Resource Locator: An Alternative Means of Establishing Trust on the World Wide Web" (with FAP Petitcolas and VM Matyas) in *Proceedings of the Third USENIX Workshop on Electronic Commerce* pp 141–153

[63] "The Use of Information Retrieval Techniques for Intrusion Detection" (with A Khattak), at *'Recent Advances in Intrusion Detection'*, Louvain-la-Neuve, Sep 98

[64] *'Health Informatics Journal'* v 4 no 3/4 (December 1998) *guest editor*

[65] *'Signature Directive Consultation'* (with C Bowden), result of a consultation exercise carried out by the Foundation for Information Policy Research (FIPR) at the request of the European Commission, on the EU Draft Directive on Electronic Signatures (COM1998 297 final); full text available from `http://www.cl.cam.ac.uk/users/rja14/signaturedoc.html`

[66] "Software Piracy Detector Sensing Electromagnetic Computer Emanations" (with MG Kuhn), UK patent no GB 2,330,924B, granted 6 August 2003, filed 29 October 1997

[67] "Low Cost Countermeasures Against Compromising Electromagnetic Computer Emanations" (with MG Kuhn), UK patent no GB 2333883, granted October 2003; US patent application pending

[68] "Safety and privacy in clinical systems: the state of play", in [64] pp 121–123

[69] "Information technology in medical practice: safety and privacy lessons from the United Kingdom", in *Medical Journal of Australia* v 170 (15/2/99) pp 181–184

[70] "Jikzi: A New Framework for Secure Publishing", with JH Lee, in *Security Protocols – 7th International Workshop* (1999), Springer LNCS v 1796 pp 21–47

[71] "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", with F Stajano, in *Security Protocols – 7th International Workshop* (1999), Springer LNCS v 1796 pp 172–194

[72] "Evaluation of Copyright Marking Systems", (with FAP Petitcolas), in *Proceedings of IEEE International Conference on Multimedia Computing & Systems, vol. 1* (7-11 June 1999, Florence, Italy) pp 574–579

[73] "Information Hiding – A Survey" (with F Petitcolas and MG Kuhn), in *Proceedings of the IEEE* v 87 no 7 (July 1999) pp 1062–1077

[74] "Murphy's law, the fitness of evolving species, and the limits of software reliability" (with RM Brady and RC Ball), Computer Laboratory Technical Report no. 471 (September 1999)

[75] "Soft Tempest – An Opportunity for NATO" (with MG Kuhn), at *Protecting NATO Information Systems in the 21st century*, NATO RTO-MP-27 AC/323(IST)TP/3 pp 5.1–5.5

[76] "The Cocaine Auction Protocol: On the Power of Anonymous Broadcast" (with F Stajano), in *Information Hiding – Third International Workshop* (1999), Springer LNCS v 1768 pp 434–447

[77] "How to Cheat at the Lottery", *Proceedings of the Fifteenth Computer Security Applications Conference* (1999) pp xix–xvii

[78] "The Case for Serpent" (with Eli Biham and Lars Knudsen), at Third AES Conference (2000)

[79] *'The Memorability and Security of Passwords – Some Empirical Results'* (with Jianxin Yan, Alan Blackwell and Alastair Grant), Cambridge University Computer Laboratory Technical Report 500 (2000)

[80] "The Correctness of Crypto Transaction Sets", in *Proceedings of Protocols 2000*, Springer LNCS vol 2133 pp 125–141

[81] "The Grenade Timer" (with F Stajano), at *7th International Workshop on Multimedia Mobile Communications* (MoMoC) (Tokyo, October 2000)

[82] "Jikzi: A New Framework for Security Policy, Trusted Publishing and Electronic Commerce" (with JH Lee), in *Computer Communications* v 23 no 17 (1/11/2000) pp 1621–1626

[83] "Digital Signature", reference section in *Encyclopaedia of Computer Science*, Fourth Edition, Nature Publishing Group (2000) ISBN 1-561-59248-X pp 581–583

[84] "The XenoService - A Distributed Defeat for Distributed Denial of Service" (with JX Yan, S Early); presented at Information Survivability Workshop, Oct 2000, Boston

[85] "Security Policies" (with F Stajano and JH Lee), in *Advances in Computers* v 55 pp 185–235 (2001)

[86] "Improving Smartcard Security using Self-timed Circuit Technology" (with Simon Moore, Markus Kuhn); presented at Fourth ACiD-WG Workshop, Grenoble, ISBN 2-913329-44-6, 2000

[87] "Undermining data privacy in health information", in British Medical Journal v 322 (24 February 2001) pp 442-443

[88] *'Security Engineering – A Guide to Building Dependable Distributed Systems'* Wiley (March 2001), ISBN 0-471-38922-6

[89] "API-Level Attacks on Embedded Systems" (with Mike Bond), in *IEEE Computer* v 34 no 10 (October 2001) pp 67-75

[90] "Why Information Security is Hard – An Economic Perspective", in *Proceedings of the Seventeenth Computer Security Applications Conference* IEEE Computer Society Press (2001), ISBN 0-7695-1405-7, pp 358–365; also given as a distinguished lecture at the Symposium on Operating Systems Principles, Banff, October 2001; received ACSAC Test of Time paper award as the conference's highest-cited paper ever, 2019

[91] "The Resurrecting Duckling: Security Issues for Ubiquitous Computing", with Frank Stajano; in *IEEE Computer* Security and Privacy inaugural issue – supplement to v 35 no 4 (April 2002) pp 22–26

[92] "Improving Smart Card Security using Self-timed Circuits" (with Simon Moore, Paul Cunningham, Robert Mullins and George Taylor), at Asynch 2002 *best presentation award*

[93] "Two Remarks on Public Key Cryptography", writes up ideas of forward security presented at an invited talk, ACM CCS, Zürich, April 1997; now available as Computer Laboratory Technical report no. 549

