Curriculum Vitae – Ross Anderson

I am Professor of Security Engineering at the Computer Laboratory at Cambridge University, and a Fellow of Churchill College. 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.

The focus of my work in academia has been building security engineering into a discipline. Twenty years ago, some tractable parts of it – cryptography, protocols and operating system security – had well-developed 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 a combination of snake-oil and black magic.

Over the last twenty odd years I've started strong research threads in neglected areas, ranging from hardware security to the uses of signal processing. I've also documented the evolution of a number of interesting new applications from ATMs to medical records, which have failure modes from which engineers can learn. In the past fifteen years I've developed security economics as an alternative framework for understanding the subject: very often systems fail not because of some technical mistake but because of misaligned incentives. For example, the people guarding a system are often not the people who suffer when it fails. This work is now spreading into the behavioural economics and psychology of security. I have written a book, *'Security Engineering – A Guide to Building Dependable Distributed Systems'* [88, 157], which is now the standard reference. Along the way I've contributed to the design of a number of widely-deployed systems, from peer-to-peer systems through the STS specification for prepayment utility meters (with 400 million installed) to the HomePlug standard for power-line communications (widely used to extend wifi). This work has been recognised by the Lovelace Medal, the UK's top award in computing.

Security engineering is much broader than 'computer security', and is becoming essential to the safety of cars, medical devices and much else, as well as to privacy and fraud prevention. And as we start doing regular security patches for durable goods, security will become a larger part of the total lifecycle cost; Mercedes can't just refuse to patch the products they sold five years ago the way that Google or Microsoft can. And as crime has moved online, security is moving steadily up the political agenda – along with privacy, surveillance and competition policy.

I chair the Foundation for Information Policy Research and am an elected member of Cambridge University's Council. I also teach undergraduate software and security engineering, a service course in economics, law and ethics for computer scientists, and two graduate courses in security.

Ross Anderson FRS FREng
Julyy 2017

1 Research

1.1 Economics and security

A major achievement has been establishing security economics as a thriving academic discipline. We observed that information insecurity is due to perverse incentives at least as often as to deficient mechanisms: systems typically fail when the people who guard them are not the people who suffer when they fail. But there is more to it than that. Many real problems can be best explained using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons. Although I did some early work in 1993-4 [10, 12], the field really took off only since 2001 [90, 94, 101, 103, 105, 106]. For recent surveys, see [134, 145, 169] and [186]. My most important recent work may have been major studies for the European Commission of the security economics of cyber-crime [154, 160], the resilience of the Internet [185] and what happens to safety regulation once there's software in everything [238]; and a major study of the costs of cybercrime that was originally commissioned by the UK Ministry of Defence [194]. I have other papers on online crime [174], attitudes to online crime [214], and the security economics of critical national infrastructure [168, 173] and surveillance [213]. A long-term project is to grow security economics out through behavioural economics into psychology [177, 186, 190, 191, 208, 214, 215, 217, 218, 224, 226, 230].

1.2 Peer-to-Peer systems and networks

Since 2000, there has been an explosion of interest in peer-to-peer networking – building useful systems out of intermittently connected machines, with virtual infrastructures tailored to the application. I wrote one of the seminal papers, on The Eternity Service [35]. My ideas were taken up by Freenet, Gnutella, Publius, Kazaa and others. Further papers include [58, 62, 70, 71, 76, 82, 84, 105, 106, 108, 121, 224]. I designed the key-management protocols for HomePlug, now deployed in millions of consumer electronic devices [128, 138]. We also looked at social networks where we've discovered all sorts of privacy problems [161, 166].

In a related thread of work, we 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 a number of metrics and other analysis techiques for both static and dynamic networks [118, 121, 144, 155, 148, 200, 188, 189, 204].

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 applied this principle to computer security by studying the failure modes of a number of important distributed systems including ATM and bank card systems [10, 12, 17, 113, 120, 142, 125, 139, 143, 153, 159, 163, 175, 178, 179, 190, 193, 199, 200, 210, 216, 221, 226, 227, 232], prepayment electricity meters [18, 30], medical record systems [23, 29, 61, 68, 69, 129, 136, 151, 219] and digital tachographs [56]. This work follows our laboratory's maxim that 'good research comes from real problems'. It has led to a number of papers in which I try to distil the essence of good security design [6, 14, 16, 21, 25, 31, 36, 47]. One high-impact 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 [165]; another tackled smart grids and smart meters [168, 173, 180, 182, 201]. Recently we've been looking at security vulnerabilities in mobile phones [207, 222, 223, 229] and at ways of extending mobile payments offline [228, 239].

1.4 Cryptographic protocols and APIs

Many of the most interesting technical attacks on security systems fall under the general heading of protocol failure. This includes design flaws in which the wrong things are encrypted, or the right things are encrypted in the wrong way; such flaws are common in practice but rather hard to spot. 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, 228], 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 [181, 182], the interaction between protocols and economics [115, 184], with psychology [177, 190] and the effects on innovation [176, 183, 184, 185].

