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 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 ten 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 prepayment utility meters to the HomePlug standard for power-line communications.

Security engineering is much broader than ‘computer security’. There are already more mobile phones connected to the Internet than computers. We are starting to see many of the world’s heart monitors, bus ticket dispensers, burglar alarms, and utility meters talking IP. Computing will be embedded invisibly everywhere; and many of the problems we’ve experienced with PCs are starting to turn up in other applications. Many insecure systems are built, and the resulting safety, privacy and crime prevention problems (both real and perceived) are a significant impediment to building the ‘electronic society’. The resulting policy issues – privacy, surveillance, forensics, DRM and competition policy – are steadily moving up the political agenda.

I chair the Foundation for Information Policy Research, the UK’s premier information think-tank, and am on Cambridge University’s Board of Scrutiny. I also teach undergraduate software engineering, a service course in economics, law and ethics for computer science, two graduate courses in security, and a systems course for our Masters in Public Policy degree.

Ross Anderson FRS FREng
October 2014
1 Research

1.1 Economics and security

A major achievement has been establishing security economics as a thriving academic discipline. Back in 2000 I was one of two pioneers. This discipline now has over 100 researchers at its annual conference (WEIS, which I cofounded in 2002). 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] and the resilience of the Internet [185] (both of which got adopted as policy), and a major study of the costs of cybercrime for the UK Ministry of Defence [194]. I have other papers on online crime [174], attitudes to online crime [214], and the security economics of both 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]. I have organised seven workshops now on Security and Human Behaviour that have brought together security engineers with behavioral economists, psychologists, and others.

1.2 Peer-to-Peer systems and networks

Since about the middle of 2000, there has been an explosion of interest in peer-to-peer networking – the business of building useful systems out of large numbers of intermittently connected machines, with virtual infrastructures that are tailored to the application. I wrote one of the seminal papers, on The Eternity Service [35]. I had been alarmed by the Scientologists’ success at closing down the penet remailer in Finland, and tried to design a system that would be less vulnerable to attacks based on coercion. 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]. 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 techniques 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, 217], prepayment electricity meters [18, 30], medical record systems [23, 29, 61, 68, 69, 129, 136, 151] 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 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]; I’ve more recently been tackling smart grids and smart meters [168, 173, 180, 182, 201].

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 extremely common in practice but notoriously difficult 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], 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 can have been 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 manufacturers to redesign many products and the field now has its own workshop.

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 without using the
circuits supplied by the chip vendor for that purpose. From 1999 to 2003, I had a large EU-funded project aimed at making smartcard CPUs much less vulnerable to attack by constructing them from self-timed dual-rail logic with inbuilt alarm circuitry [86, 92, 98]. Recently we’ve shown that the supposed tamper-resistance of common PIN Entry Devices is quite unsatisfactory and that the system used to certify them is deeply flawed [153, 199]. Our most recent work on reverse engineering recast de-compilation as a search problem [206].

1.6 Analysis and design of ciphers

Cryptology is a subject to which I return every few years. 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 providing a computer with Tempest protection (that is, preventing opponents from reconstructing information from stray RF emanations) 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].

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 stright 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 May 1998, I was one of the founders of the Foundation for Information Policy Research, which has grown into the UK’s premier think-tank for information policy. We secured worthwhile amendments to various laws including the RIP Act and the Export Control Act in the UK and the IPR Enforcement Directive in Brussels. I also advise the European Commission on ‘Trusted Computing’: the FAQ I wrote on this [100, 101] and 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 polic [130, 131, 132, 133, 140, 141, 150, 152, 171, 195, 196, 196].

I was invited to join the Government Chief Scientific Adviser’s Blackett Review of Cyber Security, which led in 2011 to the Government making an extra £640m available for cyber security over the period 2011–5. I’m on the steering groups of the Royal Society’s project on cybersecurity research, and of the Nuffield Bioethics Council’s project on biodata.