[94] "Unsettling Parallels Between Security and the Environment", at Workshop on Economics and Information Security 2002, at `http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/`

[95] "Optical Fault Induction Attacks" (with S Skorogbogatov), in *Cryptographic Hardware and Embedded Systems 2002*, Springer LNCS vol 2523 pp 2–12, at `http://www.cl.cam.ac.uk/~rja14/Papers/faultpap3.pdf`

[96] "Security in Open Versus Closed Systems – the Dance of Boltzmann, Coase and Moore", at Open Source Software Economics 2002

[97] "On a New Way to Read Data from Memory" (with D Samyde, S Skorogbogatov and JJ Quisquater), in proceedings of first IEEE Security in Storage Workshop, at `http://www.cl.cam.ac.uk/~rja14/Papers/SISW02.pdf`

[98] "Balanced Self-Checking Asynchronous Logic for Smart Card Applications" (with Simon Moore, Robert Mullins, George Taylor and Jacques Fournier), in *Microprocessors and Microsystems Journal*, v 27 no 9 (Oct 2003) pp 421–430

[99] "Security in a digital repository" (with Richard Clayton and Ellis Weinberger), National Preservation Office Journal issue 11, October 2002, pp 12–13

[100] "TCPA / Palladium Frequently Asked Questions", in *Computer Security Journal* v 18 no 3–4, Summer/Fall 2002, pp 63–70; and at `http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html`

[101] "Trusted Computing' and Competition Policy – Issues for Computing Professionals", in Upgrade v 4 no 3 (June 2003) pp 35–41; at `http://www.upgrade-cepis.org/issues/2003/3/upgrade-vIV-3.html`

[102] "Protocol Analysis, Composability and Computation" (with Mike Bond), in *Computer Systems: Papers for Roger Needham*, Microsoft Research, Feb 2003, pp 7–10; published as *Computer Systems: Theory, Technology and Applications*, Springer 2003.

[103] "Cryptography and Competition Policy – Issues with 'Trusted Computing' ", at Workshop on Economics and Information Security 2003; also given as the Caroline and Edward Wenk Jr. Lecture in Technology and Public Policy, Johns Hopkins University, 2003; at `http://www.cl.cam.ac.uk/~rja14/Papers/tcpa.pdf`

[104] "The Dancing Bear - A New Way of Composing Ciphers", in *Security Protocols – 12th International Workshop*, Cambridge, UK, 26–28 April 2004; Springer LNCS v 3957 pp 231–238

[105] "The Economics of Censorship Resistance" (with George Danezis), at Workshop on Economics of Information Security, Minneapolis, Mn., 13–14 May 2004; journal version in *IEEE Security & Privacy* v 3 no 1 (2005) pp 45–50 as "The Economics of Resisting Censorship"

[106] "On Dealing with Adversaries Fairly" (with Andrei Serjantov), at Workshop on Economics of Information Security, Minneapolis, Mn., 13–14 May 2004

[107] "Cryptography and Competition Policy" (book chapter version of [103]) in *Economics of Information Security*, ed. LJ Camp, S Lewis, Kluwer 2004, pp 35–52

[108] "Key Infection: Smart Trust for Smart Dust" (with Haowen Chan and Adrian Perrig), at ICNP, Berlin, Germany, 5–8 October 2004 pp 206–215

[109] "Password Memorability and Security: Empirical Results" (with Jianxin Yan, Alan Blackwell and Alastair Grant), journal version of [79], in IEEE Security & Privacy, Sep–Oct 2004 pp 25–29

[110] *'EDRI, FIPR and VOSN response to the European commission consultation on the review of the "acquis communautaire" in the field of copyright and related rights* (with Teresa Hackett), October 2004

[111] "User Interface for a Computing Device" (with Alan Blackwell, Jon Crowcroft and Steven Murdoch), UK Patent Application 0426818.1, 7 December 2004

[112] *'Response to EU consultation on review of copyright law'* (with Teresa Hackett and Volker Grassmuck), EDRI 2004; at `http://www.edri.org/campaigns/copyright`

[113] "Chip and Spin" (with Mike Bond and Steven Murdoch), in *Computer Security Journal* v 22 no 2 (2006) pp 1–6, at `http://www.chipandspin.co.uk`

[114] "System Security for Cyborgs", in *Second International Workshop on Body Sensor Networks*, April 12-13 2005, pp 36-39

[115] "The Initial Costs and Maintenance Costs of Protocols", in *Security Protocols Workshop* 2005 Springer LNCS v 4631 pp 333–343

[116] "How Much is Location Privacy Worth?" (with George Danezis and Stephen Murdoch), at *Workshop on Economics of Information Security* 2005; also at `http://www.spiked-online.com/articles/0000000CAC3F.htm`

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

[118] "The Topology of Covert Conflict" (with Shishir Nagaraja), Computer Laboratory Technical Report no. 637 (July 2005); also at *Workshop on Economics of Information Security* (June 2006)

[119] "Combining cryptography with biometrics effectively" (with Feng Hao and John Daugman), Computer Laboratory Technical Report no. 640 (July 2005)

[120] "Robbing the bank with a theorem prover" (with Paul Youn, Ben Adida, Mike Bond, Jolyon Clulow, Jonathan Herzog, Amerson Lin and Ron Rivest), Computer Laboratory Technical Report no. 644 (August 2005); also at *Security Protocols 2007*, Springer LNCS v 5964 (2011) pp 171–177

[121] "Sybil-Resistant DHT Routing" (with George Danezis, Chris Lesneiwski-Laas and Frans Kaashoek), in ESORICS 2005, Springer LNCS vol 3769 pp 305–318

[122] "Cryptographic processors – a survey" (with Mike Bond, Jolyon Clulow and Sergei Skorobogatov), Computer Laboratory Technical Report no. 641 (July 2005), shortened version in *Proc. IEEE* v 94 no 2 (Feb 2006) pp 357–369

