Frank Stajano (Ed.)

Rossfest Festschrift

in memory of Ross Anderson

Table of Contents

III Cherished memories

IV Family eulogies (Churchill College, 22 June 2024)

Preface

This posthumous Rossfest Festschrift is a celebration and remembrance of our friend and colleague Ross Anderson, who passed away suddenly on 28 March 2024, aged 67.

Ross Anderson FRS FRSE FREng was Professor of Security Engineering at the University of Cambridge and lately also at the University of Edinburgh. He was a world-leading figure in security. He had a gift for pulling together the relevant key people and opening up a new subfield of security research by convening a workshop on the topic that would then go on to become an established series, from Fast Software Encryption to Information Hiding, Workshop on Economics and Information Security, Security and Human Behavior and so forth. He co-authored between 300 and 400 papers, depending on how you count (see his curated bibliography in this volume). His encyclopedic *Security Engineering* textbook, weighing in at well over 1000 pages, is dense with both war stories and references to research papers. An inspiring and encouraging supervisor, Ross graduated thirty-one PhD students. And, as a contagiously enthusiastic public speaker, he inspired thousands of researchers around the world.

The Rossfest Symposium was held at the Computer Laboratory of the University of Cambridge on 25 March 2025, almost exactly a year after his passing, as an opportunity for all of us who were touched by Ross to get together and celebrate his legacy. Over 170 friends and colleagues registered to attend.

We are very grateful to our sponsors, thanks to whom we were able to offer tea/coffee breaks and lunch to all participants at no charge. The sponsors were

- The University of Hertfordshire, through Professor Bruce Christianson
- Google DeepMind
- Ross's own Computer Laboratory (a.k.a. Department of Computer Science and Technology at the University of Cambridge), through Professor Alastair Beresford

Thanks to all the participants who travelled to Cambridge in order to show and express their appreciation for this extraordinary man.

I invited five other former PhD students of Ross to join me on an Organising Committee that would select the submissions to be included in this Festschrift and would plan the schedule for the day. They were

- Joseph Bonneau, New York University
- Richard Clayton, University of Cambridge
- Markus Kuhn, University of Cambridge
- Tyler Moore, University of Tulsa
- Ilia Shumailov, Google DeepMind

Special credit and thanks are due to Richard Clayton for curating a definitive version of Ross's bibliography, which we are releasing online in BibTeX format

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

as well as including it in this book; to Markus Kuhn for collecting biographical sketches of all the students who graduated with Ross, for curating the archival version of Ross's website, and for LaTeXnical suggestions; and to Tyler Moore for his leading role in scheduling the many talks on the day. Further thanks to Richard Mortier for LaTeX conversions and proofreading, to Jo de Bono for administrative help and to Anh V. Vu for collecting many additional "Cherished Memories", as well as for setting up and curating `https://anderson.love`.

Renewed condolences and very special thanks to Shireen, Bavani and Iain for all their helpful and supportive messages, emails and phone calls during the preparation of Rossfest, and especially for sharing the moving family eulogies of Iain, Lily-Rani and Bavani from the memorial celebration event that took place in the Chapel at Churchill College on 22 June 2024. Thanks to Shireen for the photograph of Ross on the cover, which was taken by his father, and to Iain for that of the Anderson Tartan.

We are grateful to everyone who contributed an article, long or short, to this Rossfest Festschrift. We selected the ones we felt were appropriate for the event, but we did not peer review them. Their appearance in this self-published volume does not constitute an official publication. Do not list them on your CV as published articles, send them to the REF or anything like that. Feel free to put them on your web page but we declare them as *still unpublished*—so that, after benefitting from comments and discussion at the Rossfest Symposium, you will be able to submit an enhanced version to a proper refereed venue without being accused of self-plagiarism.

The © copyright in each of the contributions to this book rests with its author(s), but each contribution has been licensed under the CC BY-NC-ND 4.0 Creative Commons licence, which "enables reusers to copy and distribute the material in any medium or format in unadapted form only, for noncommercial purposes only, and only so long as attribution is given to the creator". For further details, visit `https://creativecommons.org/`.

I initially considered a commercial publisher for this book but soon changed my mind and decided to self-publish in order to retain complete freedom on what to include. This also allows me to release a PDF at no charge. A physical volume, for those who want one, is available through print-on-demand.

Visit `https://www.cl.cam.ac.uk/events/rossfest/` for

- the free PDF of this book
- the free BibTeX with the full bibliography curated by Richard Clayton
- a link to order printed copies of this book

Thanks to Springer for releasing their `llncs` class under Creative Commons, thus permitting its reuse even outside of their own publications, as well as to all the contributors to the free software (LaTeX and much more) that was used to put this book together.

Frank Stajano
University of Cambridge
March 2025

Part I

Ross Anderson
His life and legacy

Ross John Anderson

15 September 1956 – 28 March 2024

Frank Stajano[0000-0001-9186-6798]

University of Cambridge
frank.stajano@cl.cam.ac.uk

1 Early life and student days

Ross John Anderson was born in Wallasey, near Liverpool, on 15 September 1956, the first of two children of William and Anne Catherine Anderson. His younger brother Iain was born four years later. His father was initially a research pharmacist, working for a drug company, and later a Professor of Pharmaceutical Technology at the University of Strathclyde; while his mother was a pharmacist who worked in hospital, and later ran her own pharmacy.

When Ross was five, his family moved back to Scotland, where both his parents were from, and eventually settled in Gourock. There, he joined the local Boy Scouts, which had an active amateur radio club, and he got into shortwave listening and building basic electronic circuits.

From age eleven, Ross attended the High School of Glasgow. He was one of the smartest kids in class but his congenital strabismus, despite a correction operation at age three, meant he lacked binocular vision and was therefore hopeless at the ball games popular with his schoolmates such as rugby or cricket. He was also, as he put it, "way out on the Asperger's spectrum", and the combination of these factors meant he got bullied by the other kids. He recalled his early teen school years as pretty miserable.

Given his academic excellence, his family expected him to become a doctor. Ross, instead, found his calling when, at age 16, he discovered Felix Klein's *Elementary Mathematics from an Advanced Standpoint* in the local library. Until then, he had found maths boring—the school textbooks were too easy for him. Klein's book, instead, aimed at maths PhDs who would become school teachers, fired up his enthusiasm: here was a great mathematician and educator showing how research-grade mathematics could be used to inspire school children. Ross told himself that he would become a mathematician.

His father, worried that such a career would not allow his son to put bread on the table, insisted he go to medical school instead. Thus Ross went up to Glasgow University at 17 to read medicine, but also applied to science as a backup, in case he didn't get an offer. And then, although he had actually been accepted for medicine, proceeded to slip under the radar and attend the science classes instead. He soon noticed that most of his Glasgow maths professors had done a doctorate at Cambridge, so he figured he was in the wrong place: within

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

a few weeks he filed an application to switch to Cambridge and at the end of his first term in Glasgow he attended an admissions interview at Trinity College Cambridge, which he passed. He thus moved there to read mathematics the following October, after completing his first year at Glasgow.

Perhaps over-confidently, he parachuted himself into the second year of the Cambridge Mathematical Tripos, completing the famously demanding three-year degree in just two—an extraordinary feat which in retrospect he found to be extremely hard work. But among the Trinity mathematicians this nerdy kid was finally in his element, and no longer a misfit. Everyone else in that peer group was exceptional in one way or other: "there was a whole bunch of people who thought and behaved and socialised just like me".

After concluding his first year at Cambridge (the second year of his three-year maths degree), Ross took a year out, which he spent in Edinburgh at Ferranti, then a major electronics and defense contractor. There, he ported the inertial navigation system of the Tornado fighter-bomber to make it suitable for use in submarines—a non-trivial hardware project involving discrete logic chips and analogue to digital converters. While at Ferranti he also got a qualification as an electrical engineer by passing the Council of Engineering Institution exam, which he found fairly easy given his mathematical fluency.

On returning to Cambridge after this taste of the real world, he found his interest for pure mathematics had somewhat waned. Others in his peer group were much better at algebraic number theory and group theory than he was and he could no longer see the point of theoretical work disconnected from practical applications. So, after completing Part II, for his third year at Cambridge he did not sign up for the brutally hard Part III (a one-year postgraduate mathematical course) and instead signed up for a year of History and Philosophy of Science, which appealed to his inquisitive mind and broadened his horizons.

2 The world is your oyster

On completion of three years at Cambridge, Ross took a gap year to see the world. First, busking with his bagpipes around the Netherlands, France and Germany; then, using the proceeds to head off towards "the hippy trail to India". But it was 1979 and that plan had to change when, along the way, the Iranian revolution started and travelling through that country under flying bullets no longer seemed like a healthy choice. He ended up hopping around the Middle East for a year, visiting Turkey, Syria, Egypt, Greece, Sudan, Yemen, Saudi, Jordan and Israel.

Back in the UK, he moved to London, taking on a variety of unrelated odd jobs, from sales to publishing to typesetting. Then, in 1982, Clive Sinclair's ZX Spectrum home computer came out, he got himself one and started writing software for it. He was largely self-taught but he had had some modest exposure to computer programming (in FORTRAN on punched cards) at his Glasgow high school, and then again during his undergraduate degree, during which he had programmed some numerical analysis routines in FOCAL on a PDP-8.

One of his friends from Trinity worked as a programmer for an estate agent and had been requested to write some email encryption software, which he had done by repeatedly calling the random number generator and XORing the pseudorandom bytes with those of the plaintext. Neither he nor Ross knew much about stream ciphers at the time but Ross had a hunch that the scheme was not very secure. He started looking into it and was indeed able to crack the underlying linear congruential generator. This got him interested in cryptography. He got hold of the then recently published *Cipher Systems* textbook by Beker and Piper and, with Keith Lockstone, wrote an email encryption program, Cipher-net, featuring their own improved stream cipher, of which they managed to sell a couple of copies. He then cracked a multiplex shift register cipher developed at Royal Holloway, which at the time was the hub of civilian cryptography research in the UK, and this gave him some confidence in his cryptographic skills. He started selling cryptography software to companies that supplied banks.

One thing leading to another, headhunters from Barclays Bank offered him a job. They wanted someone who understood cryptography and could join their information systems team to look at the security of cash machines, points of sale and so on. He remained with them for three years—a stint in the corporate world that he did not particularly enjoy but which was very influential in his career, both for the know-how he acquired on ATMs and on banking back-ends, which later led to his first significant paper as a PhD student, and for what it taught him about the hierarchies, incentives and inefficiencies of large organisations, which later resurfaced in his work on security economics. After Barclays, bitten by the travel bug, in 1989 he left for Hong Kong, taking on a more senior role in a project for another large British bank, Standard Chartered. He helped them establish a new branch network system for use in 23 countries in Asia. Comparing his experience at the two banks gave him first-hand knowledge of good and bad ways to run large IT projects.

But he found that the cramped and frenetic expat lifestyle in Hong Kong did not suit him, so he declined the bank's offer of a permanent post there. He went on as an independent consultant, travelling around the world as projects called. ESCOM, the Electricity Supply Commission of South Africa, in anticipation of the change of regime from de Klerk to Mandela, needed to find a way to bring electricity (and charge for it) to millions of black African households, in areas where people didn't even have addresses, let alone credit ratings. So Ross got involved in a major ESCOM project to design and deploy prepayment electricity meters: customers could buy 20-digit numbers that, through cryptography, would top up their electricity meter by a certain number of kWh. Although the design had some initial teething problems it eventually turned out to be a big success and allowed Nelson Mandela to deliver on his election promise to electrify two million homes. Thirty years later, derivatives of that design are deployed in around a hundred million meters, in around a hundred countries. This project gave Ross further first-hand experience of large-scale IT security systems and their failure modes that would serve him well during his subsequent life in academia, setting him apart from the theoretical cryptographers.

The most significant reward of his South African experience was not, however, the success of the ESCOM prepayment electricity meters project—rather, it was his encounter with his future wife Shireen, whom he adored and who would thereafter share the rest of his life with him.

3 Back to Cambridge as a mature student

By 1991, the UK was in a recession: large firms were cutting back on external contractors and business for an independent consultant was slow. Also, Ross experienced impostor syndrome for having advised banks for years as a cryptography expert without ever having taken a proper university course on the topic. Having toyed for years with the idea of going back to University for a PhD, he felt that was finally the right time; and he had saved enough from his security work to be able to self-fund his graduate studies. And so he went back to Cambridge for a chat with computer security pioneers Roger Needham and David Wheeler. Roger (of Needham–Schroeder fame) was then the head of the Computer Laboratory while David, once Roger's PhD supervisor, had written the initial orders for EDSAC, the first stored-program computer to go into regular use. Roger's most recent achievement was the BAN logic, a powerful tool for the verification of security protocols. He gave a copy of the BAN tech report to Ross who, back in South Africa, studied it carefully and applied to prove the security of NetCard, an early offline smartcard micropayment protocol on which he had been working as a consultant. This duly impressed Roger and contributed to earning Ross a PhD place at Cambridge.

Roger had a profound influence on Ross and they had deep respect and admiration for each other. I could witness first-hand the dynamics of their interaction when I joined the Security Group as Ross's student a few years later.

Roger was well known as an inexhaustible source of witty aphorisms, which Ross often quoted at opportune times—whether in presentations, publications, interviews, casual conversations and later mentorship of his own graduate students. Among them:

- "If you think your problem can be fixed by cryptography, you don't understand cryptography and you don't understand your problem"
- "Serendipity is looking for a needle in a haystack and finding the farmer's daughter"
- "Optimization is the process of taking something that works and replacing it by something that doesn't quite work but is cheaper"
- "Great research is done with a shovel, not with tweezers"

The latter, which Roger explicitly addressed at Ross early on, when some of his cryptological papers were rejected, was an exhortation to challenge novel problems and break new ground rather than settling for minor incremental improvements. As Ross retold it to Jeffrey Yost:

> "Look, when you find yourself down on your hands and knees with tweezers picking up the crumbs left by 200 mathematicians that trampled the

> place flat already, you're in the wrong place. Leave that to the guys from the University of Mudflats and go and find a big pile of muck, a big pile of steaming muck and drive a shovel into it."

Ross was full of initiative, in unconventional ways for a PhD student, and Roger supported that. Painful rejections of some of his early publication attempts on identity-based signatures, because others had already published similar ideas a few years before, convinced Ross that he needed to be on top of the current literature. With characteristic determination he set out to review and summarise all new scientific articles on security; in the early 1990s the field was still small enough that such an endeavour was just about doable, though not for the faint-hearted. But also, with entrepreneurial spirit and with Roger's backing, he founded an abstracts journal, *Computer and Communications Security Reviews*, in which he published those pithy and timely summaries, and marketed it to university libraries and computer departments, securing a stream of institutional subscriptions. Members of the Security Group at Cambridge were invited to contribute reviews of papers presented at conferences they attended, and got free access in return. Ross edited the journal for several years before eventually selling it to a commercial academic publisher.

A later joint venture between Ross and Roger was, in 1998, their founding of FIPR, a non-profit think tank about Internet policy. They shared strong feelings on the importance of contributing actively to policy and governance, rather than merely to technical and scientific advances. Roger had served as a local district councillor and, for the University of Cambridge, as a Pro-Vice-Chancellor. Ross, once he became faculty at Cambridge, served several terms on the University Council and, among other initiatives, founded the Campaign for Cambridge Freedoms to stop an attempted IP land grab by the University administrators on the copyrights, performance rights and patent rights of the creative outputs of the academics.

As we mentioned, Ross self-funded his PhD out of his own savings. He did not have a scholarship or stipend and was thus keen to take on the occasional odd job. During his first year, he served as expert witness in a court case involving ATM fraud. Bank customers were suffering phantom withdrawals but the banks insisted that their systems were secure and insinuated it was the victims who were fraudulently attempting to be refunded. A class action lawsuit ensued, with 2,000 victims suing 13 banks for 2 million pounds. Ross was hired as expert witness by virtue of being essentially the only person with in-depth understanding of ATMs who was not on the payroll of a bank or bank supplier. Unfortunately the high court judge allowed himself to be persuaded by the banks' lawyers to break up the class action lawsuit into individual small claims court cases, on the premise that there was no common factor between the complaints. This premise was conclusively proved wrong the following year, when the perpetrator was caught and jailed for six and a half years. The banks had been denying the possibility of fraud, partly to protect their reputation as trustworthy holders of your cash, and partly to avoid paying out. In that second trial, too, Ross served as expert witness. This engagement, besides paying some bills, confirmed how the

fraudster actually operated. Back in the day, to allow offline operation, the bank (at least *that* bank) stored the PIN in encrypted format on the magstripe of the bank card; the ATM would check the supplied PIN against the one found on the card. The villain obtained the account number of the victim from a discarded ATM slip, rewrote the magstripe of a blank card with the account of the victim and the crook's own encrypted PIN, and extracted money from the victim's account by inserting this fake card in the ATM and typing his own PIN. Once the bank plugged that hole and checked the PIN online with a connection to the back-end, the new modus operandi of the attacker was to park a van in front of the ATM, covertly recording passers-by who entered their PIN, and then recovering discarded ATM slips to read account numbers (which at the time were printed in full on the slip). He would then rewrite the magstripe of a blank card with the victim's account and type the PIN that he had observed in his video recording at the timestamp printed on the payslip.

All this and much more Ross wrote up in "Why Cryptosystems Fail", the landmark paper he presented at the first ACM Conference on Computers and Communications Security in November 1993, which put him on the radar of his peers in the security community. He started to make a name for himself as an academic who developed and attacked cryptographic protocols in the real world, not just on the blackboards of theoreticians who drew fancy arrows back and forth between Alice and Bob.

Following his involvement in those ATM phantom withdrawals cases, in 1994 Ross was asked to serve as expert witness in defense of John Munden, a police constable who had complained to his bank[1] about unexplained withdrawals from his account but was instead sued by the bank and convicted for attempted fraud. The bank maintained that its systems were infallible and that the fault must lie with the complainant. Ross fiercely disputed that argument and demanded that the defence be granted access to the bank's computers for cross-examination of the evidence. The bank dragged its feet for nine months. Eventually, thanks in no small part to Ross's relentless pressing, the appeals judge ruled that the prosecution computer evidence was inadmissible because they had failed to give the defence access to their system. Munden was finally acquitted in 1996, after a four-year ordeal. Ross wrote at length on this case, including in the RISKS Digest, in various papers and in his book, and distilled its lessons into a collection of principles including the following.

> Security systems which are to provide evidence must be designed and certified on the assumption that they will be examined in detail by a hostile expert.

As he continued to work on designing and breaking stream and block ciphers, Ross grew increasingly frustrated at the rejections from the established conferences such as CRYPTO or Eurocrypt, where it seemed to him that referees only cared about theorems and proofs rather than about real-world applications of cryptography. Undeterred, he got together with a few like-minded practitioners,

[1] Halifax, technically a building society at the time.

including Jim Massey (co-creator of the IDEA block cipher used in PGP) and Eli Biham (co-inventor of differential cryptanalysis), and founded a new workshop, Fast Software Encryption, on the design and cryptanalysis of symmetric ciphers and hash functions. He hosted the first FSE workshop in Cambridge in 1993, starting a series that continues to this day.

These collaborations started a productive thread of cryptographic research, particularly with Eli Biham, which continued beyond Ross's graduate student years. Outcomes included the BEAR and LION block ciphers, constructed by combining a stream cipher and a hash function; and the TIGER hash function, following the discovery of a collision in MD4. Eventually Anderson, Biham and Knudsen teamed up to produce Serpent, a 128-bit block cipher designed as a candidate for the Advanced Encryption Standard (AES), the planned replacement for the Data Encryption Standard (DES) block cipher whose 56-bit key length was by then universally recognised as too small. The brief of the competition had been to produce a design "as fast as DES and as secure as Triple DES". Serpent, a bit-slice design optimised for parallelism on the emerging 64-bit processors, went through to the final round of the competition, where it received the second-highest number of votes, losing out to Rijndael. The Serpent designers had optimised for security rather than speed, giving their cipher a very large security margin while still being faster than DES. With hindsight, Ross believed their cipher might have become the AES if they had taken the opposite trade-off and halved the number of rounds.