My highest-impact recent policy works were probably 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 last two reports have been largely adopted as policy by the European Commission, while the ‘Database State’ report was adopted by both Conservative and Liberal Democrat parties before the 2010 election, which they won. As a result, a number of its recommendations have been implemented, including the abandonment of the ContactPoint and eCAF children’s databases.
1.10 Research mentoring and management

I am currently supervising three research students (Laurent Simon, Rubin Xu and Dongting Yu). I have six postdocs (Alice Hutchings, Sophie van der Zee, David Modic, Richard Clayton, Steven Murdoch and Sergei Skorobogatov). Three former students now lecture here (Markus Kuhn, Frank Stajano and Robert Watson), while Jeff Yan and Feng Hao lecture at Newcastle, Shishir Nagaraja in Birmingham, George Danezis at UCL, Tyler Moore at Southern Methodist University in Austin, Harry Manifavas in Crete, Hyoungshick Kim in Korea and Susan Pancho in the Philippines. Twenty-three 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 and Wei-Ming Khoo).


Current direct research funding sources include Google, the US DHS, Samsung, EPSRC and the Tor Foundation.

Consultancy clients over the last fifteen 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 engineering (for part Ib), economics and law (for part Ib), security (MPhil) and systems (MPP). I help to run the group projects, which are designed to teach undergraduates about developing software in teams.

I was elected to Council – the University’s governing body – for 2003–2006, and re-elected top of the poll for 2007-2010, following my leadership of the ‘Campaign for Cambridge Freedoms’ which substantially amended a policy on intellectual property that would have done great damage. I now serve on the university’s Board of Scrutiny and its Research Ethics Committee.

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 memberships

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)


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


**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


**Royal Society Committees:** sectional committee 4

**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 Se-
curity, Cryptology and Coding Theory, January – June 1996


References


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


[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)


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


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


‘IEEE Journal on Selected Areas in Communications’, v 16 no 4 (May 1998) joint editor


“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

“Serpent and Smartcards” (with E Biham and LR Knudsen), in *the pre-proceedings of Cards 98*; available at http://www.cl.cam.ac.uk/~rja14/serpent.html

“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


“The Use of Information Retrieval Techniques for Intrusion Detection” (with A Khattak), at ‘Recent Advances in Intrusion Detection’, Louvain-la-Neuve, Sep 98

‘Health Informatics Journal’ v 4 no 3/4 (December 1998) guest editor

‘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

[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


[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


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


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


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


[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


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


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


“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

“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


[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)


[133] ‘FIPR Consultation Response on “Personal Internet Security” ’, October 2006


[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


[141] ‘FIPR Consultation Response on “The Electronic Patient Record and its Use” ’ (with Ian Brown, Douwe Korff, and Fleur Fisher), March 2007


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


“Shifting Borders” (with Steven Murdoch), in Index on Censorship, December 2007


“Tools and Technology of Internet Filtering” (with Steven Murdoch), in Access Denied, MIT Press (2008) pp 57–72

FIPR Submission to The Hunt Review of the Financial Ombudsman Service’ (with Nicholas Bohm), January 2008

“Patient Confidentiality and Central Databases”, in British Journal of General Practice v 58 no 547 (Feb 2008) pp 75–76

‘Consultation response on The Data Sharing Review’ (with Nicholas Bohm, Terri Dowty, Fleur Fisher, Douwe Korff, Eileen Munro and Martyn Thomas), FIPR, Feb 2008


“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


“Failures on Fraud”, in Speed vol 3 no 2 (Sep 2008) pp 6–7


“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

‘Database State’ (with Ian Brown, Terri Dowty, William Heath, Philip Inglesant and Angela Sasse), Joseph Rowntree Reform Trust, March 2009

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


“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

‘Consultation response on Regulation of Investigatory Powers Act 2000 Consolidating Orders and Codes of Practice’ (with Jim Killock), FIPR and ORG, July 2009

‘Consultation response on Interception Modernisation or “Protecting the Public” ’ (with Jim Killock), FIPR and ORG, July 2009

‘Consultation response on Civil Litigation Costs Review’, FIPR, July 2009


“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])

“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


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


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


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


[200] “Chip and Skim: cloning EMV cards with the pre-play attack” (with Mike Bond, Omar Choudary, Steven Murdoch and Sergei Skorobogatov), arXiv:0547955, Sep 2012

[201] “Smart Metering – Ed Miliband’s Poisoned Chalice” (with Alex Henney), submitted to DECC (2012), and at http://www.lightbluetouchpaper.org


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


[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 (to appear)

[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])


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