[123] "The Memorability and Security of Passwords" (with Jianxin Yan, Alan Blackwell and Alastair Grant), book chapter version of [79], in *'Security and Usability'*, O'Reilly (2005) pp 129–142

[124] "Trends in Security Economics" (with Tyler Moore) in *European Network and Information Security Agency Quarterly* v 1 no 3 (Dec 2005) pp 6–7

[125] "Phish and Chips" (with Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Steven Murdoch and Ron Rivest), at *Security Protocols Workshop*, Mar 2006, Springer LNCS vol 5087 pp 40–48

[126] "The Man-in-the-Middle Defence", with Mike Bond, at *Security Protocols Workshop*, Mar 2006 Springer LNCS vol 5087 pp 153–163

[127] "Combining cryptography with biometrics effectively" (with Feng Hao and John Daugman), in *IEEE Transactions on Computers* vol 55 no 9 (Sep 2006) pp 1081–1088

[128] "Protecting Domestic Power-line Communications" (with Richard Newman, Sherman Gavette and Larry Yonge), in *Symposium On Usable Privacy and Security*, CMU (July 12–14) 2006 pp 122–132

[129] "Healthcare IT in Europe and North America", *National Audit Office*, 2006

[130] *'FIPR Response to the Home Office: "Consultation on the Revised Statutory Code for Acquisition and Disclosure of Communications Data – Chapter II of Part I of the Regulation of Investigatory Powers Act 2000" '* (with Richard Clayton), September 2006

[131] *'FIPR Response to the Home Office: "Consultation on the Revised Statutory Code for Acquisition and Disclosure of Communications Data – Part III of the Regulation of Investigatory Powers Act 2000" '* (with Richard Clayton), September 2006

[132] *'FIPR Consultation Response on "New Powers Against Organised and Financial Crime" '*, October 2006

[133] *'FIPR Consultation Response on "Personal Internet Security '*, October 2006

[134] "The Economics of Information Security" (with Tyler Moore), in *Science* v 314 no 5799 (27 October 2006) pp 610–613

[135] *'Children's Databases – Safety and Privacy'* (with Ian Brown, Richard Clayton, Terri Dowty, Douwe Korff and Eileen Munro), Information Commissioner's Office, November 2006

[136] "Under threat: patient confidentiality and NHS computing", in *Drugs and Alcohol Today* v 6 no 4 (Dec 2006) pp 13–17

[137] "The Economics of Information Security – A Survey and Open Questions" (with Tyler Moore), at Softint 2007 (Jan 19–20, Toulouse); at `http://www.cl.cam.ac.uk/~rja14/Papers/toulouse-summary.pdf`

[138] "HomePlug AV Security Mechanisms" (with Richard Newman, Sherman Gavette and Larry Yonge), in *ISPLC 2007* pp 366–371

[139] "RFID and the Middleman", in *Proceedings of the Eleventh International Conference on Financial Cryptography and Data Security*, February 2007, Springer LNCS v 4886 pp 46–49

[140] *'FIPR Consultation Response on "Framework for Information Assurance" '*, March 2007

[141] *'FIPR Consultation Response on "The Electronic Patient Record and its Use" '* (with Ian Brown, Douwe Korff, and Fleur Fisher), March 2007

[142] "On the Security of the on EMV Secure Messaging API" (with Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin and Ron Rivest), at *Security Protocols 2007*, Springer LNCS v 5964 pp 147–151

[143] "Closing the Phishing Hole – Fraud, Risk and Nonbanks", at *Nonbanks in the Payment System*, Santa Fe, NM, May 2007

[144] "New Strategies for Revocation in Ad-Hoc Networks" (with Tyler Moore, Jolyon Clulow and Shishir Nagaraja), in *ESAS 2007*, Springer LNCS 4572 pp 232–246 (best paper award)

[145] "Information Security Economics – and Beyond" (with Tyler Moore), in *Advances in Cryptology – Crypto 2007*, Springer LNCS 4622, pp 68–91

[146] "Incentives and Information Security" (with Tyler Moore, Shishir Nagaraja and Andy Ozment), *Algorithmic Mechanism Design*, CUP 2007, pp 633–649

[147] "Shifting Borders" (with Steven Murdoch), in *Index on Censorship*, December 2007

[148] "Dynamic topologies for robust and scale-free networks" (with Shishir Nagaraja), in *Bio-inspired Computing and Communication* (2007), Springer LNCS v 5151 pp 411–426

[149] "Tools and Technology of Internet Filtering" (with Steven Murdoch), in *Access Denied*, MIT Press (2008) pp 57–72

[150] *FIPR Submission to The Hunt Review of the Financial Ombudsman Service'* (with Nicholas Bohm), January 2008

[151] "Patient Confidentiality and Central Databases", in *British Journal of General Practice* v 58 no 547 (Feb 2008) pp 75–76

[152] *'Consultation response on The Data Sharing Review'* (with Nicholas Bohm, Terri Dowty, Fleur Fisher, Douwe Korff, Eileen Munro and Martyn Thomas), FIPR, Feb 2008

[153] "Thinking inside the box: system-level failures of tamper proofing" (with Saar Drimer and Steven Murdoch), Computer Lab Technical Report UCAM-CL-TR-711; also at 2008 IEEE Symposium on Security and Privacy, pp 281–295; outstanding paper award by IEEE Security & Privacy Magazine

[154] *'Security Economics and the Internal Market'* (with Rainer Böhme, Richard Clayton and Tyler Moore), published by the European Network and Information Security Agency, March 2008, at `http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm`

[155] "Fast exclusion of errant devices from vehicular networks" with Jolyon Clulow, Jean-Pierre Hubaux, Tyler Moore and Panagiotis Papadimitratos, in *Fifth Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks* (SECON 08) pp 135–143

[156] "What Next after Anonymity?" with Steven Murdoch, *Security Protocols Workshop 2008*, Springer LNCS 6615 pp 220–231

[157] *'Security Engineering – A Guide to Building Dependable Distributed Systems'*, Second edition, Wiley (April 2008), ISBN 978-0-470-06852-6