But back to Ross's student days. The Cambridge regulations require that the PhD dissertation be submitted after a minimum of nine terms (three years) of research. Seeing no reason to waste time, he pulled together his previous papers—the robustness of cryptosystems from the cash machine work, the cryptanalysis of stream ciphers and some extra material on cryptographic protocols—tying them together with the overarching thesis that robustness in cryptographic protocols comes primarily from explicitness. Roger Needham once remarked to me in an admiring tone that Ross was one of the few people he knew who could sit down and produce polished prose without hesitation on his first draft. When the time came, Roger recalled, it took Ross less than two months to produce his dissertation.

Ross's PhD was approved in 1995 and he was appointed to a lectureship the same year. Five years later, as my PhD supervisor, he motivated me to follow in his footsteps, submitting my dissertation and signing my lectureship contract within nine terms of starting. This would have never happened without his mentorship and example.

4 Academic career

The straight transition from PhD student to lecturer, without the limbo of a postdoc stage, was remarkably seamless for Ross: he basically carried on doing more of what he liked and was already doing anyway, with the significant differences that he could now admit graduate students and apply for research

grants. He had quietly avoided identifying himself as a PhD student while he was still one, projecting instead the image of an already established researcher—a believable image given his age and experience. This, for example, was his autobiographical sketch in the *Communications of the ACM* journal version of "Why Cryptosystems Fail":

> Ross J. Anderson is editor of *Computer and Communications Security Reviews*; he has worked on cryptology and computer security for the last 10 years, and consulted for a wide range of equipment manufacturers and users. Current research interests focus on the performance and reliability of computer security systems.

As lecturer, he continued to offer his expert advice and passionate eloquence to worthy causes, as he had done with the victims of phantom withdrawals, and to write it all up in compelling papers that both broadened the debate and consolidated his position on the map as a security academic who was firmly in the real world rather than in an ivory tower. Two examples of this process from his early years as lecturer were in the realms of medical confidentiality and regulation of encryption.

Around 1995, the UK government wanted to centralise all of the nation's medical records into one giant database and exert greater top-down control on the whole National Health Service—a plan that the doctors vehemently opposed. Compared to the then-current practice of holding patient records on paper at the local surgery, with access limited only to the medical practitioners who knew the patients personally, the centralised database was easy to abuse and antithetic to medical confidentiality of the patients' personal information. Ross advised the British Medical Association for a couple of years and produced an extensive report. Among other things, Ross documented the social engineering threats to which surgeries were subjected. More importantly, he developed a clear and simple "BMA Security Policy" to govern the access control and operational security aspects for the proper privacy-protecting handling of electronic patient records. He continued to be vigilant long after the formal conclusion of that collaboration, publishing detailed criticism of the Caldicott report that the Department of Health had put forth. The BMA Security Policy thereafter featured in Ross's undergraduate security course at Cambridge as one further example alongside other well-known security policies such as Bell La-Padula, Biba, Clark-Wilson and Chinese Wall. In the few years that followed, Ross developed a few more security policies with some of his graduate students, covering secure publishing on the web and pairing between wireless devices.

Throughout the 1990s, governments around the world attempted to prevent civilian use of strong cryptography for the protection of communication privacy, in what is often referred to as "the crypto wars". In 1991 Phil Zimmermann wrote and released PGP (including its source code), an email encryption program that used military-strength public key cryptography; as a result, he was under criminal investigation for years for alleged violation of US regulations on munitions export control. As part of his civil liberties fight he later released the

PGP source code as a book, using freedom of the press in order to bypass limitations on crypto code export. In 1993, the Clinton administration attempted to mandate key escrow on encrypted voice and data transmissions by forcing all new telephones to incorporate the NSA-designed Clipper chip. With a suitable warrant, US government agencies would have been able to listen in to selected communications. This caused an uproar from libertarians. Ross was a vocal advocate in this debate for decades. In 1996, with Brian Gladman and Paul Leyland, Ross established the `ukcrypto` mailing list to coordinate the formulation of UK government policy on encryption, in response to government plans that would have curtailed freedoms and liberties, particularly communications privacy. He contributed to an influential 1997 report on the risks of key escrow, signed by a Who's Who of the world's civilian cryptographers and presented as a testimony to both the US Senate and the UK House of Commons. From 1997 onwards, he was one of the leading speakers at the *Scrambling for Safety* series of workshops, set up in response to the introduction of the Regulation of Investigatory Powers bill. In 1998 he co-founded the already-mentioned non-profit Foundation for Information Policy Research (FIPR) with Caspar Bowden and Roger Needham: "We are not a lobby group; our enemy is ignorance rather than the government of the day, and our mission is to understand IT policy issues and explain them to policy makers and the press". In 1998, somehow mirroring Zimmermann's move, he also self-published *The Global Trust Register*[2], essentially a certification authority in a book, as a provocative move to preempt government plans to impose onerous licensing conditions and key escrow requirements on certification authorities. He continued to contribute to the crypto wars over the years, not only with further impassionate presentations and position papers but also with engineering designs such as the Eternity Service or the Steganographic File System.

He explored a remarkable variety of topics with his first batch of research students: before the first of us graduated, we had collectively explored and contributed to, under Ross's guidance, all of the following areas and more: micropayment systems, copyright markings on electronic documents, electronic publishing, intrusion detection, hardware tamper resistance, GSM hacking, secure pairing, formal proofs, middleware security. Ross would often mention Roger Needham's recipe for running a great research group: "recruit the best people and let them work on what turns them on". Ross's research group was not a coordinated team of people working together on a common overarching grand project but a bunch of hand-picked brilliant individuals, each with distinct interests that Ross encouraged us to explore. His supervision style was very informal and colloquial. There were no set times for supervisions. He would just randomly drop in for a chat about some new cool idea or piece of news. He provided opportunities—plenty of them—and let it to the initiative of the students to pick them up and do something with it, whether as a new research topic or simply an interesting side quest. For example, while he was working on his AES candidate

[2] Distributed at no additional charge with the above-mentioned *Computer and Communications Security Reviews*.

block cipher Serpent with Eli Biham and Lars Knudsen, he dropped by us with a draft of their paper asking if any of us were willing to reimplement the cipher from the specification in the paper, to verify whether we would get the same results as them. Two of us, Markus Kuhn and I, took him up and contributed independent implementations. Mine helped the authors discover and fix a minor bug in theirs and was shipped to NIST as the reference version. This is just one example out of over a hundred others that could also be made: each of us, including every one of his thirty-plus graduate students, was offered a continuous stream of such opportunities. Ross's supervision style was to admit people with initiative and originality and then let them get along without micromanaging them; but this much appreciated "long leash" approach did not mean we never saw him. On the contrary, he would frequently drop by and offer new ideas, challenge old ones and encourage us to go further than we thought we could. He encouraged us to attend the lab's daily tea break, whether we drank tea or not, to socialise with other members of the Computer Lab outside the Security Group. He also continued Roger Needham's long-standing tradition of the weekly Security Group meeting from 4 to 5 pm on a Friday afternoon, which would continue informally at the nearby Eagle pub[3] when our department's building was still in central Cambridge.

Ross seemed to know everyone in our field (and beyond), and would frequently invite eminent experts to Cambridge, and specifically to that Friday group meeting. And, every time one of them gave a presentation, he would start a blank piece of A4 paper and neatly take notes, while listening attentively and intervening with perceptive observations, sometimes breaking a proposed protocol on the fly. I don't know what systematic filing and indexing strategy he used for the piles of loose sheets he thus produced before he switched to a laptop years later, but I had conclusive proof that his unknown method worked when I proofread the first edition of his book: I recognised anecdotes and nuggets of specialised knowledge that invited speakers had shared at such meetings and that Ross had masterfully recorded and synthesised into a pithy textual vignette, and then integrated into his grand mosaic as one of the tiles. I'll come back to the book later—one of Ross's greatest and best-known achievements.

On the topic of Ross seemingly knowing everyone: this was in no way by accident. He was a purposeful and skilled master at networking. He was a "social hub" because he was the one who made the connections, who brought people together, who created communities. His role as community catalyst in security was at least equal in significance to his book, and an enduring part of his legacy. As a newly-minted lecturer at Cambridge in 1995, one of his first initiatives was to organise a residential research programme on "Computer security, cryptology and coding theory", which he hosted at the Isaac Newton Institute in Cambridge during the first six months of 1996. This event was pivotal in his career and many

[3] It was during one of those "extended sessions" at the Eagle that, in the late 1960s, Roger Needham and Mike Guy came up with the ground-breaking and now universally adopted idea of scrambling stored passwords with a one-way hash function—something Roger once described as "a two-pint solution".

of the attendees still remember it fondly. He assembled a first-class committee of scientific advisors, of the calibre of public-key co-inventor Whitfield Diffie (later Turing Award laureate), and a carefully curated list of attendees, both established and emerging. By inviting them to Cambridge for six months he naturally became friends with all of them. Always ready with a war story, a joke or a perceptive and surprising explanation of why a company or a country or a piece of software behaved a certain way, it came naturally to him to be the centre of the party, the person around whom a group would form to listen. He did it very well. Everyone knew Ross. He behaved in a way that made his seniors treat him as a peer. He, in turn, treated everyone as his peer too, from graduate students to company presidents, without distinction for rank, status or any other characteristic. Once bullied at school for being different (and smarter), when he earned his academic position he was an *ante litteram* champion of equality and diversity.

His Newton Institute residential programme incorporated three international workshops: the fourth edition of the Security Protocols Workshop that Mark Lomas, another one of Roger Needham's graduate students, had started three years prior; the second edition of Ross's own Fast Software Encryption workshop; and a third workshop, on Information Hiding, that Ross launched on that occasion. All three are still ongoing to this day.

The Information Hiding workshop consolidated a new field in which Ross himself played a pioneering role. Research themes included copyright marking of digital objects, covert channels in computer systems, detection of hidden information and various methods for the protection of anonymity of communications. With his student Fabien Petitcolas they broke most of the then-state-of-the-art copyright marking methods. Then, with Markus Kuhn, they released an open-source software tool, Stirmark, that became the field's benchmark for the evaluation of new image watermarking schemes.

Ross was a proactive talent scout: in 1994 he had approached Markus, then an undergraduate in Germany, after having spotted him on online forums as the author of ingenious attacks on encrypted pay-TV systems. The two had many common interests (cryptography, practical attacks, smart cards, hardware security and so forth) and immediately clicked. They started collaborating via email before having met in real life. At the time Ross was still completing his own PhD, but he was confident he would become faculty at Cambridge and was already planning to recruit the brilliant Markus as one of his first students. Their first paper together, "Tamper Resistance — a Cautionary Note", broke new ground and caused quite a stir. In due course it collected over a thousand citations. It was published in 1996, before Markus even started his PhD at Cambridge. In summer 1997, at one of the Friday meetings, Ross was telling me enthusiastically about this great new student who would join us in October. I later found out that Markus, as a teenager, had earned a gold medal at the very first International Olympiad in Informatics. One of the devious ideas that Ross floated to Markus when he arrived was in the realm of information hiding: could a software house embed a watermark in the on-screen display of their program, such that

a TV detector van parked outside could detect whether anyone was running the software without having paid the licence? Markus went deep down the rabbit hole of electromagnetic emanations and ended up producing a totally different deliverable, namely a special bitmapped font with low-pass-filtered image edges that made it harder for a TEMPEST eavesdropper to reconstruct the display. This technology led to a patent, to a paper at the next Information Hiding workshop, and was later incorporated in the "secure viewer" of the commercial version of the PGP email encryption program. Markus worked on other topics too, including the mentioned Stirmark, but compromising electromagnetic emanations eventually became the core of his PhD.

On the basis of Markus's experience with physical attacks on chips and smartcards described in the tamper resistance paper, Ross encouraged him to set up a hardware laboratory where this line of research could be developed. They were able to get a local semiconductor company to donate an old microscope and to get the department of Material Science to grant them time on their Focused Ion Beam machine. This line of research really took off when Ross attracted a new student, Sergei Skorobogatov, who became the go-to chip hacking expert at the lab and developed the novel technique of *semi-invasive attacks*. Non-invasive attacks, such as power analysis and glitching, manipulate the external connections of the chip but do not break into the physical package. Invasive attacks, such as microprobing, depackage the chip, dissolving the outer plastic and grinding away the passivation layer, and then manipulate the internal electrical lines of the chip by direct electrical contact. Semi-invasive attacks sit between those two extremes: the chip still gets depackaged, as with invasive attacks, but the passivation layer is not touched, as these attacks do not require electrical contact with the chip lines, which makes them cheaper to execute. Energy is transmitted to selected individual transistors of the chip using a laser. This lets the attacker read out the bit stored in a memory cell or even to flip its state.

Besides his research, as a lecturer Ross also created and taught a new undergraduate computer security course, for which he wrote his own course notes because none of the few available textbooks covered all the topics he thought were relevant—from block and stream ciphers to security protocols, to the greater practical importance of availability and integrity compared to confidentiality, to covert channels, to security policies, to the difficulties of anonymising medical records, and so forth. Inspired by the runaway success of Bruce Schneier's *Applied Cryptography*, Ross soon decided that he would write his own book; and also (never one to set his sights too low) that everyone who had bought Schneier would end up with Ross's own book next to it on the shelf. The lecture notes he had already prepared for his course provided him with an initial bulk of already-written chapters that made the endeavour less daunting—but over the course of a year he more than doubled the page count, adding chapter after chapter of well-researched specialist topics and integrating first-hand knowledge gathered from pioneers in the field (those famous loose-leaf notes taken during presentations). Ross had a special talent as a storyteller and was able to combine sharp technical commentary with relatable anecdotes, as he had already

demonstrated in "Why Cryptosystems Fail". His scientific content was solid and well-documented, his bibliography had over a thousand entries, but in addition his prose was lively and compelling. This book, while aimed at a technical audience, was a page-turner. Usability guru Don Norman commented (on the second edition):

> "I'm incredibly impressed that one person could produce such a thorough coverage. Moreover, you make the stuff easy and enjoyable to read. I find it just as entertaining — and far more useful — than novels (and my normal science fiction)."

It really put Ross on the map as a knowledgeable world-class security expert. The thread that linked all the parts, from protocols to crypto, from banking to nuclear command and control, from electronic warfare to copyright protection and management issues, was, as the title says, *Security Engineering*: the idea that effective security is not about a particular protection technology, such as cryptography or access control or tamper resistance, but about building a robust *system*, capable of resisting both accidents and malicious attacks; and that this endeavour will fail unless we take into account all parts of the system, including implementation, operations, insiders, users and incentives, rather than just the cool techie bits.

In 2000, as he was finalising his book, Ross was promoted from University Lecturer to Reader—acknowledging the excellence and international recognition of his research achievements. He was appointed Full Professor, reaching the top rung of the academic ladder, in 2003. He proudly confided at the time that he had set himself a goal of getting to full professor at Cambridge in ten years, but had managed to do it in eight.

Ross credits his encounter with economist Hal Varian as a turning point. As he was in the final passes of writing his book and refining the narrative that pulled together its disparate topics, Ross found he relied increasingly on economics to interpret and explain the paradoxes of security. Hal Varian, a Berkeley professor of economics who shortly afterwards became the Chief Economic Officer of Google and designed the ad auction mechanism at the core of their commercial success, had just written an influential bestselling business book, *Information Rules*, that explained how network effects shaped the behaviour of the big tech firms. Ross read it like the gospel, quoted it widely and brought its insights into the undergraduate courses he was lecturing. He describes his in-person meeting with Hal Varian, following extensive correspondence, as the day it dawned on both of them that their complementary disciplines could, together, explain the important failures of big socio-technical systems:

> And that was something that we just started to grasp in the Claremont car park 15 years ago, as Hal and I were sitting there. We talked and talked and talked and we missed most of the Oakland reception. I was vaguely aware that I should go and have a glass of wine and say hi to all the people in my field, and Hal was vaguely aware that he should go

> home to his family and have dinner, but we just sat there for it must have been over an hour in his car just talking all these things through and realizing, you know, wow, yes this fits, then that fits, the next fits.

Digesting and systematising those insights, Ross later wrote "Why information security is hard — an economics perspective", a landmark paper that opened up the discipline of security economics. Initially rejected by the top-tier IEEE Security and Privacy conference for lack of mathematical content, it took off when Ross presented it as an invited keynote at another conference. The following year (2002) Ross spent some of his sabbatical with Hal at Berkeley where, following a by now familiar playbook, they convened the first Workshop on Economics and Information Security (WEIS), once again acting as the catalyst for the formation of a new research community.

Back in Cambridge, in 2000, at the Security Protocols Workshop of which he was a regular attendee, Ross put forward a new research idea. There had been much research on the correctness of cryptographic protocols, which are typically short sequences of about half a dozen transactions between two participants—and yet, despite their conciseness, they are surprisingly difficult to get right, with bugs regularly being discovered in deployed protocols despite years of public scrutiny. In practical applications, however, the participants rely on cryptographic facilities (such as a crypto library, a smartcard or a hardware security module) that are capable of many different transactions—perhaps over a hundred of them. Ross's insight was that this inherent complexity would necessarily result in security vulnerabilities; if one looked carefully enough, he surmised, one might find a combination of allowed transactions that achieved a result that ought to have been disallowed.

A student who joined the group a few months later, Mike Bond, was offered this idea as his initial "side quest". Ross handed him the thick manual of the IBM 4758 cryptographic coprocessor, a tamper resistant hardware security module sold to banks for secure handling of ATM PINs and master keys, with the task of finding the security vulnerability that was probably lurking in there. Mike did not disappoint: before the post-proceedings write-up of Ross's security protocols talk was finalised, he had discovered attacks that broke the security of what was then the only cryptoprocessor in the world certified at FIPS 140-1 Level 4, the highest level of tamper resistance for unclassified equipment. This opened up the field of Security API attacks. A workshop series on Analysis of Security APIs eventually ensued, and carried on for several years.

Ross continued to attract and inspire a steady stream of capable research students, each of whom contributed new insights. Over the course of three decades he graduated over 30 students and coauthored over 300 publications[4] and thus any attempt at recounting all of his research outputs, including Ross's own endeavours in his retrospective interviews, is bound to omit more of them than

[4] Or closer to 400 if counting multiple versions and some other minor items he did not include in the last CV he wrote, as per the definitive bibliography curated by Richard Clayton and available in this Festschrift volume.

it includes. I hope that the tale I told so far of his first few years, without any pretense of completeness and without disrespect to my many "academic siblings" whom I failed to mention, gives a flavour for the kind of scholar, researcher and mentor that Ross was.

Out of the many research themes he explored in the subsequent two decades, most of which I won't mention despite their significance, "Security and Human Behaviour" stands out. Ross once joked to me that he would periodically start afresh by thinking of "Security and X" (or "Security of X") for new values of X; and that, after ATMs, clinical systems, chip and PIN, economics and so forth, he had now set X = psychology. In a sense this new research line was an offshoot of security economics, via behavioural economics[5]. This was by far the most interdisciplinary of the many workshops that Ross had founded. He teamed up with Bruce Schneier, Alessandro Acquisti and George Loewenstein to hand-pick a diverse group of about fifty researchers, purposefully limiting the number of computer nerds among the attendees and instead actively making space for humanities scholars including psychologists, sociologists, anthropologists and philosophers. The workshop, which continues to this day, took place at MIT, hosted by Internet pioneer David Clark. The ensuing cross-fertilisation was stimulating and productive and resulted in a number of collaborations. Back in Cambridge, Ross launched a multi-year project on the deterrence of deception in collaboration with other UK universities, for which he hired psychologist Sophie van der Zee into his team. They later launched yet another workshop, Decepticon, focused on deceptive behaviour and its detection.

Another major achievement that followed on in 2015 from the interdisciplinary expansion that started with SHB was the establishment of the Cambridge Cybercrime Centre, initially headed by Ross's former student Richard Clayton. This research facility collects datasets about cybercrime (sometimes hard to come by, because those who have the data might be reluctant to share it) and redistributes them, with appropriate legal safeguards, to bona fide researchers. This publicly available data repository has been supporting international academic research into cybercrime for a decade.