Perhaps my biggest innovation was API attacks, which extend protocol analysis to the application programming interfaces of cryptographic processors. These devices typically have from dozens of transactions that can be performed using internally protected keys; most of the devices we've looked at could be broken by issuing a suitably chosen sequence of transactions. I initiated this field of research with [80]; further papers can be found at [89, 102, 142, 125, 126] and a survey at [122]. Our work forced many manufacturers to redesign products.

1.5 Hardware tamper-resistance

In 1996, we demolished a popular belief in the tamper-resistance of smartcards: our initial paper on attack techniques [37] won an award and has been very widely cited. Later work on this topic can be found in [41, 122], while in [95, 97] we opened up the fast-growing field of optical security in which laser probing is used to induce revealing faults in semiconductors and to read out memory contents by inducing photocurrents, so that we could bypass the circuits supplied by the chip vendor for that purpose. We investigated whether we could make CPUs much less vulnerable using self-timed dual-rail logic with inbuilt alarm circuitry [86, 92, 98] (you can but it's too fragile to commonly used fabrication toolchains). We've shown that the supposed tamper-resistance of common PIN Entry Devices is unsatisfactory [153, 199]. We've also shown that you can recast decompilation as a search problem [206], which facilitates the analysis of large malware families that differ from each other by small tweaks. We're now applying this know-how to the many versions of IoT botnets.

1.6 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]. I returned to the subject again in the early 1990s [7, 15, 19]; this, plus some work on hash functions [11, 26] led me to find ways to construct block ciphers from hash functions and stream ciphers [27]. My most substantial work 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.

1.7 Signal processing and security

In the late 1990s, I spent some time applying signal processing ideas to computer security. The most novel development was 'Soft Tempest'. It had previously been believed that Tempest protection (preventing opponents from reconstructing information from stray RF emanations from computers) necessarily involved hardware techniques such as metal shielding. We showed that substantial protection can be given using software [51, 75]. We got interested in digital copyright watermarking in 1995 and within a few years we broke essentially all the existing copyright marking schemes [50]. The 'Stirmark' software we wrote became the industry standard for testing marking systems [72] (see also [32, 42, 49, 55], and our survey paper [73]).

1.8 Odds and ends

The main lesson learned from studying real security systems was that most real life failures resulted from the opportunistic exploitation of bugs and blunders. This motivated the study of design assurance. My first paper on the subject provided a rigorous explanation, under quite general assumptions, of why the growth in reliability of large systems in response to testing is often as poor as can possibly be: a software engineer's version of 'Murphy's Law' [74]; this means that testing should be parallelised as much as possible. I conducted an experiment which shows that the same applies in large part to requirements engineering [77]. The most controversial result is a proof that, under standard assumptions, open source and proprietary systems are security equivalent – in the sense that opening up the design helps the attacker and the defender to exactly the same extent [96].

A second heresy I've been nurturing is about quantum computing. This has failed to deliver the goods despite enormous funding over almost twenty years; does this tell us anything about the foundations of quantum mechanics? I suspect it just might [202, 205]. Most recently we've shown that hydrodynamic models of quantum mechanics lead to a really neat explanation of Yves Couder's famous bouncing-droplet experiment [209], and that the Bell tests – which are commonly interpreted to mean that reality must be nonlocal, noncausal ot both – imply nothing of the sort: all that's needed to explain the observed correlation between cogenerated photons is some form of long-range order, such as the order parameter in a superconductor. In fact, even James Clerk Maxwell's obsolete 1860 model of electromagnetism, in which magnetic lines of force are tubular vortices in a fluid, supports Bell-test behaviour [220]. This raises questions about the security proofs offered for quantum cryptosystems based on entanglement.

1.9 Policy

With the Snowden revelations, the world of information security has lost its innocence, as physics did in 1945. But this was just the latest incident in a long process, as states, citizens, businesses and spooks have tussled for control in cyberspace. The 1990s saw the 'Crypto wars' as governments claimed that cryptography needed to be controlled; I was an author of probably the most influential and widely cited paper on this topic [44]; I was also the first to point out that it was not a straight fight between crypto and state surveillance, as most privacy compromises come from the abuse of authorised access and most of the rest from metadata [22] (for further writings on crypto policy, see [43, 48, 53, 65, 87, 130, 131, 132, 133, 140, 170, 171]). In the last year or so, crypto controls have been brought back on the agenda by UK Prime Minister David Cameron and FBI Director James Comey; we have updated our classic paper to demonstrate that not much has changed, and the arguments against government-mandated exceptional access to systems are as strong as ever [225].

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.

The FAQ I wrote on'Trusted Computing' [100, 101] together with my economic analysis [103] helped kill the project. I coauthored a copyright policy document adopted by many European NGOs [110] wrote many other NGO submissions on policy [130, 131, 132, 133, 140, 141, 150, 152, 170, 171, 195, 196, 196]. I was on the UK Government Chief Scientific Adviser's Blackett Review of Cyber Security, which led in 2011 to an extra £640m being spent on cyber security over the period 2011–5. I was one of the authors of the Nuffield Bioethics Council's recent report on biodata [219].