[158] "Security Economics and European Policy", with Rainer Böhme, Richard Clayton and Tyler Moore), *Workshop on the Economics of Information Security* (WEIS 08); shortened version in *ISSE 2008*, Vieweg-Teubner pp 57–76

[159] "Failures on Fraud", in *Speed* vol 3 no 2 (Sep 2008) pp 6–7

[160] "Security Economics and European Policy", (with Rainer Böhme, Richard Clayton and Tyler Moore), shorter version of [158]; in proceedings *Managing Information Risk and the Economics of Security*, Springer 2008 pp 55–80

[161] "Democracy Theatre: Comments on Facebook's Proposed Governance Scheme", (with Joseph Bonneau, Sören Preibusch, Jonathan Anderson and Richard Clayton), submitted to Facebook terms of service consultation, Mar 29 2009, at `http://www.cl.cam.ac.uk/~jcb82/2009-03-29-facebook-comments.pdf`

[162] 'Cambridge University – the Unauthorised History', January 2009, at `http://www.cl.cam.ac.uk/~rja14`

[163] "The Devil's flame-thrower", *Times Higher Education Supplement* Feb 5, 2009

[164] "What's academic freedom anyway?", *Oxford Magazine* Feb 19, 2009

[165] "Optimised to Fail: Card Readers for Online Banking" (with Saar Drimer and Steven Murdoch), *Financial Cryptography and Data Security 09*, Springer LNCS 5628, pp 184–200

[166] *'Database State'* (with Ian Brown, Terri Dowty, William Heath, Philip Inglesant and Angela Sasse), Joseph Rowntree Reform Trust, March 2009

[167] "The snooping dragon: social-malware surveillance of the Tibetan movement" (with Shishir Nagaraja), University of Cambridge technical report UCAM-CL-TR-746, March 2009

[168] "Eight Friends Are Enough: Social Graph Approximation via Public Listings" (with Joseph Bonneau, Jonathan Anderson and Frank Stajano), in *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems* pp 13–18

[169] "The Trust Economy of Brief Encounters", *Security Protocols Workshop 2009*, Springer LNCS v 7028 pp 282–297

[170] "Security Economics and Critical National Infrastructure" (with Shailendra Fuloria), at *Workshop on the Economics of Information Security* (WEIS 09); in *Economics of Information Security and Privacy* (Springer, 2010) pp 55-66

[171] "Information security: where computer science, economics and psychology meet" (with Tyler Moore) in *Philosophical Transactions of the Royal Society A* v 367 no 1898 pp 2717–2727

[172] *'Consultation response on Regulation of Investigatory Powers Act 2000 Consolidating Orders and Codes of Practice'* (with Jim Killock), FIPR and ORG, July 2009

[173] *'Consultation response on Interception Modernisation or "Protecting the Public" '* (with Jim Killock), FIPR and ORG, July 2009

[174] *'Consultation response on Civil Litigation Costs Review'*, FIPR, July 2009

[175] "Certification and Evaluation: A Security Economics Perspective" (with Shailendra Fuloria), at *IEEE Emerging Technologies and Factory Automation* (Sep 2009) pp 1–7

[176] "The Economics of Online Crime" (with Tyler Moore and Richard Clayton) in *Journal of Economic Perspectives* v 23 no 3 (2009) pp 3–20

[177] "Failures of Tamper-Proofing in PIN Entry Devices" (with Saar Drimer and Steven Murdoch), *IEEE Security and Privacy* v 7 no 6 (Nov-Dec 09) pp 39–45 (journal version of [153])

[178] "Verified by VISA and MasterCard SecureCode: or, How Not to Design Authentication" (with Steven Murdoch), at *Financial Cryptography 2010* Springer LNCS 6052 pp 336–342

[179] "It's the Anthropology, Stupid!" (with Frank Stajano), at *Security Protocols Workshop 2010* Springer LNCS 7061 pp 127–141

[180] "Chip and Pin is Broken" (with Steven Murdoch, Saar Drimer and Mike Bond), at *IEEE Symposium on Security and Privacy* (2010) pp 433–444 (outstanding paper award)

[181] "On the Security of Internet Banking in South Korea" (with Hyoungshick Kim and Jun Ho Huh), Oxford University Computer Lab Technical Report RR–10–01, March 2010

[182] "On the security economics of electricity metering" (with Shailendra Fuloria), at *Workshop on the Economics of Information Security* (WEIS 10)

[183] "Key Management for Substations: Symmetric Keys, Public Keys or No Keys?" (with Shailendra Fuloria, Kevin McGrath, Kai Hansen and Fernando Alvarez), at *IEEE Power Systems Conference and Exhibition (PSCE 2010)*

[184] "Who controls the off switch?" (with Shailendra Fuloria), at *IEEE SmartGridComm* (NIST, October 2010)

[185] "Might Financial Cryptography Kill Financial Innovation? – The Curious Case of EMV" (with Mike Bond, Omar Choudary, Steven Murdoch and Frank Stajano), at *Financial Cryptography 2011*, Springer LNCS 7035 pp 220–234

[186] "Can We Fix the Security Economics of Federated Authentication?", at *Security Protocols Workshop 2011* Springer LNCS 7111 pp 25–48

[187] *'Resilience of the Internet Interconnection Ecosystem'* (with Panagiotis Trimintzios, Chris Hall, Richard Clayton and Evangelos Ouzounis), European Network and Information Security Agency, April 2011; abridged version published at WEIS 2011, *Economics of Information Security and Privacy III* (Springer 2013) pp 119–148

[188] "Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research" (with Tyler Moore), Harvard University Computer Science Group technical report TR-03-11, 2011; also published as "Internet Security" in *The Oxford Handbook of the Digital Economy* pp 572–599 (OUP, 2012)

[189] "Towards a security architecture for substations" (with Shailendra Fuloria), *IEEE PES – ISGT Europe* pp 1–6 (2011)