After earning his lectureship in 1995 Ross had bought a large house in the countryside, trading off spaciousness and nature against workplace proximity, within the constraints of the modest salary of a Cambridge lecturer. He therefore commuted to Cambridge every day from neighbouring Bedfordshire. After a couple of decades, however, he relocated to Cambridge. At that point he took up a Senior Research Fellowship at Churchill College and became a very active participant in the life of the College. He mentored postgraduate students, served on a variety of committees and frequently engaged in lively conversations over

[5] Indeed Amos Tversky and Daniel Kahneman, who invented Prospect Theory and contributed to the establishment of the discipline of behavioural economics through the comparison of their cognitive models of decision making on one side against economic models of rational behaviour on the other, were *psychologists*, yet the Nobel Prize awarded to Kahneman (which Tversky would have probably shared if he had been alive) was in *economics*.

dinner with Fellows, research students and their guests. At Churchill he is also well remembered for "piping the haggis" at Burns Night.

Preparing against the effects of EJRA regulations at Cambridge that would have forced him to retire after reaching 67—a policy he fiercely campaigned against—in 2021 he took on a part-time professorship at the University of Edinburgh, which had no such constraint, and started supervising students there as well. He continued to live in Cambridge and held joint appointments ad Cambridge and Edinburgh, as reflected in the attribution of his later papers.

Meanwhile the recognitions for Ross had started to pile up: he was elected to both the Royal Society and the Royal Academy of Engineering in 2009, and to the Royal Society of Edinburgh in 2023. In 2015 he was awarded the BCS Lovelace Medal, the highest prize in computing in the UK. But none of these accolades changed what he did: he continued to mentor new students, research new topics and speak up against the powers that be in defense of the causes he believed in. The final feather in his research cap came out of work with former student Ilia Shumailov, with whom he had been exploring "Security of X" for X now equal to artificial intelligence. This led, posthumously, to Ross's first and only article in the prestigious research journal *Nature*. Their insight was that training Large Language Models on the output of previous versions of themselves, as one would do by scraping the web, eventually results in model collapse and the production of gibberish.

5 Personal and professional qualities

It is hard to dissociate Ross's contribution to the field from his flamboyant personality and relentless drive. He had the significant impact he had because he was who he was, and another kind of person who had hypothetically done the same things would never have got his results.

As one who completed the three-year Cambridge maths course in two, there is no question that he was highly intelligent. He was a clear thinker and a fluent and engaging writer, able to turn out clear and compelling English prose at very short notice despite being a two-finger hunt-and-peck typist. He had the uncommon ability to generate perfectly formed sentences in his head and output them to the screen without hesitation—even while paying attention to someone speaking, as he did when he liveblogged the conferences he attended. He was a passionate and charismatic public speaker, with an inexhaustible memory bank of war stories and with the theatrical ability to engage the audience while delivering them.

His unsurpassed human networking abilities, which he put to good use by creating all these workshops and bootstrapping all these new research communities, are all the more remarkable given his starting point as a neurodivergent kid. For sure those who interacted and collaborated with him were also occasionally exposed to a certain lack of diplomacy but on the whole his ability to network and socialise was several standard deviations better than that of the average geek.

He was laser-focused at work but made ample time for his wife, daughter and grandchildren, whose love was his guiding light. Among the piles of papers and books that littered every flat surface in his office, prominently placed next to his monitor was a large composite frame of family photographs.

Among his numerous extracurricular interests (which included dogs, good food and nature), bagpiping deserves a special mention. He was an accomplished performer, an occasional composer and a knowledgeable expert on the origins of traditional Scottish music, which he enjoyed playing for and with his family, friends and the University of Cambridge Ceilidh Band. His love for bagpiping and traditional Scottish music began in his teenage years, with Piobaireachd music being a particular interest, and as a player of the Highland Pipes he went on to become Pipe Major of the Glasgow High School Pipe Band. In time he grew to love playing the Pastoral, Union, Uilleann and Northumbrian Pipes as well. He spent a considerable amount of time finding, collating, sometimes restoring, and making available to all, traditional Scottish Gaelic (and some Irish Gaelic) music. Some of this music may (in his view) have been lost if not for his efforts, as Piobaireachd music in particular was handed down from Pipers to their students over the past 600 years or so, until recently when fewer students have been taking up piping. Ross believed that Piobaireachd music, which has a unique form with a complex structure of theme and variation, should be declared a National Treasure of Scotland. He remained a member of the Piobaireachd Society and the Northumbrian Pipers Society for many years. He acquired and preserved several sets of bagpipes which he thought were of particular cultural significance including a set of Robertson's Pastoral Pipes from 1781. Ross explained his inspiration as to preserving the cultural importance of traditional Scottish music in an interview for Piping Today a few years ago:

> "I went to Donald MacLeod and got lessons in piobaireachd from him [in the 1970s], and that was a great inspiration. One of the things he'd say was that, while he didn't charge for lessons, he did hope we'd pass on what we knew. In a sense, what I'm doing now is just paying that back."

He was relentless in his fights for the causes he believed in, regardless of the size or importance or status of the opponent. He was a man of integrity, always ready to stand for his principles and to defend the small guy—as when he publicly gave the finger, figuratively speaking, to the UK Bank Cards association in response to their threatening request to censor the dissertation of MPhil student Omar Choudary that disclosed operational details of flaws in their systems.

To his students, he was a motivating and inspiring mentor, a role model showing that they could achieve much more than they previously thought, a sounding board for their ideas and a prolific provider of new research opportunities.

He was fond of Sir Isaiah Berlin's "Hedgehog and Fox" metaphor: the fox knows many things, but the hedgehog knows one big thing. (These were two alternative approaches to writing a PhD dissertation, he once told me, suggesting that I could glue together several small papers and be a fox, rather than being a hedgehog and having to develop a unified grand theory of everything.)

In that light, if I try to identify what Ross should be primarily remembered for, I can't pinpoint a single item: would it be security engineering? Security economics? Banking security? Serpent? The cybercrime centre? His book? Perhaps his greatest legacy is the legion of PhD students he mentored, many of whom followed in his footsteps as university professors or raised to prominent positions in industry? Or, perhaps even more, his greatest legacy is the communities he built, in his catalytic role as the creator and cheerful convener of all those workshops? Clearly each of these contributions was significant, but truly he was a fox of many things, and his rich legacy to the field of security consists of all of them.

6 Academic career and honours

- BA in Mathematics and Natural Science, Cambridge, 1978
- PhD in Computer Science, Cambridge, 1995
- Lecturer, Cambridge, 1995
- Co-founder, FIPR, 1998
- Reader in Security Engineering, Cambridge, 2000
- Professor of Security Engineering, Cambridge, 2003
- Fellow of the Royal Society (FRS), 2009
- Fellow of the Royal Academy of Engineering (FREng), 2009
- Fellow of Churchill College, 2014
- BCS Lovelace medal, 2015
- Professor of Security Engineering, Edinburgh, 2021
- Fellow of the Royal Society of Edinburgh (FRSE), 2023

Acknowledgements

My primary sources, besides Ross's own writings and my own first-hand knowledge of him as an inspiring PhD supervisor and then as a colleague at the Computer Lab, were two in-depth interviews masterfully conducted by Jeffrey Yost in 2015 and by Elisabetta Mori in 2024. I also benefitted from the recollections of the many who spoke at Ross's memorial event at Churchill College, especially those of his brother Iain and daughter Bavani, now included in this volume. Ross's onetime Director of Studies at Trinity, Keith Moffatt, originally invited me to write a biographical memoir.

Ross Anderson's Bibliography

Curated by Richard Clayton

The last version Ross created of his CV and bibliography had 302 entries—but he was actually an author or co-author of just under 400 documents. The greater number collected here records different versions (for example, workshop then journal) of much the same paper. Further additions include a number of papers, from all stages of his career, that he just seems to have overlooked.

Wherever possible, a URL has been provided that links to an open-access copy of each document, with a preference to linking to his archived website, which Markus Kuhn has carefully curated.

Especially in his early career, Ross named himself as `Ross J. Anderson`, but later on merely as `Ross Anderson`. For clarity, and to improve the sorting, all the bibliographic entries here use the latter style.

For readers who might wish to cite Ross's work in their own papers, this curated bibliography is now available for download in BibTeX format from the Rossfest web page at `https://www.cl.cam.ac.uk/events/rossfest/`.

Ross's Research Interests

Ross diligently maintained his web page (`https://www.cl.cam.ac.uk/~rja14`) and listed his work by topic. That scheme is followed here, albeit without his commentary.

Books

1995 PhD thesis: Robust Computer Security [23]
1998 The Global Trust Register 1998 [66]
1999 The Global Internet Trust Register 1999 [84]
2001 Security Engineering
A Guide to Building Dependable Distributed Systems [106]
2008 Security Engineering (Second Edition) [192]
2020 Security Engineering (Third Edition) [352]

Cryptography, including quantum cryptography

1990 Solving a Class of Stream Ciphers [3]
1991 Tree Functions and Cipher Systems [4]
1993 The Classification of Hash Functions [7]
Faster Attack on Certain Stream Ciphers [8]
A Modern Rotor Machine [9]
A practical RSA trapdoor [10]

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

1994 Fast Software Encryption (Editor) [12]
On Fibonacci Keystream Generators [15]
Searching for the Optimum Correlation Attack [16]
Whither Cryptography [17]
1996 Generation of the S boxes of Tiger [36]
Tiger: A Fast New Hash Function [37]
Two Practical and Provably Secure Block Ciphers: BEAR and LION [38]
Minding your p's and q's [41]
1997 Chameleon – A New Kind of Stream Cipher [51]
1998 Serpent: A Flexible Block Cipher With Maximum Assurance [62]
Serpent: A Proposal for the Advanced Encryption Standard [63]
Serpent and Smartcards [64]
How to Build Robust Shared Control Systems [67]
Serpent: A New Block Cipher Proposal [73]
2000 The Case for Serpent [96]
2002 Two remarks on public key cryptology [115]
2004 The Dancing Bear: A New Way of Composing Ciphers [128,129]
2011 Cryptology: Where Is the New Frontier? [243]
2013 Why quantum computing is hard – and quantum cryptography is not provably secure [274]
Violation of Bell's inequality in fluid mechanics [275]
2014 Why bouncing droplets are a pretty good model of quantum mechanics [286]
2015 Maxwell's fluid model of magnetism [302]

Robustness of cryptographic protocols

1989 Building a Mainframe Security Module [2]
1992 An Attack on Server Assisted Authentication Protocols [5]
UEPS – A Second Generation Electronic Wallet [6]
1994 Making Smartcard Systems Robust [14]
Fortifying key negotiation schemes with poorly chosen passwords [19]
1995 Programming Satan's Computer [25]
Robustness Principles for Public Key Protocols [26]
1996 NetCard – A Practical Electronic-Cash System [40]
1997 The GCHQ Protocol and Its Problems [52]
1999 The Formal Verification of a Payment System [79]
The Cocaine Auction Protocol: On the Power of Anonymous Broadcast [90]
2000 The Correctness of Crypto Transaction Sets [92,93]
2001 API-Level Attacks on Embedded Systems [110]
2003 What We Can Learn from API Security [125]
2004 Protocol Analysis, Composability and Computation [131]
2005 The Initial Costs and Maintenance Costs of Protocols [138,139]
Cryptographic processors – a survey [142,162]
Robbing the bank with a theorem prover [151,187]
2008 What Next after Anonymity? [194,201]

2010 Key Management for Substations: Symmetric Keys, Public Keys or No Keys? [237]
2014 Security Protocols and Evidence: Where Many Payment Systems Fail [291]
2016 SMAPs: Short Message Authentication Protocols [316,317]
2018 Covert and Deniable Communications [334]
2019 Snitches Get Stitches: On the Difficulty of Whistleblowing [342,343]
2022 CoverDrop: Blowing the Whistle Through A News App [365]
2023 One Protocol to Rule Them All? On Securing Interoperable Messaging [376]
Towards Human-Centric Endpoint Security [377]
2024 SoK: Web Authentication in the Age of End-to-End Encryption [387]
Threat models over space and time: A case study of end-to-end-encrypted messaging applications [390]

Machine learning and signal processing

1996 Proceedings of the First International Workshop on Information Hiding (Editor) [30]
Stretching the Limits of Steganography [33]
The Newton Channel [42]
1998 IEEE Journal on Selected Areas in Communications (Editor, special issue) [57]
The Use of Information Retrieval Techniques for Intrusion Detection [69]
The Steganographic File System [71]
On the Limits of Steganography [72]
Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations [75]
Attacks on Copyright Marking Systems [76]
1999 Soft Tempest – An Opportunity for NATO [85]
Evaluation of Copyright Marking Systems [88]
Information Hiding – A Survey [89]
2013 PIN Skimmer: Inferring PINs Through The Camera and Microphone [278]
2015 He Who Pays The AI, Calls The Tune [297]
2016 Don't Interrupt Me While I Type: Inferring Text Entered Through Gesture Typing on Android Keyboards [321]
2019 Sitatapatra: Blocking the Transfer of Adversarial Samples [346]
Hearing your touch: A new acoustic side channel on smartphones [347]
The Taboo Trap: Behavioural Detection of Adversarial Samples [348]
To Compress Or Not To Compress: Understanding The Interactions Between Adversarial Attacks And Neural Network Compression [351]
2020 Towards Certifiable Adversarial Sample Detection [353]
BatNet: Data transmission between smartphones over ultrasound [354]
Hey Alexa what did I just type? Decoding smartphone sounds with a voice assistant [355]
Blackbox Attacks on Reinforcement Learning Agents Using Approximated Temporal Information [356]
Nudge Attacks on Point-Cloud DNNs [357]

2021 Situational Awareness and Adversarial Machine Learning – Robots, Manners, and Stress [361]
Markpainting: Adversarial Machine Learning meets Inpainting [362]
Manipulating SGD with Data Ordering Attacks [363]
Sponge Examples: Energy-Latency Attacks on Neural Networks [364]
2022 Keynote: Trojan Source and Bad Characters: Invisible Hacks and Reluctant Patching [369]
Talking Trojan: Analyzing an Industry-Wide Disclosure [370]
Bad Characters: Imperceptible NLP Attacks [371]
2023 Trojan Source: Invisible Vulnerabilities [379]
When Vision Fails: Text Attacks Against ViT and OCR [380]
Boosting Big Brother: Attacking Search Engines with Encodings [381]
Human-Producible Adversarial Examples [382]
2024 ImpNet: Imperceptible and blackbox-undetectable backdoors in compiled neural networks [388]
Machine Learning needs Better Randomness Standards: Randomised Smoothing and PRNG-based attacks [389]
AI models collapse when trained on recursively generated data [392]

Security of clinical information systems

1995 Clinical System Security – Interim Guidelines [20]
NHS-wide networking and patient confidentiality [22]
1996 Patient Confidentiality – At Risk from NHS Wide Networking [29]
Security in Clinical Information Systems [31]
A Security Policy Model for Clinical Information Systems [32]
1997 Personal Medical Information – Security, Engineering, and Ethics [44]
Problems with the NHS cryptography strategy [45]
An Update on the BMA Security Policy [46]
Eine klare Sicherheitspolitik für klinische Informationssysteme [47]
A new IT strategy for healthcare [49]
1998 The DeCODE Proposal for an Icelandic Health Database [54]
Health Informatics Journal (Editor, special issue) [55]
Healthcare Protection Profile – Comments [56]
Safety and Privacy in Clinical Information Systems [59]
Safety and Privacy in Clinical Systems: The State of Play [60]
1999 Comments on the Security Targets for the Icelandic Health Database [77]
Information technology in medical practice: safety and privacy lessons from the United Kingdom [81]
2000 Privacy Technology Lessons from Healthcare [95]
2001 Undermining data privacy in health information [107]
2005 System Security for Cyborgs [141]
2006 Healthcare IT in Europe and North America [157]
Under threat: patient confidentiality and NHS computing [160]
Children's Databases – Safety and Privacy: A Report for the Information Commissioner [164]

2007 Clause 67, Medical Research and Privacy: the Options for the NHS [178]
2008 Confidentiality and Connecting for Health [188]
Connecting for Health [189]
2009 Database State [215]
2010 Do summary care records have the potential to do more harm than good? Yes [227]
2012 The privacy of our medical records is being sold off [257]
2013 Medical Confidentiality and the Data Protection Regulation [272]
2021 Confidentiality in Remote Clinical Practice [359]

Sustainability of security

1995 Cryptographic credit control in pre-payment metering systems [24]
1996 The design of future pre-payment systems [34]
On the Reliability of Electronic Payment Systems [35]
2010 FIPR Consultation Response on Smart Metering [229]
FIPR Consultation Response on Smart Meters [230]
2011 FIPR Consultation Response on data access and privacy for smart meters [245]
FIPR Consultation Response on license conditions and technical specifications for the rollout of smart meters [246]
Smart meter security: a survey [249]
Data Privacy and Security for Smart Meters – Response to Ofgem's Consultation [250]
2012 Smart Metering – Ed Milliband's Poisoned Chalice [264]
2017 DigiTally: Piloting Offline Payments for Phones [328]
Standardisation and Certification of Safety, Security and Privacy in the 'Internet of Things' [330,331]
2018 Tendrils of Crime: Visualizing the Diffusion of Stolen Bitcoins [333]
Making Security Sustainable [335]
Sustainable Security – an Internet of Durable Goods (keynote talk) [336]
Privacy for Tigers [337]
Making Bitcoin Legal [338]
Bitcoin Redux [339]
What You Get is What You C: Controlling Side Effects in Mainstream C Compilers [341]
2023 If It's Provably Secure, It Probably Isn't: Why Learning from Proof Failure Is Hard [374,375]
Automatic Bill of Materials [378]

Peer-to-Peer and social network systems

1996 The Eternity Service [27]
1997 Secure Books: Protecting the Distribution of Knowledge [48]

1998 On the Security of Digital Tachographs [58]
A New Family of Authentication Protocols [61]
The Eternal Resource Locator:
An Alternative Means of Establishing Trust on the World Wide Web [68]
1999 Jikzi: A New Framework for Secure Publishing [86]
The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks [91]
2000 Jikzi – a new framework for security policy, trusted publishing and electronic commerce [98]
The XenoService – A Distributed Defeat for Distributed Denial of Service [103]
2002 The Resurrecting Duckling: security issues for ubiquitous computing [120]
Security in a digital repository [121]
2004 Key Infection: Smart Trust for Smart Dust [132]
2005 The Economics of Resisting Censorship [144]
Sybil-Resistant DHT Routing [145]
The topology of covert conflict [149,169]
2007 New Strategies for Revocation in Ad-Hoc Networks [183]
Dynamic Topologies for Robust Scale-Free Networks [185]
HomePlug AV Security Mechanisms [186]
2008 Fast Exclusion of Errant Devices from Vehicular Networks [205]
2009 Eight friends are enough: Social graph approximation via public listings [221]
2012 Temporal node centrality in complex networks [265]
Centrality prediction in dynamic human contact networks [266]
Social Authentication: Harder Than It Looks [267]
2013 An Experimental Evaluation of Robustness of Networks [277]
2015 Do You Believe in Tinker Bell? The Social Externalities of Trust [299,300]

Reliability of security systems

1993 Why Cryptosystems Fail [11,18]
1994 Liability and Computer Security: Nine Principles [13]
1996 Tamper Resistance – a Cautionary Note [39]
1997 Low Cost Attacks on Tamper Resistant Devices [50]
1999 How to Cheat at the Lottery (or, Massively Parallel Requirements Engineering) [80]
The Millennium Bug – Reasons not to Panic [82]
Murphy's law, the fitness of evolving species, and the limits of software reliability [87]
2000 Improving Smart Card Security Using Self-Timed Circuits [99,117]
The Grenade Timer: Fortifying the Watchdog Timer Against Malicious Mobile Code [101]
The memorability and security of passwords – some empirical results [102,136,150]
2001 Protecting Embedded Systems – The Next Ten Years [105]
Security policies [109]