Other high-impact policy works include a report commissioned by the Chief Scientific Adviser at the Ministry of Defence on the costs of cybercrime [194]; a report for the Information Commissioner on children's databases [135]; a report published by the Joseph Rowntree Reform Trust entitled *'Database State'* on the safety, privacy and legality of large UK public-sector databases [164]; a study of the security economics and policy options in cybercrime [154]; and a study of the resilience of the Internet [185]. The 'Database State' report was adopted by both Conservative and Liberal Democrat parties before the 2010 election, which they won – leading to the abandonment of the ContactPoint and eCAF children's databases.

The hot topic in 2017 is our report on what happens to safety regulation in a world full of Internet-connected things [238].

1.10 Research mentoring and management

I am currently supervising two research students (Khaled Baqer and Alexander Vetterl). I have ninet postdocs (Richard Clayton, Franck Courbon, Alice Hutchings, David Modic, Sergio Pastrana, Laurent Simon, Sergei Skorobogatov, Daniel Thomas and Sven Uebelacker). Three former students now lecture here (Markus Kuhn, Frank Stajano and Robert Watson), while Feng Hao lectures at Newcastle, Jeff Yan and Shishir Nagaraja in Lancaster, Steven Murdoch and George Danezis at UCL, Tyler Moore at Tulsa, Oklahoma, Harry Manifavas in Dubai, Hyoungshick Kim in Korea and Susan Pancho in the Phillipines. Twenty-eight of my former research students have earned PhDs (Jong-Hyeon Lee, Fabien Petitcolas, Frank Stajano, Harry Manifavas, Markus Kuhn, Ulrich Lang, Jianxin 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 and Sheharbano Khattak).

I started four successful 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.

Current direct research funding sources include Thales, Orange, EPSRC and the Gates Foundation.

Consultancy clients over the last twenty years include RealVNC, Alcatel-Lucent, Qualcomm, Samsung, Actel, Securicor, Lehman Brothers, Kudelski, Matsushita, Microsoft, Intel, VISA, the 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 cover those areas of the curriculum which have to do with the dependability of computer systems. My lecture courses are in software and security engineering (for part Ia), economics, law and ethics (for part Ib), security (two courses for the MPhil).

I was elected to Council – the University's governing body – for 2003–2006, 2007–10, and 2015–19. I also serve on the university's Planning and Resources Committee, its Research Ethics Committee and the Council of the School of Technology.

3 Work history

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

2011: Visiting scientist, Google; visiting professor, CMU

1984–1991: Self employed consultant working mostly in projects related to computer security. The project which had the greatest impact was probably the design of protocols for a smartcard payment system [45].

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 avionics

4 Education, qualifications and awards

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

2015: ACM SIGSAC Outstanding Innovation 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; Fellow, RSA

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 and 2017; Security of Internet of Things 2012 (program co-chair); 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: Decepticon 2015; Workshop on Economics and Information Security, 2002–17; SHB 2008–17; Financial Crypto 2009–2017; GameSec 2012–6; 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; IPTPWS 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: 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; ESORICS 2011; AusCERT 2011; CMU Cylab 2011; DHS/SRI ITTC 2011; OII 2011; Visions of Computer Science (launch of the 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 Beduidenhoudt) 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*, 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

[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, at http://idei.fr/activity.php?r=1898

[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] "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

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

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

[166] "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

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

[168] "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

[169] "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

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

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

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

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

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

[175] "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])

[176] "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

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

[178] "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)

[179] "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

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

[181] "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)*

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

[183] "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

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

[185] *'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

[186] "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)

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

[188] "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

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

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

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

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

[193] "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`

[194] "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

[195] "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 *RESoLVEâĂŹ12* (Mar 3, 2012)

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

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

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

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

[200] "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

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

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

[203] "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

[204] "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

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

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

[207] "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

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

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

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

[211] "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

[212] "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 [200])

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

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

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

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

[217] "To freeze or not to freeze – A motion-capture approach to detecting deceit" (with Sophie van der Zee, Ronald Poppe and Paul Taylor), in *HICSS 2015*

[218] "Mining Bodily Cues to Deception" (with Ronald Poppe, Sophie van der Zee, Paul Taylor and Remco Veltkamp), in *HICSS 2015*

[219] *'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

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

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

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

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

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

[225] "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)*

[226] "ItâĂŹs 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

[227] "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

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

[229] "DonâĂŹt Interrupt Me While I Type: Inferring Text Entered Through Gesture Typing on Android Keyboards" (with Laurent Simon and Wenduan Xu), PETS 2016

[230] "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

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

[232] "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*

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

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

[235] "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

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

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

[238] "Standardisation and Certification of the âĂŸInternet of Things" (with Èireann Leverett and Richard Clayton, *Workshop on the Economics of Information Security* (2017)

[239] "DigiTally: Piloting Offline Payments for Phones" (with Khaled Baqer, Lorna Mutegi, Jeunese Adrienne Payne and Joseph Sevilla), at SOUPS 2017