[190] "Centrality prediction in dynamic human contact networks" (with Hyoungshick Kim, John Tang and Cecilia Mascolo), in *Computer Networks* v 56, Special issue on Complex Dynamic Networks: Tools and Methods (2012) pp 983–996

[191] "Temporal node centrality in complex networks" (with Hyoungshick Kim), Phys Rev E v 85 026107 (2012)

[192] "A birthday present every eleven wallets?" (with Joe Bonneau), at *Financial Cryptography 2012* Springer LNCS v 7397 pp 25–40

[193] "Social Authentication – harder than it looks" (with Hyoungshick Kim), at *Financial Cryptography 2012* Springer LNCS v 7397 pp 1–15

[194] "Ethics Committees and IRBs: Boon, or Bane, or More Research Needed?", at *Financial Cryptography 2012* Springer LNCS v 7398 pp 133–5

[195] "Risk and privacy implications of consumer payment innovation", in *Consumer Payment Innovation in the Connected Age*, Kansas City Fed, March 2012, at `https://www.kansascityfed.org/publications/research/pscp/pscp-2012.cfm`

[196] "Measuring the Cost of Cybercrime" (with Chris Barton, Rainer Böhme. Richard Clayton, Michel van Eeten, Michael Levi, Tyler Moore and Stefan Savage), at the *Workshop on the Economics of Information Security* 2012; in *The Economics of Information Security and Privacy* (Springer 2013) pp 265–300

[197] "CHERI: a research platform deconflating hardware virtualization and protection" (with Robert Watson, Peter Neumann, Jonathan Woodruff, Jonathan Anderson, Nirav Dave, Ben Laurie, Simon Moore, Steven Murdoch, Philip Paeps, Michael Roe and Hassen Saidi), at *RESoLVE'12* (Mar 3, 2012)

[198] *Consultation response on 'Making Open Data Real'*, Foundation for Information Policy Research, October 2011, published August 2012

[199] *Consultation response on 'ICO Draft Anonymisation Code of Practice'*, Foundation for Information Policy Research, August 2012

[200] "Aurasium: Practical Policy Enforcement in Android Applications" (with Rubin Xu and Hassen Saidi), at *Usenix 2012*

[201] "How Certification Systems Fail: Lessons from the Ware Report" (with Steven Murdoch and Mike Bond), IEEE Security and Privacy, June 2012 pp 40–44

[202] "Chip and Skim: cloning EMV cards with the pre-play attack"(with Mike Bond, Omar Choudary, Steven Murdoch and Sergei Skorobogatov), *a rXiv:0547955*, Sep 2012

[203] "Smart Metering – Ed Milliband's Poisoned Chalice" (with Alex Henney), submitted to DECC (2012), and at `http://www.lightbluetouchpaper.org`

[204] "Security Economics – A Personal Perspective", *ACSAC 2012* (keynote talk)

[205] "Why quantum computing is hard – and quantum cryptography is not provably secure" (with Robert Brady), *arXiv:1301.7351*, Jan 2013

[206] "Authentication for Resilience: The Case of SDN" (with Dongting Yu, Andrew Moore and Chris Hall), in *Security Protocols Workshop 2013* Springer LNCS 8263 pp 39–53

[207] "An Experimental Evaluation of Robustness of Networks" (with Hyoungshick Kim), in *IEEE Systems Journal – Special Issue on Security and Privacy in Complex Systems* v 7 no 2 (June 2013) pp 179–188

[208] "Violation of Bell's inequality in fluid mechanics" (with Robert Brady, *arXiv:1305.6822*, May 2013

[209] "Rendezvous: A Search Engine for Binary Code" (with Wei-Ming Khoo and Alan Mycroft) at *MSR 2013* pp 329–338

[210] "PIN Skimmer: Inferring PINs Through The Camera and Microphone" (with Laurent Simon), at *Third ACM workshop on Security and Privacy in Smartphones & mobile devices (SPSM 2013)* pp 67–78

[211] "Reading this may harm your computer – The psychology of malware warnings" (with David Modic), *SSRN 2374379* (Jan 3 2014)

[212] "Why bouncing droplets are a pretty good model of quantum mechanics" (with Robert Brady), *arXiv:1401.4356*, Jan 2014

[213] "Security protocols and evidence: where many payment systems fail" (with Steven Murdoch), at *Financial Cryptography 2014*, Springer LNCS 8437 pp 21–32

[214] "Collaborating with the enemy on network management" (with Chris Hall, Dongting Yu, Zhu-Li Zhang, Jonathan Stout, Andrew Odlyzko, Andrew Moore, Jean Camp and Kevin Benton) at *Security Protocols Workshop 2014* Springer LNCS v 8809 pp 154–171

[215] "Chip and Skim: Cloning EMV Cards with the Pre-Play Attack" (with Mike Bond, Omar Choudary, Steven Murdoch and Sergei Skorobogatov) at *IEEE Security and Privacy 2014* (updated version of [202])

[216] "Privacy versus government surveillance – where network effects meet public choice" at *Workshop on the Economics of Information Security 2014*

[217] "Experimental Measurement of Attitudes Regarding Cybercrime" (with James Graves and Alessandro Acquisti), at *Workshop on the Economics of Information Security 2014*

[218] "We Will Make You Like Our Research: The Development of a Susceptibility-to-Persuasion Scale" (with David Modic), *SSRN 2446971* (April 21 2014)

[219] "EMV: Why Payment Systems Fail" (with Steven Murdoch), in *Communications of the ACM* v 57 no 6 (June 2014) pp 24–28

[220] "To freeze or not to freeze – A motion-capture approach to detecting deceit" (with Sophie van der Zee, Ronald Poppe and Paul Taylor), in *Rapid Screening Technologies, Deception Detection and Credibility Assessment Symposium, HICSS 2015*