2002 On a New Way to Read Data from Memory [118]
Optical Fault Induction Attacks [119]
2003 Balanced self-checking asynchronous logic for smart card applications [126]
2005 A Note on EMV Secure Messaging in the IBM 4758 CCA [137]
Combining cryptography with biometrics effectively [147,168]
2006 Phish and Chips [152]
The Man-in-the-Middle Defence [158,161]
Chip and Spin [163]
Protecting domestic power-line communications [170]
2007 On the Security of the EMV Secure Messaging API (Extended Abstract) [171]
RFID and the Middleman [174]
Software Security: State of the Art [175]
2008 Failures on Fraud [190]
Security, Functionality and Scale? (invited talk) [193]
Thinking Inside the Box: System-Level Failures of Tamper Proofing [202,203]
2009 Failures of Tamper-Proofing in PIN Entry Devices [223]
Optimised to Fail: Card Readers for Online Banking [224]
The Snooping Dragon: social-malware surveillance of the Tibetan movement [226]
2010 Who Controls the off Switch? [234]
The Protection of Substation Communications [235]
Chip and PIN is Broken [240]
2011 Can We Fix the Security Economics of Federated Authentication? [241,242]
Might Financial Cryptography Kill Financial Innovation? – The Curious Case of EMV [248]
2012 Risk and Privacy Implications of Consumer Payment Innovation in the Connected Age [260]
A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs [263]
How Certification Systems Fail: Lessons from the Ware Report [269]
CHERI: a research platform deconflating hardware virtualization and protection [270]
Aurasium: Practical Policy Enforcement for Android Applications [271]
2013 Rendezvous: a search engine for binary code [276]
Authentication for Resilience: The Case of SDN [279]
2014 Collaborating with the Enemy on Network Management [283,288]
EMV: why payment systems fail [284]
Chip and Skim: Cloning EMV Cards with the Pre-play Attack [285]
2015 Be Prepared: The EMV Preplay Attack [301]
Security Analysis of Android Factory Resets [306]
Security Analysis of Consumer-Grade Anti-Theft Solutions Provided by Android Mobile Anti-Virus Apps [307]
2016 International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms [318,329]
2022 Attack of the Clones: Measuring the Maintainability, Originality and Security of Bitcoin 'Forks' in the Wild [372]

Economics, psychology and criminology of information security

2001 Why Information Security is Hard: An Economic Perspective [108]
2002 Security in Open versus Closed Systems – The Dance of Boltzmann, Coase and Moore [113]
Unsettling Parallels Between Security and the Environment [116]
2004 The Economics of Censorship Resistance [134]
On Dealing with Adversaries Fairly [135]
2005 Guest Editors' Introduction: Economics of Information Security [143]
How Much Is Location Privacy Worth? [146]
Trends in Security Economics [148]
2006 The Economics of Information Security [167]
2007 Closing the phishing hole: fraud, risk, and nonbanks [172]
Open and Closed Source Systems are Equivalent (that is, in an ideal world) [173]
The Economics of Information Security – A Survey and Open Questions [179]
Incentives and Information Security [181]
Silver Bullet Talks with Ross Anderson [182]
Information Security Economics – and Beyond [180,191]
2008 Security Economics and European Policy [198,199,214]
Security Economics and the Internal Market [200]
How brain type influences online safety [204]
2009 The Trust Economy of Brief Encounters [211,212]
Certification and Evaluation: A Security Economics Perspective [216]
Security Economics and Critical National Infrastructure [217,233]
Information security: where computer science, economics and psychology meet [220]
The Economics of Online Crime [225]
2010 It's the Anthropology, Stupid! [231,236]
On the Security Economics of Electricity Metering [232]
On the Security of Internet Banking in South Korea [238]
Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication [239]
2011 The Dependability of Complex Socio-technical Systems [244]
Towards a security architecture for substations [251]
Resilience of the Internet Interconnection Ecosystem [252,253]
Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research [254,268]
2012 Security Economics: A Personal Perspective [261]
Measuring the Cost of Cybercrime [262,273]
2014 Experimental Measurement of Attitudes Regarding Cybercrime [287]
Reading this may harm your computer: The psychology of malware warnings [289]
We will make you like our research: The development of a susceptibility-to-persuasion scale [290,340]

2015 It's All Over but the Crying:
The Emotional and Financial Impact of Internet Fraud [303]
Mining Bodily Cues to Deception [304,391]
To freeze or not to freeze: A culture-sensitive motion capture approach to detecting deceit [308,350]
2016 Taking down websites to prevent crime [319]
When Lying Feels the Right Thing to Do [322,323]
2017 Reconciling Multiple Objectives – Politics or Markets? [325,327]
2019 Measuring the Changing Cost of Cybercrime [344]
Perception Versus Punishment in Cybercrime [345]
The gift of the gab: Are rental scammers skilled at the art of persuasion? [349]
2021 Silicon Den: Cybercrime is Entrepreneurship [360]
2022 PostCog: A tool for interdisciplinary research into underground forums at scale [373]
2023 A Case Study in Censorship [383]
Defacement Attacks on Israeli Websites [384]
ExtremeBB: A Database for Large-Scale Research into Online Hate, Harassment, the Manosphere and Extremism [385]
2024 No Easy Way Out: the Effectiveness of Deplatforming an Extremist Forum to Suppress Hate and Harassment [393]
Getting Bored of Cyberwar: Exploring the Role of Low-level Cybercrime Actors in the Russia-Ukraine Conflict [394]

Public policy issues

1995 Crypto in Europe – Markets, Law and Policy [21]
1996 The Export Control Act and Scientific Research [28]
1997 The risks of key recovery, key escrow, and trusted third-party encryption [43]
1998 Signature Directive Consultation [65]
1999 FIPR Consultation Response – Framework for Smart Card Use in Government [78]
The Risks and Costs of UK Escrow Policy [83]
2000 Digital Signature [94]
Roundtable on Information Security Policy [97]
Government Access to Keys – Panel Discussion [100]
2001 Commonsense in the Crisis [104]
2002 Free Speech Online and Offline [111,112]
TCPA/Palladium frequently asked questions [114]
2003 Cryptography and Competition Policy –
Issues with 'Trusted Computing' [122,123,127]
'Trusted Computing' and Competition Policy –
Issues for Computing Professionals [124]
2004 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 [133]

2006 FIPR Consultation Response on: New Powers Against Organised and Financial Crime [153]
FIPR Consultation Response on: Personal Internet Security [154]
FIPR response to the Home Affairs Committee Inquiry into 'A Surveillance Society' [155]
FIPR's Consultation Response on DRM [156]
FIPR Response to the Home Office: "Consultation on the Draft Code of Practice for the Investigation of Protected Electronic Information – Part III of the Regulation of Investigatory Powers Act 2000 [165]
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 [166]
2007 FIPR Consultation Response on 'Framework for Information Assurance' [176]
FIPR Consultation Response on 'The Electronic Patient Record and its Use' [177]
Shifting Borders [184]
2008 FIPR Submission to The Hunt Review of the Financial Ombudsman Service [195]
FIPR Consultation Response on The Data Sharing Review [196]
FIPR Consultation Response on The National Payments Plan [197]
Tools and Technology of Internet Filtering [206]
2009 Cambridge University – the Unauthorised History [207]
The Devil's flame-thrower [208]
FIPR Consultation Response on Civil Litigation Costs Review [209]
Technical perspective – A chilly sense of security [210]
What's academic freedom anyway? [213]
FIPR and ORG Consultation Response on Interception Modernisation or 'Protecting the Public' [218]
FIPR and ORG Consultation Response on Regulation of Investigatory Powers Act 2000 Consolidating Orders and Codes of Practice [219]
Democracy Theatre: Comments on Facebook's Proposed Governance Scheme [222]
2010 FIPR Consultation Response on 'An Information Revolution' – the latest NHS IT Strategy [228]
2011 FIPR Consultation Response on Making Open Data Real [247]
2012 Ethics Committees and IRBs: Boon, or Bane, or More Research Needed? [255]
FIPR Written evidence to the Information Commissioner on the Draft Anonymisation Code of Practice [256]
Protocol Governance: The Elite, or the Mob? [258,259]
2014 Privacy versus government surveillance: where network effects meet public choice [280]
FIPR Consultation Response on The Joint Committee on the National Security Strategy [281]
FIPR Consultation Response on The Speaker's Commission on Digital Democracy [282]

2015 Keys under doormats: Mandating insecurity by requiring government access to all data and communications [292,293,294,295,296]
What Goes Around Comes Around [298]
The collection, linking and use of data in biomedical research and health care: ethical issues [305]
2016 Apple's Cloud Key Vault, Exceptional Access, and False Equivalences [309]
Warning Signs: A Checklist for Recognizing Flaws of Proposed "Exceptional Access" Systems [310]
Are the Real Limits to Scale a Matter of Science, or Engineering, or of Something Else? (Abstract only) [311]
Brexit and technology: How network effects will damage UK IT industry [312]
Hard Newcap or Soft Newcap? A Christmas Fable [313]
Replacing Magic With Mechanism? [314]
What would Brexit really mean for Cambridge [315]
Are Payment Card Contracts Unfair? (Short Paper) [320]
2017 De-Anonymization [324]
The Threat: A Conversation With Ross Anderson [326]
2018 Letter Regarding the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018 [332]
2021 Bugs in our Pockets: The risks of client-side scanning [358,386]
2022 Chat Control or Child Protection? [366]
Legislating for Online Safety [367]
The Online Safety Bill [368]

Patents

1986 Patent Application GB8606842: Fast cryptogenerator [1]
1997 Patent GB2330924: Software piracy detector sensing electromagnetic computer emanations [53]
1998 Patent GB2365153: Microprocessor resistant to power analysis [70]
Patent GB2333883: Low Cost Countermeasures Against Compromising Electromagnetic Computer Emanations [74]
2004 Patent Application GB0426818: User interface for a computing device [130]

Music

2005 The Pastoral Repertoire, Rediscovered [140]
2006 The Sutherland Manuscript [159]

Ross's Co-authors

Ross worked with 245 co-authors. Their names (and number of works they wrote together) are:

Harold Abelson (11), Ruba Abu-Salma (3), Alessandro Acquisti (2), Ben Adida (5), Mansoor Ahmed-Rengers (6), William Aiken (1), Fernando Alvarez (2), Jonathan Anderson (3), Robin C. Ball (1), Khaled Baqer (6), Richard Barnes (1), Chris Barton (3), Daniel Bates (1), Ingolf Becker (3), Steven M. Bellovin (10), Josh Benaloh (10), Kevin Benton (1), Alastair R. Beresford (2), Francesco Bergadano (1), Tanya Berger-Wolf (1), S. Johann Bezuidenhoudt (4), Eli Biham (8), Alan F. Blackwell (4), Matt Blaze (10), Jenny Blessing (5), Nicholas Bohm (7), Terry Bollinger (1), Mike Bond (16), Joseph Bonneau (3), Nicholas Boucher (10), Caspar Bowden (1), Xavier Boyen (1), Robert M. Brady (5), Doug Brown (1), Ian Brown (5), Iain E. Buchan (1), Tom Burrows (1), Paula Buttery (1), Rainer Böhme (8), Andrew Caines (1), Jon Callas (2), L. Jean Camp (1), Haowen Chan (1), David Chisnall (1), Jusop Choi (1), Wonseok Choi (1), Marios O. Choudary (3), Yi Ting Chua (1), Richard Clayton (21), Eleanor Clifford (1), Jolyon Clulow (9), Ben Collier (2), Mauro Conti (1), Alissa Cooper (1), Diane Coyle (1), Bruno Crispo (3), Jon Crowcroft (1), Han Cui (1), Chris Culnane (1), Paul A. Cunningham (1), Pranav Dahiya (1), George Danezis (4), Partha Das Chowdhury (2), John Daugman (2), Nirav Dave (1), Whitfield Diffie (10), Cunsheng Ding (1), Terri Dowty (3), Enrique Draier (1), Saar Drimer (5), Stephen Early (1), Michel J. G. van Eeten (2), Murat A. Erdogdu (1), Kassem Fawaz (1), Fleur Fisher (2), Jacques J. A. Fournier (1), Shailendra Fuloria (10), Yarin Gal (1), Xitong Gao (2), Yue Gao (1), Joseph Gardiner (2), Sherman Gavette (2), Carlos Gañán (1), Sam Gilbert (2), John Gilmore (8), Brian Gladman (1), Rajeev Gore (1), Alasdair Grant (3), Tom Grasso (1), James T. Graves (2), Matthew Green (7), Harshad Gupta (1), Teresa Hackett (1), Darija Halatova (2), Chris Hall (5), Rudolf Hanka (2), Kai Hansen (1), Feng Hao (2), William S. Harbison (1), Alan Hassey (1), William Heath (1), Tor Helleseth (1), Alex Henney (1), Jonathan Herzog (2), Andreas von Heydwolff (1), Stephen Hinde (1), Jean-Pierre Hubaux (1), Daniel Hugenroth (2), Jack Hughes (1), Jun Ho Huh (2), Alice Hutchings (9), Philip Inglesant (1), Václav Matyáš Jr. (4), M. Frans Kaashoek (1), Jane Kaye (1), Dmitry Kazhdan (1), Grant Kelly (1), David Khachaturov (2), Abida Khattak (1), Wei Ming Khoo (1), Jim Killock (2), Hyoungshick Kim (6), Taesoo Kim (1), Yongdae Kim (1), Torleiv Kløve (1), Lars R. Knudsen (5), Douwe Korff (3), Markus G. Kuhn (10), Susan Landau (9), Ben Laurie (2), Jong-Hyeon Lee (6), Chris Lesniewski-Laas (1), Éireann Leverett (3), Michael Levi (3), Stephen Lewis (1), Amerson Lin (5), K. Lockstone (1), T. Mark A. Lomas (2), Anneke Lucassen (1), Philip Machanick (1), Charalampos Manifavas (5), Cecilia Mascolo (1), Paul M. Matthews (1), Kevin McGrath (2), Gary McGraw (2), Nancy R. Mead (1), David Modic (4), Andrew W. Moore (2), Simon W. Moore (5), Tyler Moore (19), Robert D. Mullins (11), Eileen Munro (2), Steven J. Murdoch (22), Lorna Mutegi (1), Alan Mycroft (1), Shishir Nagaraja (6), Roger M. Needham (4), Peter G. Neumann (12), Richard E. Newman (2),

Mark Nottingham (1), Kaisa Nyberg (1), Andrew M. Odlyzko (1), Evangelos Ouzounis (2), Andy Ozment (1), Philip Paeps (1), Luca Pajola (1), Jussi Palomäki (1), Panagiotis Papadimitratos (1), Nicolas Papernot (6), Michael Parker (1), Neville Pattinson (1), Jeunese Adrienne Payne (1), Adrian Perrig (1), Ildiko Pete (1), Fabien A. P. Petitcolas (8), Josef Pieprzyk (1), Ronald Poppe (6), Sören Preibusch (2), Bart Preneel (1), Arthur B. Pyster (1), Jean-Jacques Quisquater (1), Awais Rashid (2), Maxim Raya (1), Martin Richards (1), Alessandro Rietmann (1), Ronald L. Rivest (16), Michael Roe (3), Maria Sameen (2), David Samyde (1), M. Angela Sasse (4), Stefan Savage (3), Hassen Saïdi (2), Jeffrey I. Schiller (11), Howard Schmidt (1), Bruce Schneier (12), Andrei Serjantov (1), Joseph Sevilla (1), Adi Shamir (1), Timothy J. Shimeall (1), Margaret V. Shotter (1), Ilia Shumailov (26), Zakhar Shumaylov (2), Laurent Simon (6), Sergei P. Skorobogatov (6), Michael A. Specter (8), Frank Stajano (8), Jonathan Stout (1), Gianluca Stringhini (3), Chris Sutherland (1), John Kit Tang (2), Don Taylor (1), George S. Taylor (2), Paul J. Taylor (4), Vanessa Teague (3), Daniel R. Thomas (1), Martyn Thomas (2), Panagiotis Trimintzios (2), Carmela Troncoso (2), Marie Vasek (1), Diana A. Vasile (1), Serge Vaudenay (2), Remco C. Veltkamp (2), Anh V. Vu (6), Susan E. Wallace (1), Robert N. M. Watson (1), Geoff Watts (1), Ellis Weinberger (1), Daniel J. Weitzner (8), Mike Wells (1), Paul Whitehouse (1), Lydia Wilson (1), John Wise (1), Jonathan Woodruff (1), Cheng-Zhong Xu (1), Rubin Xu (1), Wenduan Xu (1), Jeff Yan (5), Yuval Yarom (1), Larry Yonge (2), Paul Youn (2), Dongting Yu (2), Almos Zarandy (2), Sophie van der Zee (7), Zhi-Li Zhang (1), Yiren Zhao (11).

References

1. Ross Anderson and K. Lockstone. "Patent Application GB8606842: Fast cryptogenerator", 1986.
2. Ross Anderson. "Building a Mainframe Security Module". *Proceedings, Infosec '89 Conference on Network Security*, pages 75–87, 1989.
3. Ross Anderson. "Solving a Class of Stream Ciphers". *Cryptologia*, **14**(3):285–288, 1990. URL `https://doi.org/10.1080/0161-119091864977`.
4. Ross Anderson. "Tree Functions and Cipher Systems". *Cryptologia*, **15**(3):194–202, 1991. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/tree.pdf`.
5. Ross Anderson. "An Attack on Server Assisted Authentication Protocols". *Electronics Letters*, **28**:1473, 1992. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/server-assisted.pdf`.
6. Ross Anderson. "UEPS – A Second Generation Electronic Wallet". In Yves Deswarte, Gérard Eizenberg and Jean-Jacques Quisquater (Editors), *Computer Security – ESORICS*, volume 648 of *Lecture Notes in Computer Science*, pages 411–418. Springer, 1992. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/smartcards-tr.pdf`.
7. Ross Anderson. "The Classification of Hash Functions". In Paddy Farrell (Editor), *Codes and Cyphers – Cryptography and Coding (IMA Conference on Cryptography and Coding)*, pages 83–93. 1993. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/hash.pdf`.

8. Ross Anderson. "Faster Attack on Certain Stream Ciphers". *Electronics Letters*, **29**:1322–1323, 1993. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/muxfsr.pdf`.
9. Ross Anderson. "A Modern Rotor Machine". In Ross Anderson (Editor), *Fast Software Encryption*, volume 809 of *Lecture Notes in Computer Science*, pages 47–50. Springer, 1993. URL `https://doi.org/10.1007/3-540-58108-1_6`.
10. Ross Anderson. "A practical RSA trapdoor". *Electronics Letters*, **29**:995, 1993. URL `https://doi.org/10.1049/el:19930662`.
11. Ross Anderson. "Why Cryptosystems Fail". In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu and Victoria Ashby (Editors), *ACM Conference on Computer and Communications Security (CCS)*, pages 215–227. 1993. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/wcf.pdf`.
12. Ross Anderson (Editor). *Fast Software Encryption*, volume 809 of *Lecture Notes in Computer Science*. Springer, 1994. URL `https://doi.org/10.1007/3-540-58108-1`.
13. Ross Anderson. "Liability and Computer Security: Nine Principles". In Dieter Gollmann (Editor), *Computer Security – ESORICS*, volume 875 of *Lecture Notes in Computer Science*, pages 231–245. Springer, 1994. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/liability.pdf`.
14. Ross Anderson. "Making Smartcard Systems Robust". In *Proceedings of Cardis 94*, pages 1–14. 1994. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/smartcards-tr.pdf`.
15. Ross Anderson. "On Fibonacci Keystream Generators". In Bart Preneel (Editor), *Fast Software Encryption*, volume 1008 of *Lecture Notes in Computer Science*, pages 346–352. Springer, 1994. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/fibonacci.pdf`.
16. Ross Anderson. "Searching for the Optimum Correlation Attack". In Bart Preneel (Editor), *Fast Software Encryption*, volume 1008 of *Lecture Notes in Computer Science*, pages 137–143. Springer, 1994. URL `https://www.cl.cam.ac.uk/archive/rja14/correlation.pdf`.
17. Ross Anderson. "Whither Cryptography". *Information Management & Computer Security*, **2**(5):13–20, 1994. URL `https://doi.org/10.1108/09685229410792961`.
18. Ross Anderson. "Why Cryptosystems Fail". *Communications of the ACM*, **37**(11):32–40, 1994. URL `https://dl.acm.org/doi/10.1145/188280.188291`.
19. Ross Anderson and T. Mark A. Lomas. "Fortifying key negotiation schemes with poorly chosen passwords". *Electronics Letters*, **30**:1040–1041, 1994. URL `https://www.cl.cam.ac.uk/archive/rja14/fortify.pdf`.
20. Ross Anderson. "Clinical System Security – Interim Guidelines". *British Medical Journal*, **312**:109–111, 1995. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/guidelines.txt`.
21. Ross Anderson. "Crypto in Europe – Markets, Law and Policy". In Ed Dawson and Jovan Dj. Golic (Editors), *Cryptography: Policy and Algorithms, International Conference, Proceedings*, volume 1029 of *Lecture Notes in Computer Science*, pages 75–89. Springer, 1995. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/queensland.pdf`.
22. Ross Anderson. "NHS-wide networking and patient confidentiality". *British Medical Journal*, **311**:5–6, 1995. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/bmj-objections.pdf`.
23. Ross Anderson. *Robust Computer Security*. Ph.D. thesis, University of Cambridge, 1995.

24. Ross Anderson and S. Johann Bezuidenhoudt. "Cryptographic credit control in pre-payment metering systems". In *IEEE Symposium on Security and Privacy*, pages 15–23. 1995. URL `https://www.cl.cam.ac.uk/archive/rja14/prepay-oakland.pdf`.
25. Ross Anderson and Roger M. Needham. "Programming Satan's Computer". In Jan van Leeuwen (Editor), *Computer Science Today: Recent Trends and Developments*, volume 1000 of *Lecture Notes in Computer Science*, pages 426–440. Springer, 1995. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/satan.pdf`.
26. Ross Anderson and Roger M. Needham. "Robustness Principles for Public Key Protocols". In Don Coppersmith (Editor), *Advances in Cryptology – CRYPTO*, volume 963 of *Lecture Notes in Computer Science*, pages 236–247. Springer, 1995. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/robustness.pdf`.
27. Ross Anderson. "The Eternity Service". In *Proceedings of Pragocrypt '96*, pages 242–252. 1996. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/eternity.pdf`.
28. Ross Anderson. "The Export Control Act and Scientific Research", 1996. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/fipr-exportcontrol-2006.pdf`.
29. Ross Anderson. "Patient Confidentiality – At Risk from NHS Wide Networking". In *Proceedings of HealthCare '96*. 1996. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/hcs96.pdf`.
30. Ross Anderson (Editor). *Proceedings of the First International Workshop on Information Hiding*, volume 1174 of *Lecture Notes in Computer Science*. Springer, 1996. URL `https://doi.org/10.1007/3-540-61996-8`.
31. Ross Anderson. *Security in Clinical Information Systems*. British Medical Association, 1996. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/policy11.pdf`.
32. Ross Anderson. "A Security Policy Model for Clinical Information Systems". In *IEEE Symposium on Security and Privacy*, pages 30–43. 1996. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/oakpolicy.pdf`.
33. Ross Anderson. "Stretching the Limits of Steganography". In Ross Anderson (Editor), *Information Hiding, Proceedings*, volume 1174 of *Lecture Notes in Computer Science*, pages 39–48. Springer, 1996. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/stegan.pdf`.
34. Ross Anderson, Johann Bezuidenhoudt, Neville Pattinson and Don Taylor. "The design of future pre-payment systems". In *IEE Metering and Tariffs for Electricity Supply (MATES)*, pages 119–123. 1996. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/mates.pdf`.
35. Ross Anderson and S. Johann Bezuidenhoudt. "On the Reliability of Electronic Payment Systems". *IEEE Transactions on Software Engineering*, **22**(5):294–301, 1996. URL `https://www.cl.cam.ac.uk/archive/rja14/prepay-meters.pdf`.
36. Ross Anderson and Eli Biham. "Generation of the S boxes of Tiger", 1996. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/tigersb.pdf`.
37. Ross Anderson and Eli Biham. "Tiger: A Fast New Hash Function". In Dieter Gollmann (Editor), *Fast Software Encryption*, volume 1039 of *Lecture Notes in Computer Science*, pages 89–97. Springer, 1996. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/tiger.pdf`.
38. Ross Anderson and Eli Biham. "Two Practical and Provably Secure Block Ciphers: BEAR and LION". In Dieter Gollmann (Editor), *Fast Software Encryption*,

volume 1039 of *Lecture Notes in Computer Science*, pages 113–120. Springer, 1996. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/bear-lion.pdf.

39. Ross Anderson and Markus Kuhn. "Tamper Resistance – a Cautionary Note". In *USENIX Workshop on Electronic Commerce*, pages 1–11. 1996. URL https://www.usenix.org/conference/2nd-usenix-workshop-electronic-commerce/tamper-resistance-cautionary-note.
40. Ross Anderson, Charalampos Manifavas and Chris Sutherland. "NetCard – A Practical Electronic-Cash System". In T. Mark A. Lomas (Editor), *Security Protocols IV*, volume 1189 of *Lecture Notes in Computer Science*, pages 49–57. Springer, 1996. URL https://www.cl.cam.ac.uk/archive/rja14/netcard.pdf.
41. Ross Anderson and Serge Vaudenay. "Minding your p's and q's". In Kwangjo Kim and Tsutomu Matsumoto (Editors), *Advances in Cryptology – ASIACRYPT*, volume 1163 of *Lecture Notes in Computer Science*, pages 26–35. Springer, 1996. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/psandqs.pdf.
42. Ross Anderson, Serge Vaudenay, Bart Preneel and Kaisa Nyberg. "The Newton Channel". In Ross Anderson (Editor), *Information Hiding, Proceedings*, volume 1174 of *Lecture Notes in Computer Science*, pages 151–156. Springer, 1996. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/newtchan.pdf.
43. Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller and Bruce Schneier. "The risks of key recovery, key escrow, and trusted third-party encryption". *World Wide Web Journal*, **2**:241–257, 1997. URL https://dspace.mit.edu/handle/1721.1/117329.
44. Ross Anderson (Editor). *Personal Medical Information – Security, Engineering, and Ethics*. Springer, 1997. URL https://doi.org/10.1007/978-3-642-59023-8.
45. Ross Anderson. "Problems with the NHS cryptography strategy", 1997. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/zergo-critique.pdf.
46. Ross Anderson. "An Update on the BMA Security Policy". In Ross Anderson (Editor), *Personal Medical Information – Security, Engineering, and Ethics*, pages 233–250. Springer, 1997. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/bmaupdate.pdf.
47. Ross Anderson and Andreas von Heydwolff. "Eine klare Sicherheitspolitik für klinische Informationssysteme". *Datenschutz und Datensicherheit*, **21**(10):569–574, 1997.
48. Ross Anderson, Václav Matyás Jr., Fabien A. P. Petitcolas, Iain E. Buchan and Rudolf Hanka. "Secure Books: Protecting the Distribution of Knowledge". In Bruce Christianson, Bruno Crispo, T. Mark A. Lomas and Michael Roe (Editors), *Security Protocols V*, volume 1361 of *Lecture Notes in Computer Science*, pages 1–11. Springer, 1997. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/wax-securebook.pdf.
49. Ross Anderson, Grant Kelly and Mike Wells. "A new IT strategy for healthcare", 1997. URL https://fipr.org/110112briefing1997.pdf.
50. Ross Anderson and Markus G. Kuhn. "Low Cost Attacks on Tamper Resistant Devices". In Bruce Christianson, Bruno Crispo, T. Mark A. Lomas and Michael Roe (Editors), *Security Protocols V*, volume 1361 of *Lecture Notes in Computer Science*, pages 125–136. Springer, 1997. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/tamper2.pdf.
51. Ross Anderson and Charalampos Manifavas. "Chameleon – A New Kind of Stream Cipher". In Eli Biham (Editor), *Fast Software Encryption*, volume 1267 of *Lecture*

Notes in Computer Science, pages 107–113. Springer, 1997. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/chameleon.pdf.

52. Ross Anderson and Michael Roe. "The GCHQ Protocol and Its Problems". In Walter Fumy (Editor), *Advances in Cryptology – EUROCRYPT*, volume 1233 of *Lecture Notes in Computer Science*, pages 134–148. Springer, 1997. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/euroclipper.pdf.
53. Markus G. Kuhn and Ross Anderson. "Patent GB2330924: Software piracy detector sensing electromagnetic computer emanations", 1997. URL https://www.search-for-intellectual-property.service.gov.uk/GB2330924.
54. Ross Anderson. "The DeCODE Proposal for an Icelandic Health Database". *Læknablaðið (The Icelandic Medical Journal)*, **84**(11):874–875, 1998. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/iceland.pdf.
55. Ross Anderson (Editor). *Health Informatics Journal*, volume 4(3–4). 1998.
56. Ross Anderson. "Healthcare Protection Profile – Comments", 1998. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/healthpp.pdf.
57. Ross Anderson (Editor). *IEEE Journal on Selected Areas in Communications*, volume 16(4). 1998.
58. Ross Anderson. "On the Security of Digital Tachographs". In Jean-Jacques Quisquater, Yves Deswarte, Catherine Meadows and Dieter Gollmann (Editors), *Computer Security – ESORICS*, volume 1485 of *Lecture Notes in Computer Science*, pages 111–125. Springer, 1998. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/tacho.pdf.
59. Ross Anderson. "Safety and Privacy in Clinical Information Systems". In Jo Lenaghan (Editor), *Rethinking IT and health*, pages 140–160. Institute for Public Policy Research, 1998.
60. Ross Anderson. "Safety and Privacy in Clinical Systems: The State of Play". *Health Informatics Journal*, **4**(3-4):121–123, 1998. URL https://doi.org/10.1177/146045829800400301.
61. Ross Anderson, Francesco Bergadano, Bruno Crispo, Jong-Hyeon Lee, Charalampos Manifavas and Roger M. Needham. "A New Family of Authentication Protocols". *ACM SIGOPS Operating Systems Review*, **32**(4):9–20, 1998. URL https://www.cl.cam.ac.uk/archive/rja14/fawkes.pdf.
62. Ross Anderson, Eli Biham and Lars Knudsen. "Serpent: A Flexible Block Cipher With Maximum Assurance". In *The First Advanced Encryption Standard Candidate Conference*. 1998. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/ventura.pdf.
63. Ross Anderson, Eli Biham and Lars Knudsen. "Serpent: A Proposal for the Advanced Encryption Standard", 1998. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/serpent.pdf.
64. Ross Anderson, Eli Biham and Lars R. Knudsen. "Serpent and Smartcards". In Jean-Jacques Quisquater and Bruce Schneier (Editors), *Smart Card Research and Applications CARDIS*, volume 1820 of *Lecture Notes in Computer Science*, pages 246–253. Springer, 1998. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/serpent_card_final.pdf.
65. Ross Anderson and Caspar Bowden. "Signature Directive Consultation", 1998. URL http://www.cl.cam.ac.uk/users/rja14/signaturedoc.html.
66. Ross Anderson, Bruno Crispo, Jong-Hyeon Lee, Charalampos Manifavas, Fabien Petitcolas and Václav Matyás Jr. *The Global Trust Register 1998*. Northgate Consultants, 1998.

67. Ross Anderson, Cunsheng Ding, Tor Helleseth and Torleiv Kløve. "How to Build Robust Shared Control Systems". *Designs Codes and Cryptography*, **15**(2):111–124, 1998. URL https://cse.hkust.edu.hk/faculty/cding/JOURNALS/dcc981.pdf.
68. Ross Anderson, Václav Matyás Jr. and Fabien A. P. Petitcolas. "The Eternal Resource Locator: An Alternative Means of Establishing Trust on the World Wide Web". In Bennet S. Yee (Editor), *USENIX Workshop on Electronic Commerce*. 1998. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/ec98-erl.pdf.
69. Ross Anderson and Abida Khattak. "The Use of Information Retrieval Techniques for Intrusion Detection". In *Recent Advances in Intrusion Detection*. 1998. URL https://research.cs.umbc.edu/cadip/readings/DMID/raid.pdf.
70. Ross Anderson and Simon W. Moore. "Patent GB2365153: Microprocessor resistant to power analysis", 1998. URL https://www.search-for-intellectual-property.service.gov.uk/GB2365153.
71. Ross Anderson, Roger M. Needham and Adi Shamir. "The Steganographic File System". In David Aucsmith (Editor), *Information Hiding, Proceedings*, volume 1525 of *Lecture Notes in Computer Science*, pages 73–82. Springer, 1998. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/onanewwo-fs.pdf.
72. Ross Anderson and Fabien A. P. Petitcolas. "On the Limits of Steganography". *IEEE Journal of Selected Areas in Communications*, **16**(4):474–481, 1998. URL https://www.cl.cam.ac.uk/archive/rja14/jsac98-limsteg.pdf.
73. Eli Biham, Ross Anderson and Lars R. Knudsen. "Serpent: A New Block Cipher Proposal". In Serge Vaudenay (Editor), *Fast Software Encryption*, volume 1372 of *Lecture Notes in Computer Science*, pages 222–238. Springer, 1998. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/serpent0.pdf.
74. Markus G. Kuhn and Ross Anderson. "Patent GB2333883: Low Cost Countermeasures Against Compromising Electromagnetic Computer Emanations", 1998. URL https://www.search-for-intellectual-property.service.gov.uk/GB2333883.
75. Markus G. Kuhn and Ross Anderson. "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations". In David Aucsmith (Editor), *Information Hiding, Proceedings*, volume 1525 of *Lecture Notes in Computer Science*, pages 124–142. Springer, 1998. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/ih98-tempest-old.pdf.
76. Fabien A. P. Petitcolas, Ross Anderson and Markus G. Kuhn. "Attacks on Copyright Marking Systems". In David Aucsmith (Editor), *Information Hiding, Proceedings*, volume 1525 of *Lecture Notes in Computer Science*, pages 218–238. Springer, 1998. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/ih98-attacks.pdf.
77. Ross Anderson. "Comments on the Security Targets for the Icelandic Health Database", 1999. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/iceland-admiral.pdf.
78. Ross Anderson. "FIPR Consultation Response – Framework for Smart Card Use in Government", 1999. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/smartcards-fipr.pdf.
79. Ross Anderson. "The Formal Verification of a Payment System". In Michael G. Hinchey and Jonathan P. Bowen (Editors), *Industrial-Strength Formal Methods in Practice*, pages 43–52. Springer, 1999. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/uepsbook.pdf.

80. Ross Anderson. "How to Cheat at the Lottery (or, Massively Parallel Requirements Engineering)". In *Annual Computer Security Applications Conference (ACSAC)*. IEEE Computer Society, 1999. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/lottery.pdf`.
81. Ross Anderson. "Information technology in medical practice: safety and privacy lessons from the United Kingdom". *Medical Journal of Australia*, pages 181–184, 1999. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/ausmedjour.pdf`.
82. Ross Anderson. "The Millennium Bug – Reasons not to Panic", 1999. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/y2k.pdf`.
83. Ross Anderson. "The Risks and Costs of UK Escrow Policy". In *UK House of Commons Trade and Industry Committee, Seventh report, Session 1998–99*. HM Stationery Office, 1999. URL `http://www.cl.cam.ac.uk/users/rja14/dtiselcom.html`.
84. Ross Anderson, Bruno Crispo, Jong-Hyeon Lee, Charalampos Manifavas, Fabien Petitcolas and Václav Matyás Jr. *The Global Internet Trust Register 1999*. MIT Press, 1999.
85. Ross Anderson and Markus G. Kuhn. "Soft Tempest – An Opportunity for NATO". In *Protecting NATO Information Systems in the 21st century, NATO RTO-MP-27 AC/323(IST)TP/3*, pages 5.1–5.5. 1999. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/nato-tempest.pdf`.
86. Ross Anderson and Jong-Hyeon Lee. "Jikzi: A New Framework for Secure Publishing". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols VII*, volume 1796 of *Lecture Notes in Computer Science*, pages 21–47. Springer, 1999. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/jikzi-cpw.pdf`.
87. Robert M. Brady, Ross Anderson and Robin C. Ball. "Murphy's law, the fitness of evolving species, and the limits of software reliability". Technical report, University of Cambridge, Computer Laboratory, 1999. URL `https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-471.pdf`.
88. Fabien A. P. Petitcolas and Ross Anderson. "Evaluation of Copyright Marking Systems". In *IEEE International Conference on Multimedia Computing and Systems, ICMCS*, volume I, pages 574–579. 1999. URL `https://www.petitcolas.net/fabien/publications/ieeemm99-evaluation.pdf`.
89. Fabien A. P. Petitcolas, Ross Anderson and Markus G. Kuhn. "Information Hiding – A Survey". *Proceedings of the IEEE*, **87**(7):1062–1078, 1999. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/ieee99-infohiding.pdf`.
90. Frank Stajano and Ross Anderson. "The Cocaine Auction Protocol: On the Power of Anonymous Broadcast". In Andreas Pfitzmann (Editor), *Information Hiding, Proceedings*, volume 1768 of *Lecture Notes in Computer Science*, pages 434–447. Springer, 1999. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/cocaine.pdf`.
91. Frank Stajano and Ross Anderson. "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols VII*, volume 1796 of *Lecture Notes in Computer Science*, pages 172–194. Springer, 1999. URL `https://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf`.
92. Ross Anderson. "The Correctness of Crypto Transaction Sets". In Bruce Christianson, Bruno Crispo and Michael Roe (Editors), *Security Protocols VIII*, volume 2133 of *Lecture Notes in Computer Science*, pages 125–127. Springer, 2000. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/protocols00.pdf`.

93. Ross Anderson. "The Correctness of Crypto Transaction Sets (Discussion)". In Bruce Christianson, Bruno Crispo and Michael Roe (Editors), *Security Protocols VIII*, volume 2133 of *Lecture Notes in Computer Science*, pages 128–141. Springer, 2000. URL https://doi.org/10.1007/3-540-44810-1_18.
94. Ross Anderson. "Digital Signature". In Anthony Ralston, David Hemmendinger and Edwin D Reilly (Editors), *Encyclopedia of Computer Science*, pages 581–583. Grove's Dictionaries, fourth edition, 2000.
95. Ross Anderson. "Privacy Technology Lessons from Healthcare". In *IEEE Symposium on Security and Privacy*, pages 78–79. 2000. URL https://doi.org/10.1109/SECPRI.2000.848466.
96. Ross Anderson, Eli Biham and Lars R. Knudsen. "The Case for Serpent". In *The Third Advanced Encryption Standard Candidate Conference*, pages 349–354. National Institute of Standards and Technology,, 2000. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/serpentcase.pdf.
97. Ross Anderson, Terry Bollinger, Doug Brown, Enrique Draier, Philip Machanick, Gary McGraw, Nancy R. Mead, Arthur B. Pyster, Howard Schmidt and Timothy J. Shimeall. "Roundtable on Information Security Policy". *IEEE Software*, **17**(5):26–32, 2000. URL https://doi.org/10.1109/MS.2000.10046.
98. Ross Anderson and Jong-Hyeon Lee. "Jikzi – a new framework for security policy, trusted publishing and electronic commerce". *Computer Communications*, **23**(17):1621–1626, 2000. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/jikzi.pdf.
99. Simon W. Moore, Ross Anderson and Markus G. Kuhn. "Improving Smartcard Security using Self-Timed Circuit Technology". In *Fourth AciD-WG Workshop*. 2000.
100. Michael Roe, Ross Anderson, William S. Harbison and T. Mark A. Lomas. "Government Access to Keys – Panel Discussion". In Bruce Christianson, Bruno Crispo and Michael Roe (Editors), *Security Protocols VIII*, volume 2133 of *Lecture Notes in Computer Science*, pages 62–73. Springer, 2000. URL https://doi.org/10.1007/3-540-44810-1_10.
101. Frank Stajano and Ross Anderson. "The Grenade Timer: Fortifying the Watchdog Timer Against Malicious Mobile Code". In *7th International Workshop on Multimedia Mobile Communications*. 2000. URL https://www.cl.cam.ac.uk/archive/rja14/grenade.pdf.
102. Jianxin Yan, Alan Blackwell, Ross Anderson and Alasdair Grant. "The memorability and security of passwords – some empirical results". Technical Report UCAM-CL-TR-500, University of Cambridge, Computer Laboratory, 2000. URL https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-500.pdf.
103. Jianxin Yan, Stephen Early and Ross Anderson. "The XenoService – A Distributed Defeat for Distributed Denial of Service". In *Information Survivability Workshop*. 2000. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/xeno.pdf.
104. Ross Anderson. "Commonsense in the Crisis", 2001. URL https://www.cl.cam.ac.uk/archive/rja14/wtc.html.
105. Ross Anderson. "Protecting Embedded Systems – The Next Ten Years". In Çetin Kaya Koç, David Naccache and Christof Paar (Editors), *Cryptographic Hardware and Embedded Systems – CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 1–2. Springer, 2001. URL https://doi.org/10.1007/3-540-44709-1_1.
106. Ross Anderson. *Security Engineering – A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, 2001.