[221] "Mining Bodily Cues to Deception" (with Ronald Poppe, Sophie van der Zee, Paul Taylor and Remco Veltkamp), in *Rapid Screening Technologies, Deception Detection and Credibility Assessment Symposium, HICSS 2015*; journal version in *Journal of Nonverbal Behavior* 4 Dec 2023

[222] *'The collection, linking and use of data in biomedical research and health care: ethical issues'* (with Martin Richards, Stephen Hinde, Jane Kaye, Anneke Lucassen, Paul Matthews, Michael Parker, Margaret Shotter, Geoff Watts, Susan Wallace and John Wise), Nuffield Bioethics Council, Feb 2015

[223] "Maxwell's fluid model of magnetism" (with Robert Brady), Arxiv 1502.05926

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

[225] "Be Prepared: The EMV Pre-play Attack" (with Mike Bond, Marios Chaudary, Steven Murdoch and Sergei Skorobogatov), in *IEEE Security and Privacy Magazine* (Mar 2015) pp 56–64

[226] "Security Analysis of Factory Resets" (with Laurent Simon), at *Mobile Security Technologies (MoST) 2015*

[227] "Security Analysis of Consumer-Grade Anti-Theft Solutions Provided by Android Mobile Anti-Virus Apps" (with Laurent Simon), at *Mobile Security Technologies (MoST) 2015*

[228] "What goes around comes around", in *Privacy in the Modern Age: The Search for Solutions*, EPIC (2015)

[229] "Do You Believe in Tinker Bell? The Social Externalities of Trust" (with Khaled Baqer), in *Protocols Workshop 2015* Springer LNCS 9379 pp 224–246

[230] "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications" (with Hal Abelson, Steve Bellovin, Josh Benaloh, Matt Blaze, Whit Diffie, John Gilmore, Matt Green, Susan Landau, Peter Neumann, Ron Rivest, Jeff Schiller, Bruce Schneier, Michael Specter and Danny Weitzner), MIT CSAIL Tech Report 2015-026 (July 6, 2015); also in *Journal of Cybersecurity* (2015); abridged version in *Communications of the ACM* v 58 no 10 (Oct 2015) *(winner of JD Falk award)*

[231] "It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud" (with David Modic), *IEEE Security & Privacy* v 13 no 5 (2015) pp 99–103

[232] "Are Payment Card Contracts Unfair?" (with Steven Murdoch, Ingolf Becker, Ruba Abu-Salma, Nicholas Bohm, Alice Hutchings, Angela Sasse, and Gianluca Stringhini), at *Financial Cryptography 2016*, Springer LNCS v 9603 pp 600–608

[233] "SMAPs: Short Message Authentication Protocols" (with Khaled Baqer, Johann Bezuidenhoudt and Markus Kuhn) in *Security Protocols 2016*, Springer LNCS v 10368

[234] "Don't Interrupt Me While I Type: Inferring Text Entered Through Gesture Typing on Android Keyboards" (with Laurent Simon and Wenduan Xu), *PETS 2016*

[235] "When Lying Feels the Right Thing to Do" (with Sophie van der Zee and Ronald Poppe), Frontiers in Psychology, 2 June 2016; reprinted as a chapter in *Dishonest Behavior: From Theory to Practice*, Frontiers in Psychology ebook (2017), edited by Guy Hochman, Shahar Ayal and Dan Ariely, pp 74–86

[236] "Taking Down Websites to Prevent Crime" (with Alice Hutchings and Richard Clayton), APWG eCrime 2016 pp 102–111

[237] "International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms" (with Ingolf Becker, Alice Hutchings, Ruba Abu-Salma, Nicholas Bohm, Steven Murdoch, Angela Sasse and Gianluca Stringhini), at *WEIS 2016*

[238] "Replacing Magic With Mechanism?", in *What do you consider the most interesting recent [scientific] news? What makes it important?*, Edge, 2016; at `https://www.edge.org/response-detail/26757`

[239] "Brexit and technology: How network effects will damage UK IT industry", Computer Weekly, 20 June 2016

[240] "What would Brexit really mean for Cambridge", in *Cambridge News*, 21st June 2016; at `http://www.lightbluetouchpaper.org`

[241] "Apple's Cloud Key Vault, Exceptional Access, and False Equivalences" (with Harold Abelson, Steve Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter Neumann, Ron Rivest, Jeff Schiller, Bruce Schneier, Michael Specter and Daniel J.Weitzner), Lawfare, September 7th 2016

[242] "Hard Newcap or Soft Newcap? A Christmas Fable", 21 Dec 2016, at `http://www.lightbluetouchpaper.org`

[243] "Reconciling Multiple Objectives – Politics or Markets?" (with Khaled Baqer) in *Security Protocols 2017*

[244] "De-Anonymization", in *What scientific term or concept ought to be more widely known?*, Edge, 2017; at `https://www.edge.org/response-detail/27195`

[245] "DigiTally: Piloting Offline Payments for Phones" (with Khaled Baqer, Lorna Mutegi, Jeunese Adrienne Payne and Joseph Sevilla), in the proceedings of the Symposium on Usability and Privacy (SOUPS) 2017, pp 131–143

[246] "Standardisation and Certification of the Internet of Things" (with Eireann Leverett and Richard Clayton), *Workshop on the Economics of Information Security* (2017) – abridged version of [247]

[247] "Standardisation and Certification of Safety, Security and Privacy in the Internet of Things" (with Èireann Leverett and Richard Clayton), European Union (written 2016; dated 2017; actually published 2018), `https://publications.europa.eu/en/publication-detail/-/publication/80bb1618-16bb-11e8-9253-01aa75ed71a1/language-en`

[248] "International comparison of bank fraud reimbursement: customer perceptions and contractual terms" (with Ingolf Becker, Alice Hutchings, Ruba Abu-Salma, Nicholas Bohm, Steven Murdoch, Angela Sasse and Gianluca Stringhini), in *Journal of Cybersecurity* v 3 no 2 (June 2017 – journal version of [237])