107. Ross Anderson. "Undermining data privacy in health information". *British Medical Journal*, **322**(7284):442–443, 2001. URL `https://pmc.ncbi.nlm.nih.gov/articles/PMC1119671/`.
108. Ross Anderson. "Why Information Security is Hard: An Economic Perspective". In *Annual Computer Security Applications Conference (ACSAC)*, pages 358–365. IEEE Computer Society, 2001. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/econ.pdf`.
109. Ross Anderson, Frank Stajano and Jong-Hyeon Lee. "Security policies". *Advances in Computers*, **55**:185–235, 2001. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/security-policies.pdf`.
110. Mike Bond and Ross Anderson. "API-Level Attacks on Embedded Systems". *Computer*, **34**(10):67–75, 2001. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/API-Attacks.pdf`.
111. Ross Anderson. "Free Speech Online and Offline". *Computer*, **35**(6):28–30, 2002. URL `https://doi.org/10.1109/MC.2002.1009163`.
112. Ross Anderson. "Free speech online and offline". *Communications of the ACM*, **45**(6):120, 2002. URL `https://doi.org/10.1145/508448.508479`.
113. Ross Anderson. "Security in Open versus Closed Systems – The Dance of Boltzmann, Coase and Moore". In *Open Source Software : Economics, Law and Policy*. 2002. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/toulouse.pdf`.
114. Ross Anderson. "TCPA/Palladium frequently asked questions". *Computer Security Journal*, **18**(3–4):63–70, 2002.
115. Ross Anderson. "Two remarks on public key cryptology". Technical Report UCAM-CL-TR-549, University of Cambridge, Computer Laboratory, 2002. URL `https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-549.pdf`.
116. Ross Anderson. "Unsettling Parallels Between Security and the Environment". In *Workshop on Economics and Information Security*. 2002. URL `https://web.archive.org/web/20120214110013/http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/37.txt`.
117. Simon W. Moore, Ross Anderson, Paul A. Cunningham, Robert D. Mullins and George S. Taylor. "Improving Smart Card Security Using Self-Timed Circuits". In *International Symposium on Advanced Research in Asynchronous Circuits and Systems (ASYNC)*, pages 211–218. 2002. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/async2002paperV2.pdf`.
118. David Samyde, Sergei P. Skorobogatov, Ross Anderson and Jean-Jacques Quisquater. "On a New Way to Read Data from Memory". In *Proceedings of the First International IEEE Security in Storage Workshop*, pages 65–69. 2002. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/SISW02.pdf`.
119. Sergei P. Skorobogatov and Ross Anderson. "Optical Fault Induction Attacks". In Burton S. Kaliski Jr., Çetin Kaya Koç and Christof Paar (Editors), *Cryptographic Hardware and Embedded Systems – CHES*, volume 2523 of *Lecture Notes in Computer Science*, pages 2–12. Springer, 2002. URL `https://www.cl.cam.ac.uk/archive/rja14/faultpap3.pdf`.
120. Frank Stajano and Ross Anderson. "The Resurrecting Duckling: security issues for ubiquitous computing". *Computer*, **35**(4):supl22–supl26, 2002. URL `https://www.cl.cam.ac.uk/archive/rja14/Papers/ducklingieee-final.pdf`.
121. Ellis Weinberger, Richard Clayton and Ross Anderson. "Security in a digital repository". *National Preservation Office Journal*, **11**:12–13, 2002.

122. Ross Anderson. "Cryptography and Competition Policy – Issues with 'Trusted Computing"'. In *Workshop on Economics and Information Security*. 2003. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/tcpa.pdf.
123. Ross Anderson. "Cryptography and competition policy: issues with 'Trusted Computing"'. In Elizabeth Borowsky and Sergio Rajsbaum (Editors), *Proceedings of the Twenty-Second ACM Symposium on Principles of Distributed Computing, PODC 2003*, pages 3–10. 2003. URL https://doi.org/10.1145/872035.872036.
124. Ross Anderson. "'Trusted Computing' and Competition Policy – Issues for Computing Professionals". *Upgrade*, **4**(3), 2003. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/tcpa-short.pdf.
125. Ross Anderson. "What We Can Learn from API Security (Transcript of Discussion)". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols XI*, volume 3364 of *Lecture Notes in Computer Science*, pages 288–300. Springer, 2003. URL https://doi.org/10.1007/11542322_35.
126. Simon W. Moore, Ross Anderson, Robert D. Mullins, George S. Taylor and Jacques J. A. Fournier. "Balanced self-checking asynchronous logic for smart card applications". *Microprocessors and Microsystems*, **27**(9):421–430, 2003. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/micromicro2003.pdf.
127. Ross Anderson. "Cryptography and Competition Policy – Issues with 'Trusted Computing"'. In L. Jean Camp and Stephen Lewis (Editors), *Economics of Information Security*, volume 12 of *Advances in Information Security*, pages 35–52. Springer, 2004. URL https://doi.org/10.1007/1-4020-8090-5_3.
128. Ross Anderson. "The Dancing Bear: A New Way of Composing Ciphers". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols XII*, volume 3957 of *Lecture Notes in Computer Science*, pages 231–238. Springer, 2004. URL https://www.cl.cam.ac.uk/archive/rja14/grizzle.pdf.
129. Ross Anderson. "The Dancing Bear: A New Way of Composing Ciphers (Transcript of Discussion)". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols XII*, volume 3957 of *Lecture Notes in Computer Science*, pages 239–245. Springer, 2004. URL https://doi.org/10.1007/11861386_27.
130. Ross Anderson, Alan Blackwell, Jon Crowcroft and Steven Murdoch. "Patent Application GB0426818: User interface for a computing device", 2004.
131. Ross Anderson and Michael Bond. "Protocol Analysis, Composability and Computation". In Andrew Herbert and Karen Spärck Jones (Editors), *Computer Systems: Theory, Technology, and Applications*, pages 15–19. Springer, 2004. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/bond-anderson.pdf.
132. Ross Anderson, Haowen Chan and Adrian Perrig. "Key Infection: Smart Trust for Smart Dust". In *IEEE International Conference on Network Protocols (ICNP)*, pages 206–215. 2004. URL https://www.cl.cam.ac.uk/archive/rja14/key-infection.pdf.
133. Ross Anderson and Teresa Hackett. "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", 2004. URL https://www.edri.org/files/edri_response_review.pdf.
134. George Danezis and Ross Anderson. "The Economics of Censorship Resistance". In *Workshop on Economics and Information Security*. 2004. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/redblue.pdf.

135. Andrei Serjantov and Ross Anderson. "On Dealing with Adversaries Fairly". In *Workshop on Economics and Information Security*. 2004. URL https://www.cl.cam.ac.uk/archive/rja14/fair4.pdf.
136. Jeff Jianxin Yan, Alan F. Blackwell, Ross Anderson and Alasdair Grant. "Password Memorability and Security: Empirical Results". *IEEE Security and Privacy*, **2**(5):25–31, 2004. URL https://prof-jeffyan.github.io/jyan_ieee_pwd.pdf.
137. Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Ross Anderson and Ron Rivest. "A Note on EMV Secure Messaging in the IBM 4758 CCA", 2005. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/CCA-EMV.pdf.
138. Ross Anderson. "The Initial Costs and Maintenance Costs of Protocols". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols XIII*, volume 4631 of *Lecture Notes in Computer Science*, pages 333–335. Springer, 2005. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/protocols05.pdf.
139. Ross Anderson. "The Initial Costs and Maintenance Costs of Protocols (Transcript of Discussion)". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols XIII*, volume 4631 of *Lecture Notes in Computer Science*, pages 336–343. Springer, 2005. URL https://doi.org/10.1007/978-3-540-77156-2_43.
140. Ross Anderson. "The Pastoral Repertoire, Rediscovered". *Common Stock*, **20**(2):24–30, 2005. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/pastoral.pdf.
141. Ross Anderson. "System Security for Cyborgs". In *2nd International Workshop on Wearable and Implantable Body Sensor Networks*, pages 36–39. 2005. URL https://www.cl.cam.ac.uk/archive/rja14/cyborg.pdf.
142. Ross Anderson, Mike Bond, Jolyon Clulow and Sergei Skorobogatov. "Cryptographic processors – a survey". Technical Report UCAM-CL-TR-641, University of Cambridge, Computer Laboratory, 2005. URL https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-641.pdf.
143. Ross Anderson and Bruce Schneier. "Guest Editors' Introduction: Economics of Information Security". *IEEE Security and Privacy*, **3**(1):12–13, 2005. URL https://doi.org/10.1109/MSP.2005.14.
144. George Danezis and Ross Anderson. "The Economics of Resisting Censorship". *IEEE Security and Privacy*, **3**(1):45–50, 2005. URL https://doi.org/10.1109/MSP.2005.29.
145. George Danezis, Chris Lesniewski-Laas, M. Frans Kaashoek and Ross Anderson. "Sybil-Resistant DHT Routing". In Sabrina De Capitani di Vimercati, Paul F. Syverson and Dieter Gollmann (Editors), *Computer Security – ESORICS*, volume 3679 of *Lecture Notes in Computer Science*, pages 305–318. Springer, 2005. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/sybildht.pdf.
146. George Danezis, Stephen Lewis and Ross Anderson. "How Much Is Location Privacy Worth?" In *Workshop on the Economics of Information Security*. 2005. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/location-privacy.pdf.
147. Feng Hao, Ross Anderson and John Daugman. "Combining cryptography with biometrics effectively". Technical Report UCAM-CL-TR-640, University of Cambridge, Computer Laboratory, 2005. URL https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-640.pdf.
148. Tyler Moore and Ross Anderson. "Trends in Security Economics". *European Network and Information Security Agency Quarterly*, **1**(3):6–7, 2005.

149. Shishir Nagaraja and Ross Anderson. "The topology of covert conflict". Technical Report UCAM-CL-TR-637, University of Cambridge, Computer Laboratory, 2005. URL https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-637.pdf.
150. Jeff Yan, Alan Blackwell, Ross Anderson and Alasdair Grant. "The Memorability and Security of Passwords". In Lorrie Faith Cranor and Simson Garfinkel (Editors), *Security and usability*, pages 129–142. O'Reilly Media, 2005. URL https://www.oreilly.com/library/view/security-and-usability/0596008279/ch07.html.
151. Paul Youn, Ben Adida, Mike Bond, Jolyon Clulow, Jonathan Herzog, Amerson Lin, Ronald L. Rivest and Ross Anderson. "Robbing the bank with a theorem prover". Technical Report UCAM-CL-TR-644, University of Cambridge, Computer Laboratory, 2005. URL https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-644.pdf.
152. Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Steven J. Murdoch, Ross Anderson and Ronald L. Rivest. "Phish and Chips". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols XIV*, volume 5087 of *Lecture Notes in Computer Science*, pages 40–48. Springer, 2006. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/Phish-and-Chips.pdf.
153. Ross Anderson. "FIPR Consultation Response on: New Powers Against Organised and Financial Crime", 2006. URL https://fipr.org/061017socaresponse.pdf.
154. Ross Anderson. "FIPR Consultation Response on: Personal Internet Security", 2006. URL https://fipr.org/061023security.pdf.
155. Ross Anderson. "FIPR response to the Home Affairs Committee Inquiry into 'A Surveillance Society"', 2006. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/fipr-exportcontrol-2006.pdf.
156. Ross Anderson. "FIPR's Consultation Response on DRM", 2006. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/apig.pdf.
157. Ross Anderson. "Healthcare IT in Europe and North America", 2006. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/nao-report-final.doc.
158. Ross Anderson. "The Man-in-the-Middle Defence (Transcript of Discussion)". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols XIV*, volume 5087 of *Lecture Notes in Computer Science*, pages 157–163. Springer, 2006. URL https://doi.org/10.1007/978-3-642-04904-0_21.
159. Ross Anderson. "The Sutherland Manuscript", 2006. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/Sutherland-Manuscript.pdf.
160. Ross Anderson. "Under threat: patient confidentiality and NHS computing". *Drugs and Alcohol Today*, **6**(4):13–17, 2006. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/drugsandalcohol.pdf.
161. Ross Anderson and Mike Bond. "The Man-in-the-Middle Defence". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols XIV*, volume 5087 of *Lecture Notes in Computer Science*, pages 153–156. Springer, 2006. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/Man-in-the-Middle-Defence.pdf.
162. Ross Anderson, Mike Bond, Jolyon Clulow and Sergei Skorobogatov. "Cryptographic Processors – A Survey". *Proceedings of the IEEE*, **94**(2):357–369, 2006. URL https://doi.org/10.1109/JPROC.2005.862423.
163. Ross Anderson, Mike Bond and Steven J. Murdoch. "Chip and Spin". *Computer Security Journal*, **22**(2):1–6, 2006. URL https://www.chipandspin.co.uk/spin.pdf.

164. Ross Anderson, Ian Brown, Richard Clayton, Terri Dowty, Douwe Korff and Eileen Munro. "Children's Databases – Safety and Privacy: A Report for the Information Commissioner", 2006. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/kids.pdf.
165. Ross Anderson and Richard Clayton. "FIPR Response to the Home Office: "Consultation on the Draft Code of Practice for the Investigation of Protected Electronic Information – Part III of the Regulation of Investigatory Powers Act 2000", 2006. URL https://fipr.org/060901encryption.pdf.
166. Ross Anderson and Richard Clayton. "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", 2006. URL https://fipr.org/060901commsdata.pdf.
167. Ross Anderson and Tyler Moore. "The Economics of Information Security". *Science*, **314**(5799):610–613, 2006. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/econ_science.pdf.
168. Feng Hao, Ross Anderson and John Daugman. "Combining Crypto with Biometrics Effectively". *IEEE Transactions on Computers*, **55**(9):1081–1088, 2006. URL https://www.cse.msu.edu/~rossarun/BiometricsTextBook/Papers/Security/Hao_IrisBioCrypt_IEEEComputers06.pdf.
169. Shishir Nagaraja and Ross Anderson. "The Topology of Covert Conflict". In *Workshop on the Economics of Information Security*. 2006. URL http://weis2006.econinfosec.org/docs/38.pdf.
170. Richard E. Newman, Sherman Gavette, Larry Yonge and Ross Anderson. "Protecting domestic power-line communications". In Lorrie Faith Cranor (Editor), *Proceedings of the 2nd Symposium on Usable Privacy and Security, SOUPS*, pages 122–132. 2006. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/homeplug-soupspaper.pdf.
171. Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Ross Anderson and Ronald L. Rivest. "On the Security of the EMV Secure Messaging API (Extended Abstract)". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols XV*, volume 5964 of *Lecture Notes in Computer Science*, pages 147–149. Springer, 2007. URL https://people.csail.mit.edu/rivest/pubs/ABCLx07.pdf.
172. Ross Anderson. "Closing the phishing hole: fraud, risk, and nonbanks". In *Nonbanks in the payments system: innovation, competition, and risk: an International payments policy conference*. 2007. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/nonbanks.pdf.
173. Ross Anderson. "Open and Closed Source Systems are Equivalent (that is, in an ideal world)". In Joseph Feller, Brian Fitzgerald, Scott A Hissam and Karim R Lakhani (Editors), *Perspectives on Free and Open Source Software*, pages 127–142. MIT Press, 2007. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/toulousebook.pdf.
174. Ross Anderson. "RFID and the Middleman". In Sven Dietrich and Rachna Dhamija (Editors), *Financial Cryptography and Data Security*, volume 4886 of *Lecture Notes in Computer Science*, pages 46–49. Springer, 2007. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/rfid-fc07.pdf.
175. Ross Anderson. "Software Security: State of the Art". *IEEE Security and Privacy*, **5**(1):8, 2007. URL https://doi.ieeecomputersociety.org/10.1109/MSP.2007.18.

176. Ross Anderson, Nicholas Bohm, Brian Gladman and Paul Whitehouse. "FIPR Consultation Response on 'Framework for Information Assurance'", 2007. URL https://fipr.org/egov-framework.pdf.
177. Ross Anderson, Ian Brown, Fleur Fisher and Douwe Korff. "FIPR Consultation Response on 'The Electronic Patient Record and its Use'", 2007. URL https://publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422we22.htm.
178. Ross Anderson, Rudolf Hanka and Alan Hassey. "Clause 67, Medical Research and Privacy: the Options for the NHS", 2007. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/hcbillc67.pdf.
179. Ross Anderson and Tyler Moore. "The Economics of Information Security – A Survey and Open Questions". In *Softint 2007*. 2007. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/toulouse-summary.pdf.
180. Ross Anderson and Tyler Moore. "Information Security Economics – and Beyond". In Alfred Menezes (Editor), *Advances in Cryptology – CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 68–91. Springer, 2007. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/econ_czech.pdf.
181. Ross Anderson, Tyler Moore, Shishir Nagaraja and Andy Ozment. "Incentives and Information Security". In Noam Nisan, Tim Roughgarden, Eva Tardos and Vijay V Vazirani (Editors), *Algorithmic Game Theory*, pages 633–650. Cambridge University Press, 2007. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/book-chapter-agt-1.pdf.
182. Gary McGraw and Ross Anderson. "Silver Bullet Talks with Ross Anderson". *IEEE Security and Privacy*, **5**(4):10–13, 2007. URL https://doi.org/10.1109/MSP.2007.94.
183. Tyler Moore, Jolyon Clulow, Shishir Nagaraja and Ross Anderson. "New Strategies for Revocation in Ad-Hoc Networks". In Frank Stajano, Catherine Meadows, Srdjan Capkun and Tyler Moore (Editors), *4th European Workshop on Security and Privacy in Ad-hoc and Sensor Networks (ESAS)*, volume 4572 of *Lecture Notes in Computer Science*, pages 232–246. Springer, 2007. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/esas07.pdf.
184. Steven J. Murdoch and Ross Anderson. "Shifting Borders". *Index on Censorship*, **36**(4):156–159, 2007. URL https://murdoch.is/papers/index07borders.pdf.
185. Shishir Nagaraja and Ross Anderson. "Dynamic Topologies for Robust Scale-Free Networks". In Pietro Liò, Eiko Yoneki, Jon Crowcroft and Dinesh C. Verma (Editors), *Bio-Inspired Computing and Communication*, volume 5151 of *Lecture Notes in Computer Science*, pages 411–426. Springer, 2007. URL https://doi.org/10.1007/978-3-540-92191-2_36.
186. Richard Newman, Larry Yonge, Sherman Gavette and Ross Anderson. "HomePlug AV Security Mechanisms". In *2007 IEEE International Symposium on Power Line Communications and Its Applications*, pages 366–371. 2007. URL https://www.cise.ufl.edu/~nemo/papers/ISPLC2007_AV_Security.pdf.
187. Paul Youn, Ben Adida, Mike Bond, Jolyon Clulow, Jonathan Herzog, Amerson Lin, Ronald L. Rivest and Ross Anderson. "Robbing the Bank with a Theorem Prover – (Abstract)". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Michael Roe (Editors), *Security Protocols XV*, volume 5964 of *Lecture Notes in Computer Science*, page 171. Springer, 2007. URL https://people.csail.mit.edu/rivest/pubs/YABCx07.pdf.
188. Ross Anderson. "Confidentiality and Connecting for Health". *British Journal of General Practice*, **58**(547):75–76, 2008. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/bjgp.pdf.

189. Ross Anderson. "Connecting for Health". *British Journal of General Practice*, **58**(549):279–280, 2008. URL https://bjgp.org/content/58/549/279.full.pdf.
190. Ross Anderson. "Failures on Fraud". *Speed*, **3**(2), 2008. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/fraudfailures.pdf.
191. Ross Anderson. "Information Security Economics – and Beyond". In Ron van der Meyden and Leendert W. N. van der Torre (Editors), *Deontic Logic in Computer Science DEON*, volume 5076 of *Lecture Notes in Computer Science*, page 49. Springer, 2008. URL https://doi.org/10.1007/978-3-540-70525-3_5.
192. Ross Anderson. *Security Engineering – A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, second edition, 2008.
193. Ross Anderson. "Security, Functionality and Scale? (invited talk)". In Vijay Atluri (Editor), *Data and Applications Security*, volume 5094 of *Lecture Notes in Computer Science*, page 64. Springer, 2008. URL https://link.springer.com/content/pdf/10.1007/978-3-540-70567-3_5.pdf.
194. Ross Anderson. "What Next After Anonymity? (Transcript of Discussion)". In Bruce Christianson, James A. Malcolm, Vashek Matyáš and Michael Roe (Editors), *Security Protocols XVI*, volume 6615 of *Lecture Notes in Computer Science*, pages 223–231. Springer, 2008. URL https://doi.org/10.1007/978-3-642-22137-8_30.
195. Ross Anderson and Nicholas Bohm. "FIPR Submission to The Hunt Review of the Financial Ombudsman Service", 2008. URL https://fipr.org/080116huntreview.pdf.
196. Ross Anderson, Nicholas Bohm, Terri Dowty, Fleur Fisher, Douwe Korff, Eileen Munro and Martyn Thomas. "FIPR Consultation Response on The Data Sharing Review", 2008. URL https://fipr.org/080215datasharing.pdf.
197. Ross Anderson, Nicholas Bohm and Martyn Thomas. "FIPR Consultation Response on The National Payments Plan", 2008. URL https://fipr.org/080204payments.pdf.
198. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore. "Security Economics and European Policy". In *Workshop on Economics and Information Security*. 2008. URL https://econinfosec.org/archive/weis2008/papers/MooreSecurity.pdf.
199. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore. "Security Economics and European Policy". In Norbert Pohlmann, Helmut Reimer and Wolfgang Schneider (Editors), *Information Security Solutions Europe (ISSE)*, pages 57–76. Vieweg+Teubner, 2008. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/enisareport-isse.pdf.
200. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore. *Security Economics and the Internal Market*. ENISA, 2008. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/enisareport-full.pdf.
201. Ross Anderson and Steven J. Murdoch. "What Next after Anonymity?" In Bruce Christianson, James A. Malcolm, Vashek Matyáš and Michael Roe (Editors), *Security Protocols XVI*, volume 6615 of *Lecture Notes in Computer Science*, pages 220–222. Springer, 2008. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/afteranonymity.pdf.
202. Saar Drimer, Steven J. Murdoch and Ross Anderson. "Thinking inside the box: system-level failures of tamper proofing". Technical Report UCAM-CL-TR-711, University of Cambridge, Computer Laboratory, 2008. URL https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-711.pdf.

203. Saar Drimer, Steven J. Murdoch and Ross Anderson. "Thinking Inside the Box: System-Level Failures of Tamper Proofing". In *IEEE Symposium on Security and Privacy*, pages 281–295. 2008. URL https://doi.org/10.1109/SP.2008.16.
204. Tyler Moore and Ross Anderson. "How brain type influences online safety". In *Security and Human Behavior*. 2008. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/eqsqphish.pdf.
205. Tyler Moore, Maxim Raya, Jolyon Clulow, Panagiotis Papadimitratos, Ross Anderson and Jean-Pierre Hubaux. "Fast Exclusion of Errant Devices from Vehicular Networks". In *IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON*, pages 135–143. 2008. URL https://tylermoore.utulsa.edu/secon08.pdf.
206. Steven J. Murdoch and Ross Anderson. "Tools and Technology of Internet Filtering". In *Access Denied: The Practice and Policy of Global Internet Filtering*, pages 57–72. The MIT Press, 2008. URL https://doi.org/10.7551/mitpress/7617.003.0006.
207. Ross Anderson. "Cambridge University – the Unauthorised History", 2009. URL https://www.cl.cam.ac.uk/archive/rja14/unauthorised.html.
208. Ross Anderson. "The Devil's flame-thrower". *Times Higher Education Supplement*, Feb 5, 2009. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/governance-feb09.pdf.
209. Ross Anderson. "FIPR Consultation Response on Civil Litigation Costs Review", 2009. URL https://fipr.org/090730jackson.pdf.
210. Ross Anderson. "Technical perspective – A chilly sense of security". *Communications of the ACM*, **52**(5):90, 2009. URL https://dl.acm.org/doi/pdf/10.1145/1506409.1506428.
211. Ross Anderson. "The Trust Economy of Brief Encounters". In Bruce Christianson, James A. Malcolm, Vashek Matyáš and Michael Roe (Editors), *Security Protocols XVII*, volume 7028 of *Lecture Notes in Computer Science*, pages 282–284. Springer, 2009. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/spw09.pdf.
212. Ross Anderson. "The Trust Economy of Brief Encounters (Transcript of Discussion)". In Bruce Christianson, James A. Malcolm, Vashek Matyáš and Michael Roe (Editors), *Security Protocols XVII*, volume 7028 of *Lecture Notes in Computer Science*, pages 285–297. Springer, 2009. URL https://link.springer.com/chapter/10.1007/978-3-642-36213-2_32.
213. Ross Anderson. "What's academic freedom anyway?" *Oxford Magazine*, Feb 19, 2009. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/ac-freedom.pdf.
214. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore. "Security Economics and European Policy". In M. Eric Johnson (Editor), *Managing Information Risk and the Economics of Security*, pages 55–80. Springer, 2009. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/enisa-short.pdf.
215. Ross Anderson, Ian Brown, Terri Dowty, Philip Inglesant, William Heath and Angela Sasse. *Database State*. Joseph Rowntree Reform Trust, 2009. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/database-state.pdf.
216. Ross Anderson and Shailendra Fuloria. "Certification and Evaluation: A Security Economics Perspective". In *IEEE Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–7. 2009. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/certi_eval.pdf.

217. Ross Anderson and Shailendra Fuloria. "Security Economics and Critical National Infrastructure". In *Workshop on Economics and Information Security*. 2009. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/econ-cni09.pdf.
218. Ross Anderson and Jim Killock. "FIPR and ORG Consultation Response on Interception Modernisation or 'Protecting the Public"', 2009. URL https://fipr.org/090722imp.pdf.
219. Ross Anderson and Jim Killock. "FIPR and ORG Consultation Response on Regulation of Investigatory Powers Act 2000 Consolidating Orders and Codes of Practice", 2009. URL https://fipr.org/090714rip.pdf.
220. Ross Anderson and Tyler Moore. "Information security: where computer science, economics and psychology meet". *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, **367**(1898):2717–2727, 2009. URL https://doi.org/10.1098/rsta.2009.0027.
221. Joseph Bonneau, Jonathan Anderson, Ross Anderson and Frank Stajano. "Eight friends are enough: Social graph approximation via public listings". In Tao Stein and Meeyoung Cha (Editors), *ACM EuroSys Workshop on Social Network Systems (SNS)*, pages 13–18. 2009. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/8_friends_paper.pdf.
222. Joseph Bonneau, Sören Preibusch, Jonathan Anderson, Richard Clayton and Ross Anderson. "Democracy Theatre: Comments on Facebook's Proposed Governance Scheme", 2009. URL https://jbonneau.com/doc/BPACA09-unpublished-facebook_comments.pdf.
223. Saar Drimer, Steven J. Murdoch and Ross Anderson. "Failures of Tamper-Proofing in PIN Entry Devices". *IEEE Security and Privacy*, **7**(6):39–45, 2009. URL https://murdoch.is/papers/ieeesp09tamper.pdf.
224. Saar Drimer, Steven J. Murdoch and Ross Anderson. "Optimised to Fail: Card Readers for Online Banking". In Roger Dingledine and Philippe Golle (Editors), *Financial Cryptography and Data Security*, volume 5628 of *Lecture Notes in Computer Science*, pages 184–200. Springer, 2009. URL https://murdoch.is/papers/fc09optimised.pdf.
225. Tyler Moore, Richard Clayton and Ross Anderson. "The Economics of Online Crime". *Journal of Economic Perspectives*, **23**(3):3–20, 2009. URL https://www.aeaweb.org/articles?id=10.1257/jep.23.3.3.
226. Shishir Nagaraja and Ross Anderson. "The snooping dragon: social-malware surveillance of the Tibetan movement". Technical Report UCAM-CL-TR-746, University of Cambridge, Computer Laboratory, 2009. URL https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf.
227. Ross Anderson. "Do summary care records have the potential to do more harm than good? Yes". *British Medical Journal*, Jun 16, 2010. URL https://www.bmj.com/content/340/bmj.c3020.
228. Ross Anderson. "FIPR Consultation Response on 'An Information Revolution' – the latest NHS IT Strategy", 2010. URL https://fipr.org/110112nhsit.pdf.
229. Ross Anderson. "FIPR Consultation Response on Smart Metering", 2010. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/fipr-smartmeters2010.pdf.
230. Ross Anderson. "FIPR Consultation Response on Smart Meters", 2010. URL https://fipr.org/100110smartmeters.pdf.
231. Ross Anderson. "It's the Anthropology, Stupid! (Transcript of Discussion)". In Bruce Christianson and James A. Malcolm (Editors), *Security Protocols XVIII*, volume 7061 of *Lecture Notes in Computer Science*, pages 131–141. Springer,

2010. URL https://link.springer.com/content/pdf/10.1007/978-3-662-45921-8_21.pdf.

232. Ross Anderson and Shailendra Fuloria. "On the Security Economics of Electricity Metering". In *Workshop on the Economics of Information Security*. 2010. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/meters-weis.pdf.
233. Ross Anderson and Shailendra Fuloria. "Security Economics and Critical National Infrastructure". In Tyler Moore, David Pym and Christos Ioannidis (Editors), *Economics of Information Security and Privacy*, pages 55–66. Springer, 2010. URL https://doi.org/10.1007/978-1-4419-6967-5_4.
234. Ross Anderson and Shailendra Fuloria. "Who Controls the off Switch?" In *IEEE International Conference on Smart Grid Communications*, pages 96–101. 2010. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/meters-offswitch.pdf.
235. Ross Anderson, Shailendra Fuloria, Kevin McGrath, Kai Hansen and Fernando Alvarez. "The Protection of Substation Communications". In *Proceedings of SCADA Security Scientific Symposium*, pages 1–13. 2010. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/S4-2010.pdf.
236. Ross Anderson and Frank Stajano. "It's the Anthropology, Stupid!" In Bruce Christianson and James A. Malcolm (Editors), *Security Protocols XVIII*, volume 7061 of *Lecture Notes in Computer Science*, pages 127–130. Springer, 2010. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/hbac.pdf.
237. Shailendra Fuloria, Ross Anderson, Fernando Alvarez and Kevin McGrath. "Key Management for Substations: Symmetric Keys, Public Keys or No Keys?" In *IEEE Power Systems Conference and Exhibition (PSCE 2010)*. 2010. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/IEEE-PSCE-1.pdf.
238. Hyoungshick Kim, Jun Ho Huh and Ross Anderson. "On the Security of Internet Banking in South Korea". Technical Report RR-10-01, Oxford University, Computing Science, 2010. URL https://www.cs.ox.ac.uk/files/2782/RR-10-01.pdf.
239. Steven J. Murdoch and Ross Anderson. "Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication". In Radu Sion (Editor), *Financial Cryptography and Data Security*, volume 6052 of *Lecture Notes in Computer Science*, pages 336–342. Springer, 2010. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/fc10vbvsecurecode.pdf.
240. Steven J. Murdoch, Saar Drimer, Ross Anderson and Mike Bond. "Chip and PIN is Broken". In *IEEE Symposium on Security and Privacy*, pages 433–446. 2010. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/nopin-final-submitted.pdf.
241. Ross Anderson. "Can We Fix the Security Economics of Federated Authentication?" In Bruce Christianson, Bruno Crispo, James A. Malcolm and Frank Stajano (Editors), *Security Protocols XIX*, volume 7114 of *Lecture Notes in Computer Science*, pages 25–32. Springer, 2011. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/sefa-pr11.pdf.
242. Ross Anderson. "Can We Fix the Security Economics of Federated Authentication? (Transcript of Discussion)". In Bruce Christianson, Bruno Crispo, James A. Malcolm and Frank Stajano (Editors), *Security Protocols XIX*, volume 7114 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 2011. URL https://link.springer.com/chapter/10.1007/978-3-642-25867-1_5.
243. Ross Anderson. "Cryptology: Where Is the New Frontier?" In Daniel J. Bernstein and Sanjit Chatterjee (Editors), *Progress in Cryptology – INDOCRYPT*, volume

7107 of *Lecture Notes in Computer Science*, page 160. Springer, 2011. URL https://link.springer.com/chapter/10.1007/978-3-642-25578-6_13.

244. Ross Anderson. "The Dependability of Complex Socio-technical Systems". In Dimitra Giannakopoulou and Fernando Orejas (Editors), *Fundamental Approaches to Software Engineering – 14th International Conference, FASE 2011, Proceedings*, volume 6603 of *Lecture Notes in Computer Science*, page 1. Springer, 2011. URL https://link.springer.com/chapter/10.1007/978-3-642-19811-3_1.
245. Ross Anderson. "FIPR Consultation Response on data access and privacy for smart meters", 2011. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/fipr-sm-privacy2011.pdf.
246. Ross Anderson. "FIPR Consultation Response on license conditions and technical specifications for the rollout of smart meters", 2011. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/fipr-sm-rollout2011.pdf.
247. Ross Anderson. "FIPR Consultation Response on Making Open Data Real", 2011. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/fipr-open-data-real-2011.pdf.
248. Ross Anderson, Mike Bond, Omar Choudary, Steven J. Murdoch and Frank Stajano. "Might Financial Cryptography Kill Financial Innovation? – The Curious Case of EMV". In George Danezis (Editor), *Financial Cryptography and Data Security*, volume 7035 of *Lecture Notes in Computer Science*, pages 220–234. Springer, 2011. URL https://www.cl.cam.ac.uk/~osc22/docs/fc11_p2pemv.pdf.
249. Ross Anderson and Shailendra Fuloria. "Smart meter security: a survey", 2011. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/JSAC-draft.pdf.
250. Ross Anderson, Shailendra Fuloria and Éireann Leverett. "Data Privacy and Security for Smart Meters – Response to Ofgem's Consultation", 2011. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/DECC-sm-final.pdf.
251. Shailendra Fuloria and Ross Anderson. "Towards a security architecture for substations". In *IEEE PES International Conference and Exhibition on "Innovative Smart Grid Technologies"*, pages 1–6. 2011. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/substation-arch.pdf.
252. Chris Hall, Ross Anderson, Richard Clayton, Evangelos Ouzounis and Panagiotis Trimintzios. "Resilience of the Internet Interconnection Ecosystem". In Bruce Schneier (Editor), *Economics of Information Security and Privacy*, pages 119–148. Springer, 2011. URL https://link.springer.com/chapter/10.1007/978-1-4614-1981-5_6.
253. Chris Hall, Ross Anderson, Richard Clayton, Evangelos Ouzounis and Panagiotis Trimintzios. "Resilience of the Internet Interconnection Ecosystem". In *Workshop on the Economics of Information Security*. 2011. URL https://www.cl.cam.ac.uk/~rnc1/weisresilience.pdf.
254. Tyler Moore and Ross Anderson. "Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research". Technical Report TR-03-11, Harvard Computer Science Group, 2011. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/moore-anderson-infoeconsurvey2011.pdf.
255. Ross Anderson. "Ethics Committees and IRBs: Boon, or Bane, or More Research Needed?" In Jim Blythe, Sven Dietrich and L. Jean Camp (Editors), *Financial Cryptography and Data Security*, volume 7398 of *Lecture Notes in Computer Science*, pages 133–135. Springer, 2012. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/wecsr-2012.pdf.

256. Ross Anderson. "FIPR Written evidence to the Information Commissioner on the Draft Anonymisation Code of Practice", 2012. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/fipr-ico-anoncop-2012.pdf.
257. Ross Anderson. "The privacy of our medical records is being sold off". *The Guardian*, Aug 28, 2012. URL https://www.theguardian.com/commentisfree/2012/aug/28/code-practice-medical-data-vulnerable.
258. Ross Anderson. "Protocol Governance: The Elite, or the Mob?" In Bruce Christianson, James A. Malcolm, Frank Stajano and Jonathan Anderson (Editors), *Security Protocols XX*, volume 7622 of *Lecture Notes in Computer Science*, page 145. Springer, 2012. URL https://link.springer.com/chapter/10.1007/978-3-642-35694-0_16.
259. Ross Anderson. "Protocol Governance: The Elite, or the Mob? (Transcript of Discussion)". In Bruce Christianson, James A. Malcolm, Frank Stajano and Jonathan Anderson (Editors), *Security Protocols XX*, volume 7622 of *Lecture Notes in Computer Science*, pages 146–160. Springer, 2012. URL https://link.springer.com/chapter/10.1007/978-3-642-35694-0_17.
260. Ross Anderson. "Risk and Privacy Implications of Consumer Payment Innovation in the Connected Age". In *Consumer Payment Innovation in the Connected Age*. 2012. URL https://www.kansascityfed.org/Root/documents/4094/2012-Anderson_final.pdf.
261. Ross Anderson. "Security Economics: A Personal Perspective". In Robert H. Obbes Zakon (Editor), *Annual Computer Security Applications Conference (ACSAC)*, pages 139–144. ACM, 2012. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/econ_acsac2012.pdf.
262. Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel van Eeten, Michael Levi, Tyler Moore and Stefan Savage. "Measuring the Cost of Cybercrime". In *Workshop on the Economics of Information Security*. 2012. URL https://econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf.
263. Joseph Bonneau, Sören Preibusch and Ross Anderson. "A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs". In Angelos D. Keromytis (Editor), *Financial Cryptography and Data Security*, volume 7397 of *Lecture Notes in Computer Science*, pages 25–40. Springer, 2012. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/BPA12-FC-banking_pin_security.pdf.
264. Alex Henney and Ross Anderson. "Smart Metering – Ed Milliband's Poisoned Chalice", 2012. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/SmartMetering-Feb82012.pdf.
265. Hyoungshick Kim and Ross Anderson. "Temporal node centrality in complex networks". *Physical Review E*, **85**:026107, 2012. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/TemporalCentrality.pdf.
266. Hyoungshick Kim, John Tang, Ross Anderson and Cecilia Mascolo. "Centrality prediction in dynamic human contact networks". *Computer Networks*, **56**(3):983–996, 2012. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/computernets12.pdf.
267. Hyoungshick Kim, John Kit Tang and Ross Anderson. "Social Authentication: Harder Than It Looks". In Angelos D. Keromytis (Editor), *Financial Cryptography and Data Security*, volume 7397 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2012. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/socialauthentication.pdf.