[249] "The Threat – A Conversation with Ross Anderson", *Edge*, Oct 25 2017; at `https://www.edge.org/conversation/ross_anderson-the-threat`

[250] "Perception Versus Punishment in Cybercrime" (with Jim Graves and Alessandro Acquisti) in *Journal of Criminal Law and Criminology* v 109 (2019)

[251] "Making Security Sustainable", in *Communications of the ACM* v 61 no 3 (Mar 2018) pp 24–26

[252] "Making Bitcoin Legal" (with Ilia Shumailov and Mansoor Ahmed), in *Security Protocols XXVI, LNCS v 11286* (2018) pp 243–265

[253] "What you get is what you C: controlling side-effects in mainstream C compilers" (with Laurent Simon and David Chisnall), at *IEEE European Symposium on Security and Privacy* (2018)

[254] "We Will Make You Like Our Research: The Development of a Susceptibility-to-Persuasion Scale" (with David Modic and Jussi Palomäki), in *PLOS One* v 13 no 3 (March 15 2018 – journal version of [218])

[255] "Bitcoin Redux" (with Ilia Shumailov, Mansoor Ahmed and Alessandro Rietmann), in *Workshop on the Economics of Information Security* (2018)

[256] "Privacy for Tigers", invited talk at *Usenix Security 2018*, at `https://www.usenix.org/presentation/anderson`

[257] "To compress or not to compress: Understanding the Interactions between Adversarial Attacks and Neural Network Compression" (with Yiren Zhao, Ilia Shumailov and Robert Mullins), *arXiv:1810.00208*, Sep 2018; *SysML 2019*, April 2019

[258] "Letter regarding the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018" (with H Abelson, R Barnes, X Boyen, A Cooper, C Culane, R Gore, B Laurie, PG Neumann, M Nottingham, J Pieprzyk, R Rivest, B Schneier, J Schiller, M Specter, V Teague, Y Yarom, DJ Weitzner), 14 Nov 2018

[259] "The Taboo Trap: Behavioural Detection of Adversarial Samples" (with Ilia Shumailov, Yiren Zhao and Robert Mullins), *arXiv:1811.07375*, Nov 2018

[260] "Tendrils of Crime: Visualizing the Diffusion of Stolen Bitcoins" (with Mansoor Ahmed and Ilia Shumailov), *arXiv:1901.01769*,; in *GramSec 2018*, Springer LNCS v 11086 pp 1–12

[261] "Sitatapatra: Blocking the Transfer of Adversarial Samples" (with Ilia Shumailov, Xitong Gao, Yiren Zhao, Robert Mullins and Cheng-Zhong Xu) *arXiv:1901.08121*, Jan 2019

[262] "Hearing your touch: A new acoustic side channel on smartphones" (with Ilia Shumailov, Laurent Simon and Jeff Yan), *arXiv:1903.11137*, Mar 2019

[263] "To freeze or not to freeze – A culture-sensitive motion capture approach to detecting deceit" (with Sophie van der Zee, Ronald Poppe and Paul Taylor), in *PLOS One* April 12, 2019 (journal version of [220])

[264] "How brain type influences online safety" (with Tyler Moore), at *SHB 2008*, finally put online Apr 2019

[265] "Measuring the Changing Cost of Cybercrime" (with Chris Barton, Rainer Böhme, Richard Clayton, Carlos Gañán, Tom Grasso, Michael Levi, Tyler Moore and Marie Vasek), *Workshop on the Economics of Information Security* 2019

[266] "Snitches Get Stitches: On the Difficulty of Whistleblowing" (with Mansoor Ahmed-Rengers, Darija Halatova and Ilia Shumailov), *Security Protocols Workshop 2019*, Springer LNCS v 12287 pp 289–303

[267] "Blackbox Attacks on Reinforcement Learning Agents Using Approximated Temporal Information" (with Yiren Zhao, Ilia Shumailov, Han Cui, Xitong Gao and Robert Mullins), *arXiv:1909.02918*, Nov 21 2019 and *3rd DSN Workshop on Dependable and Secure Machine Learning* (DSN-DSML'20), June 2020

[268] "Towards Certifiable Adversarial Sample Detection" (with Yiren Zhao, Ilia Shumailov, and Robert Mullins), *arXiv:2002.08740*, Feb 20 2020 and *Artificial Intelligence and Security (AISec 2020)*

[269] "Sponge Examples: Energy-Latency Attacks on Neural Networks" (with Ilia Shumailov, Yiren Zhao, Daniel Bates, Nicolas Papernot and Robert Mullins), *arXiv:2006.03463* Jun 5 2020; *6th IEEE European Symposium on Security and Privacy (EuroS&P 2021)*

[270] "BatNet: Data transmission between smartphones over ultrasound" (with Almos Zarandy and Ilia Shumailov) *arXiv:2008.00136*, Jul 30 2020

[271] "Nudge Attacks on Point-Cloud DNNs" (with Yiren Zhao, Ilia Shumailov and Robert Mullins), *arXiv:2011.11637*, Nov 22 2020

[272] *'Security Engineering – A Guide to Building Dependable Distributed Systems'* (3rd edition), Wiley 2020

[273] "Hey Alexa what did I just type? Decoding smartphone sounds with a voice assistant" (with Almos Zarandy and Ilia Shumailov), *arXiv:2012.00687* Dec 1 2020

[274] "Manipulating SGD with Data Ordering Attacks" (with Ilia Shumailov, Zakhar Shumaylov, Dmitry Kazhdan, Yiren Zhao, Nicolas Papernot and Murat A. Erdogdu), *arXiv:2104.09667* Apr 19 2021, and *Proceedings of the 35th Conference on Neural Information Processing Systems (NIPS 21)*

[275] "Situational Awareness and Machine Learning – Robots, Manners and Stress" (with Ilia Shumailov), preprint, May 2021

[276] "Markpainting: Adversarial Machine Learning meets Inpainting" (with David Khachaturov, Ilia Shumailov, Yiren Zhao and Nicolas Papernot), *arXiv:2106.00660* June 1 2021; and in *Proceedings of the 38th International Conference on Machine Learning* (PMLR) 139:5409-5419

[277] "Bad Characters: Imperceptible NLP Attacks" (with Nicholas Boucher, Ilia Shumailov and Nicolas Papernot), *arXiv:2106.09898* June 17 2021, and *IEEE Symposium on Security and Privacy*, May 2022

[278] "Silicon den: Cybercrime is entrepreneurship" (with Richard Clayton, Rainer Böhme and Ben Collier), *WEIS 2021*, June 28 2021

[279] "Confidentiality in Remote Clinical Practice", International Psychoanalytical Association, 2021

[280] "Bugs in our Pockets: The Risks of Client-Side Scanning" (with Hal Abelson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague and Carmela Troncoso) *arXiv:2110.07450*, Oct 14 2021

[281] "ExtremeBB: Enabling Large-Scale Research into Extremism, the Manosphere and Their Correlation by Online Forum Data" (with Anh V. Vu, Lydia Wilson, Yi Ting Chua and Ilia Shumailov), *arXiv:2111.04479*, Nov 8 2021; appeared at ACL WOAH 2023

[282] "Trojan Source: Invisible Vulnerabilities" (with Nicholas Boucher), *arXiv:2111.00169*, Nov 1 2021

[283] "CoverDrop: Blowing the Whistle Through A News App" (with Mansoor Ahmed-Rengers, Diana A. Vasile, Daniel Hugenroth and Alastair R. Beresford), in *Proceedings on Privacy Enhancing Technologies* (2022) v 2 pp 47–67 (best student paper award)

[284] "Trojan Source and Bad Characters: Invisible Hacks and Reluctant Patching" (with Nicholas Boucher). LangSec 2022 keynote, at `https://www.youtube.com/watch?v=nXCEuHekt-0`

[285] "Attack of the Clones: Measuring the Maintainability, Originality and Security of Bitcoin 'Forks' in the Wild" (with Jusop Choi, Wonseok Choi, William Aiken, Hyoungshick Kim, Jun Ho Huh, Taesoo Kim and Yongdae Kim), 2022, *arxiv:2201.08678*

[286] "Getting Bored of Cyberwar: Exploring the Role of the Cybercrime Underground in the Russia-Ukraine Conflict" (with Anh V. Vu, Daniel R. Thomas, Ben Collier, Alice Hutchings and Richard Clayton), *arxiv:2208.10629*

[287] "PostCog: A Tool for Interdisciplinary Research into Underground Forums at Scale", *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'22)* (with Ildiko Pete, Jack Hughes, Andrew Caines, Anh Viet Vu, Harshad Gupta, Alice Hutchings and Paula Buttery)

[288] "Talking Trojan: Analyzing an Industry-Wide Disclosure" (with Nicholas Boucher), SCORED 2022, *arxiv:2209.10717*

[289] "The Online Safety Bill" (with Sam Gilbert and Diane Coyle), Bennett Institute for Public Policy 2022

[290] "Legislating for Online Safety" (with Sam Gilbert), InterMedia v 50 no 2 (Dec 2022) pp 8–12 (magazine version of [289])

[291] "Chat Control or Child Protection?", 2022 *arXiv:2210.08958*

[292] "ImpNet: Imperceptible and blackbox-undetectable backdoors in compiled neural networks" (with Tim Clifford, Ilia Shumailov, Yiren Zhao and Robert Mullins), 2022, *arxiv.org:2210.00108*

[293] "Threat Models over Space and Time: A Case Study of E2EE Messaging Applications" (with Partha Das Chowdhury, Maria Sameen, Jenny Blessing, Nicholas Boucher, Joseph Gardiner, Tom Burrows and Awais Rashid), *arXiv:2301.05653* and *Security Protocols 2023*

[294] "One Protocol to Rule Them All? On Securing Interoperable Messaging" (with Jenny Blessing), *arXiv:2303.14178* and *Security Protocols 2023*

[295] "A Case Study in Censorship" (with Anh Viet Vu and Alice Hutchings), *Cambridge Cybercrime Centre Briefing Paper, 18 August 2013*

[296] "No Easy Way Out: the Effectiveness of Deplatforming an Extremist Forum to Suppress Hate and Harassment" (with Anh Viet Vu and Alice Hutchings), *arXiv:2304.07037* and *IEEE Symposium on Security and Privacy* (2024)

[297] "Boosting Big Brother: Attacking Search Engines with Encodings" (with Nicholas Boucher, Luca Pajola, Ilia Shumailov, Ross Anderson, and Mauro Conti), *arXiv:2304.14031*; also at RAID 2023 (best paper award)

[298] "If it's Provably Secure, It Probably Isn't: Why Learning from Proof Failure is Hard" (with Nicholas Boucher), *arXiv:2305.04755* and *Security Protocols 2023*

[299] "The Curse of Recursion: Training on Generated Data Makes Models Forget" (with Ilia Shumailov, Zakhar Shumaylov, Yiren Zhao, Yarin Gal and Nicolas Papernot)*arXiv:2305.17493*

[300] 281 "When Vision Fails: Text Attacks Against ViT and OCR" (with Nicholas Boucher, Jenny Blessing, Ilia Shumailov, Ross Anderson, and Nicolas Papernot), *arXiv:2306.07033*

[301] 282 "Machine Learning needs its own Randomness Standard: Randomised Smoothing and PRNG-based attacks" (with Pranav Dahiya and Ilia Shumailov), *arXiv:2306.14043* (acceped at IEEE Security & Privacy 2024)

[302] "Bugs in our Pockets: The Risks of Client-Side Scanning" (with Hal Abelson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague and Carmela Troncoso), *Journal of Cybersecurity* v 10 issue 1, Jan 27 2024, journal version of [281]