268. Tyler Moore and Ross Anderson. "Internet Security". In *The Oxford Handbook of the Digital Economy*, pages 572–599. Oxford University Press, 2012. URL https://tylermoore.ens.utulsa.edu/oxford12.pdf.
269. Steven J. Murdoch, Mike Bond and Ross Anderson. "How Certification Systems Fail: Lessons from the Ware Report". *IEEE Security and Privacy*, **10**(6):40–44, 2012. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/cert-fail.pdf.
270. Robert N. M. Watson, Peter G. Neumann, Jonathan Woodruff, Jonathan Anderson, Ross Anderson, Nirav Dave, Ben Laurie, Simon W. Moore, Steven J. Murdoch, Philip Paeps, Michael Roe and Hassen Saïdi. "CHERI: a research platform deconflating hardware virtualization and protection". In *Runtime Environments, Systems, Layering and Virtualized Environments (RESoLVE)*. 2012. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/2012resolve-cheri.pdf.
271. Rubin Xu, Hassen Saïdi and Ross Anderson. "Aurasium: Practical Policy Enforcement for Android Applications". In Tadayoshi Kohno (Editor), *Proceedings of the 21th USENIX Security Symposium*, pages 539–552. 2012. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/aurasium-usenix-sec-12.pdf.
272. Ross Anderson. "Medical Confidentiality and the Data Protection Regulation", 2013. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/Med-Confidentiality-and-DPR.pdf.
273. Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore and Stefan Savage. "Measuring the Cost of Cybercrime". In Rainer Böhme (Editor), *Economics of Information Security and Privacy*, pages 265–300. Springer, 2013. URL https://link.springer.com/chapter/10.1007/978-3-642-39498-0_12.
274. Ross Anderson and Robert Brady. "Why quantum computing is hard – and quantum cryptography is not provably secure", 2013. URL https://arxiv.org/abs/1301.7351.
275. Robert Brady and Ross Anderson. "Violation of Bell's inequality in fluid mechanics", 2013. URL https://arxiv.org/abs/1305.6822.
276. Wei Ming Khoo, Alan Mycroft and Ross Anderson. "Rendezvous: a search engine for binary code". In Thomas Zimmermann, Massimiliano Di Penta and Sunghun Kim (Editors), *Proceedings of the 10th Working Conference on Mining Software Repositories, MSR '13*, pages 329–338. IEEE Computer Society, 2013. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/rendezvous.pdf.
277. Hyoungshick Kim and Ross Anderson. "An Experimental Evaluation of Robustness of Networks". *IEEE Systems Journal*, **7**(2):179–188, 2013. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/NetworkRobustness_v2.pdf.
278. Laurent Simon and Ross Anderson. "PIN Skimmer: Inferring PINs Through The Camera and Microphone". In William Enck, Adrienne Porter Felt and N. Asokan (Editors), *ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 67–78. 2013. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/pinskimmer_spsm13.pdf.
279. Dongting Yu, Andrew W. Moore, Chris Hall and Ross Anderson. "Authentication for Resilience: The Case of SDN". In Bruce Christianson, James A. Malcolm, Frank Stajano, Jonathan Anderson and Joseph Bonneau (Editors), *Security Protocols XXI*, volume 8263 of *Lecture Notes in Computer Science*, pages 39–44. Springer, 2013. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/sdnresilience-spw2013-yu.pdf.

280. Ross Anderson. "Privacy versus government surveillance: where network effects meet public choice". In *Workshop on the Economics of Information Security*. 2014. URL https://econinfosec.org/archive/weis2014/papers/Anderson-WEIS2014.pdf.
281. Ross Anderson and Ian Brown. "FIPR Consultation Response on The Joint Committee on the National Security Strategy ", 2014. URL https://fipr.org/140927nationalsecurity.pdf.
282. Ross Anderson and Ian Brown. "FIPR Consultation Response on The Speaker's Commission on Digital Democracy", 2014. URL https://fipr.org/140923digitaldemocracy.pdf.
283. Ross Anderson and Chris Hall. "Collaborating with the Enemy on Network Management (Transcript of Discussion)". In Bruce Christianson, James A. Malcolm, Vashek Matyáš, Petr Svenda, Frank Stajano and Jonathan Anderson (Editors), *Security Protocols XXII*, volume 8809 of *Lecture Notes in Computer Science*, pages 163–171. Springer, 2014. URL https://doi.org/10.1007/978-3-319-12400-1_16.
284. Ross Anderson and Steven J. Murdoch. "EMV: why payment systems fail". *Communications of the ACM*, **57**(6):24–28, 2014. URL https://www.repository.cam.ac.uk/handle/1810/285618.
285. Mike Bond, Omar Choudary, Steven J. Murdoch, Sergei P. Skorobogatov and Ross Anderson. "Chip and Skim: Cloning EMV Cards with the Pre-play Attack". In *IEEE Symposium on Security and Privacy*, pages 49–64. 2014. URL https://doi.ieeecomputersociety.org/10.1109/SP.2014.11.
286. Robert Brady and Ross Anderson. "Why bouncing droplets are a pretty good model of quantum mechanics", 2014. URL https://arxiv.org/abs/1401.4356.
287. James T. Graves, Alessandro Acquisti and Ross Anderson. "Experimental Measurement of Attitudes Regarding Cybercrime". In *Workshop on the Economics of Information Security*. 2014. URL https://econinfosec.org/archive/weis2014/papers/GravesAcquistiAnderson-WEIS2014.pdf.
288. Chris Hall, Dongting Yu, Zhi-Li Zhang, Jonathan Stout, Andrew M. Odlyzko, Andrew W. Moore, L. Jean Camp, Kevin Benton and Ross Anderson. "Collaborating with the Enemy on Network Management". In Bruce Christianson, James A. Malcolm, Vashek Matyáš, Petr Svenda, Frank Stajano and Jonathan Anderson (Editors), *Security Protocols XXII*, volume 8809 of *Lecture Notes in Computer Science*, pages 154–162. Springer, 2014. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/spw14-08-Anderson.pdf.
289. David Modic and Ross Anderson. "Reading this may harm your computer: The psychology of malware warnings". *Computers in Human Behavior*, **41**:71–79, 2014. URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2374379.
290. David Modic and Ross Anderson. "We Will Make You Like Our Research: The Development of a Susceptibility-to-Persuasion Scale", 2014. URL https://ssrn.com/abstract=2446971.
291. Steven J. Murdoch and Ross Anderson. "Security Protocols and Evidence: Where Many Payment Systems Fail". In Nicolas Christin and Reihaneh Safavi-Naini (Editors), *Financial Cryptography and Data Security*, volume 8437 of *Lecture Notes in Computer Science*, pages 21–32. Springer, 2014. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/fc14evidence.pdf.
292. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter

and Daniel J. Weitzner. "Keys under doormats". *Communications of the ACM*, **58**(10):24–26, 2015. URL https://dl.acm.org/doi/10.1145/2814825.

293. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter and Daniel J. Weitzner. "Keys under doormats: mandating insecurity by requiring government access to all data and communications". *Journal of Cybersecurity*, 2015. URL http://cybersecurity.oxfordjournals.org/content/early/2015/11/17/cybsec.tyv009.
294. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter and Daniel J. Weitzner. "Keys under doormats: mandating insecurity by requiring government access to all data and communications". *Journal of Cybersecurity*, **1**(1):69–79, 2015. URL https://www.repository.cam.ac.uk/handle/1810/285617.
295. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matthew Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Peter G. Neumann, Susan Landau, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter and Daniel J. Weitzner. "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications". Technical Report TR-2015-026, MIT CSAIL, 2015. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/doormats.pdf.
296. Harold "Hal" Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matthew Blaze, Whitfield "Whit" Diffie, John Gilmore, Matthew Green, Peter G. Neumann, Susan Landau, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter and Daniel J. Weitzner. "Keys Under Doormats". *Communications of the ACM*, **58**(10):24–26, 2015. URL http://cacm.acm.org/magazines/2015/10/192382-keys-under-doormats/fulltext.
297. Ross Anderson. "He Who Pays The AI, Calls The Tune". In *What do you think about machines that think?* Edge, 2015. URL https://www.edge.org/response-detail/26069.
298. Ross Anderson. "What Goes Around Comes Around". In Marc Rotenberg, Jeramie Scott and Julia Horwitz (Editors), *Privacy in the Modern Age*. New Press, 2015. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/WhatGoesAround.pdf.
299. Khaled Baqer and Ross Anderson. "Do You Believe in Tinker Bell? The Social Externalities of Trust". In Bruce Christianson, Petr Svenda, Vashek Matyáš, James A. Malcolm, Frank Stajano and Jonathan Anderson (Editors), *Security Protocols XXIII*, volume 9379 of *Lecture Notes in Computer Science*, pages 224–236. Springer, 2015. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/spw15-12-Anderson.pdf.
300. Khaled Baqer and Ross Anderson. "Do You Believe in Tinker Bell? The Social Externalities of Trust (Transcript of Discussion)". In Bruce Christianson, Petr Svenda, Vashek Matyáš, James A. Malcolm, Frank Stajano and Jonathan Anderson (Editors), *Security Protocols XXIII*, volume 9379 of *Lecture Notes in Computer Science*, pages 237–246. Springer, 2015. URL https://doi.org/10.1007/978-3-319-26096-9_24.
301. Mike Bond, Marios O. Choudary, Steven J. Murdoch, Sergei P. Skorobogatov and Ross Anderson. "Be Prepared: The EMV Preplay Attack". *IEEE Security and*

Privacy, **13**(2):56–64, 2015. URL https://murdoch.is/papers/ieeesp15beprepared.pdf.

302. Robert Brady and Ross Anderson. "Maxwell's fluid model of magnetism", 2015. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/maxwell.pdf.
303. David Modic and Ross Anderson. "It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud". *IEEE Security and Privacy*, **13**(5):99–103, 2015. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/modicanderson-over15.pdf.
304. Ronald Poppe, Sophie van der Zee, Paul J. Taylor, Ross Anderson and Remco C. Veltkamp. "Mining Bodily Cues to Deception". In *Rapid Screening Technologies, Deception Detection and Credibility Assessment Symposium*. 2015. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/mining-bodily-cues.pdf.
305. Martin Richards, Ross Anderson, Stephen Hinde, Jane Kaye, Anneke Lucassen, Paul M. Matthews, Michael Parker, Margaret V. Shotter, Geoff Watts, Susan E. Wallace and John Wise. *The collection, linking and use of data in biomedical research and health care: ethical issues*. Nuffield Council on Bioethics, 2015. URL https://www.nuffieldbioethics.org/publication/the-collection-linking-and-use-of-data-in-biomedical-research-and-health-care-ethical-issues/.
306. Laurent Simon and Ross Anderson. "Security Analysis of Android Factory Resets". In *Mobile Security Technologies (MoST)*. 2015. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/fr_most15.pdf.
307. Laurent Simon and Ross Anderson. "Security Analysis of Consumer-Grade Anti-Theft Solutions Provided by Android Mobile Anti-Virus Apps". In *Mobile Security Technologies (MoST)*. 2015. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/mav_most15.pdf.
308. Sophie van der Zee, Ronald Poppe, Paul J. Taylor and Ross Anderson. "To freeze or not to freeze – A motion-capture approach to detecting deceit". In *Rapid Screening Technologies, Deception Detection and Credibility Assessment Symposium*. 2015. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/HICSS-to-freeze-or-not-to-freeze.pdf.
309. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter and Daniel J. Weitzner. "Apple's Cloud Key Vault, Exceptional Access, and False Equivalences", 2016. URL https://www.lawfareblog.com/apples-cloud-key-vault-exceptional-access-and-false-equivalences.
310. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter and Daniel J. Weitzner. "Warning Signs: A Checklist for Recognizing Flaws of Proposed "Exceptional Access" Systems", 2016. URL https://www.lawfareblog.com/warning-signs-checklist-recognizing-flaws-proposed-exceptional-access-systems.
311. Ross Anderson. "Are the Real Limits to Scale a Matter of Science, or Engineering, or of Something Else? (Abstract only)". In *IEEE Computer Security Foundations Symposium, CSF*, page 16. 2016. URL https://ieeexplore.ieee.org/document/7536363.
312. Ross Anderson. "Brexit and technology: How network effects will damage UK IT industry". *Computer Weekly*, 2016. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/brexit-and-network-economics.pdf.

313. Ross Anderson. "Hard Newcap or Soft Newcap? A Christmas Fable", 2016. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/newcap2016.pdf.
314. Ross Anderson. "Replacing Magic With Mechanism?" In *What do you consider the most interesting recent [scientific] news? What makes it important?* Edge, 2016. URL https://www.edge.org/response-detail/26757.
315. Ross Anderson. "What would Brexit really mean for Cambridge". *Cambridge News*, 2016. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/brexit-and-cambridge.pdf.
316. Khaled Baqer and Ross Anderson. "SMAPs: Short Message Authentication Protocols (Transcript of Discussion)". In Jonathan Anderson, Vashek Matyáš, Bruce Christianson and Frank Stajano (Editors), *Security Protocols XXIV*, volume 10368 of *Lecture Notes in Computer Science*, pages 133–140. Springer, 2016. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/SPW24_discussion.pdf.
317. Khaled Baqer, S. Johann Bezuidenhoudt, Ross Anderson and Markus G. Kuhn. "SMAPs: Short Message Authentication Protocols". In Jonathan Anderson, Vashek Matyáš, Bruce Christianson and Frank Stajano (Editors), *Security Protocols XXIV*, volume 10368 of *Lecture Notes in Computer Science*, pages 119–132. Springer, 2016. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/SPW24.pdf.
318. Ingolf Becker, Alice Hutchings, Ruba Abu-Salma, Ross Anderson, Nicholas Bohm, Steven J. Murdoch, M. Angela Sasse and Gianluca Stringhini. "International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms". In *Workshop on the Economics of Information Security*. 2016. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/weis16fraudreimbursement.pdf.
319. Alice Hutchings, Richard Clayton and Ross Anderson. "Taking down websites to prevent crime". In *APWG Symposium on Electronic Crime Research*, pages 102–111. 2016. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/2016takedown.pdf.
320. Steven J. Murdoch, Ingolf Becker, Ruba Abu-Salma, Ross Anderson, Nicholas Bohm, Alice Hutchings, M. Angela Sasse and Gianluca Stringhini. "Are Payment Card Contracts Unfair? (Short Paper)". In Jens Grossklags and Bart Preneel (Editors), *Financial Cryptography and Data Security*, volume 9603 of *Lecture Notes in Computer Science*, pages 600–608. Springer, 2016. URL https://discovery.ucl.ac.uk/id/eprint/1473782/.
321. Laurent Simon, Wenduan Xu and Ross Anderson. "Don't Interrupt Me While I Type: Inferring Text Entered Through Gesture Typing on Android Keyboards". *Proceedings on Privacy Enhancing Technologies*, **2016**(3):136–154, 2016. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/interrupts_pets16-1.pdf.
322. Sophie van der Zee, Ross Anderson and Ronald Poppe. "When Lying Feels the Right Thing to Do". In Guy Hochman, Shahar Ayal and Dan Ariely (Editors), *Dishonest behavior: From theory to practice*. Frontiers Media SA, 2016.
323. Sophie van der Zee, Ross Anderson and Ronald Poppe. "When Lying Feels the Right Thing to Do". *Frontiers in Psychology*, **7**:734, 2016. URL https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2016.00734.
324. Ross Anderson. "De-Anonymization". In *What scientific term or concept ought to be more widely known?* Edge, 2017. URL https://www.edge.org/response-detail/27195.

325. Ross Anderson. "Reconciling Multiple Objectives – Politics or Markets? (Transcript of Discussion)". In Frank Stajano, Jonathan Anderson, Bruce Christianson and Vashek Matyáš (Editors), *Security Protocols XXV*, volume 10476 of *Lecture Notes in Computer Science*, pages 157–170. Springer, 2017. URL https://doi.org/10.1007/978-3-319-71075-4_18.
326. Ross Anderson. "The Threat: A Conversation With Ross Anderson", 2017. URL https://www.edge.org/conversation/ross_anderson-the-threat.
327. Ross Anderson and Khaled Baqer. "Reconciling Multiple Objectives – Politics or Markets?" In Frank Stajano, Jonathan Anderson, Bruce Christianson and Vashek Matyáš (Editors), *Security Protocols XXV*, volume 10476 of *Lecture Notes in Computer Science*, pages 144–156. Springer, 2017. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/reconciling-multiple-objectives.pdf.
328. Khaled Baqer, Ross Anderson, Lorna Mutegi, Jeunese Adrienne Payne and Joseph Sevilla. "DigiTally: Piloting Offline Payments for Phones". In *Symposium on Usable Privacy and Security, SOUPS*, pages 131–143. 2017. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/DigiTally_SOUPS2017.pdf.
329. Ingolf Becker, Alice Hutchings, Ruba Abu-Salma, Ross Anderson, Nicholas Bohm, Steven J. Murdoch, M. Angela Sasse and Gianluca Stringhini. "International comparison of bank fraud reimbursement: customer perceptions and contractual terms". *Journal of Cybersecurity*, **3**(2):109–125, 2017. URL https://www.repository.cam.ac.uk/handle/1810/279983.
330. Éireann Leverett, Richard Clayton and Ross Anderson. *Standardisation and Certification of Safety, Security and Privacy in the 'Internet of Things'*. Publications Office of the European Union, 2017. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/eu-jrc-77862.pdf. Editor: Gianmarco Baldini.
331. Éireann Leverett, Richard Clayton and Ross Anderson. "Standardisation and Certification of the Internet of Things". In *Workshop on the Economics of Information Security*. 2017. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/weis2017.pdf.
332. Hal Abelson, Ross Anderson, Richard Barnes, Xavier Boyen, Alissa Cooper, Chris Culnane, Rajeev Gore, Ben Laurie, Peter G. Neumann, Mark Nottingham, Josef Pieprzyk, Ron Rivest, Bruce Schneier, Jeffrey Schiller, Michael Specter, Vanessa Teague, Yuval Yarom and Daniel J. Weitzner. "Letter Regarding the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018", 2018. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/aus-transparency.pdf.
333. Mansoor Ahmed-Rengers, Ilia Shumailov and Ross Anderson. "Tendrils of Crime: Visualizing the Diffusion of Stolen Bitcoins". In George Cybenko, David J. Pym and Barbara Fila (Editors), *5th International Workshop on Graphical Models for Security, Revised Selected Papers*, volume 11086 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2018. URL https://doi.org/10.1007/978-3-030-15465-3_1.
334. Ross Anderson. "Covert and Deniable Communications". In Rainer Böhme, Cecilia Pasquini, Giulia Boato and Pascal Schöttle (Editors), *ACM Workshop on Information Hiding and Multimedia Security*, page 1. 2018. URL https://doi.org/10.1145/3206004.3206023.
335. Ross Anderson. "Making Security Sustainable". *Communications of the ACM*, **61**(3):24–26, 2018. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/making-security-sustainable.pdf.

336. Ross Anderson. "Sustainable Security – an Internet of Durable Goods (keynote talk)". In Paolo Mori, Steven Furnell and Olivier Camp (Editors), *International Conference on Information Systems Security and Privacy, ICISSP*, page 7. 2018. URL https://icissp.scitevents.org/KeynoteSpeakers.aspx?y=2018.
337. Ross Anderson and Tanya Berger-Wolf. "Privacy for Tigers". In *Proceedings of the 27th USENIX Security Symposium*. 2018. URL https://www.usenix.org/conference/usenixsecurity18/presentation/anderson.
338. Ross Anderson, Ilia Shumailov and Mansoor Ahmed. "Making Bitcoin Legal". In Vashek Matyáš, Petr Svenda, Frank Stajano, Bruce Christianson and Jonathan Anderson (Editors), *Security Protocols XXVI*, volume 11286 of *Lecture Notes in Computer Science*, pages 243–253. Springer, 2018. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/making-bitcoin-legal.pdf.
339. Ross Anderson, Ilia Shumailov, Mansoor Ahmed and Alessandro Rietmann. "Bitcoin Redux". In *Workshop on the Economics of Information Security*. 2018. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/bitcoin-redux.pdf.
340. David Modic, Ross Anderson and Jussi Palomäki. "We will make you like our research: The development of a susceptibility-to-persuasion scale". *PLoS ONE*, **13**(3), 2018. URL https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0194119.
341. Laurent Simon, David Chisnall and Ross Anderson. "What You Get is What You C: Controlling Side Effects in Mainstream C Compilers". In *IEEE European Symposium on Security and Privacy*, pages 1–15. 2018. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/whatyouc.pdf.
342. Mansoor Ahmed-Rengers, Ross Anderson, Darija Halatova and Ilia Shumailov. "Snitches Get Stitches: On the Difficulty of Whistleblowing". In Jonathan Anderson, Frank Stajano, Bruce Christianson and Vashek Matyáš (Editors), *Security Protocols XXVII*, volume 12287 of *Lecture Notes in Computer Science*, pages 289–303. Springer, 2019. URL https://www.repository.cam.ac.uk/handle/1810/303849.
343. Mansoor Ahmed-Rengers, Ross Anderson, Darija Halatova and Ilia Shumailov. "Snitches Get Stitches: On the Difficulty of Whistleblowing (Transcript of Discussion)". In Jonathan Anderson, Frank Stajano, Bruce Christianson and Vashek Matyáš (Editors), *Security Protocols XXVII*, volume 12287 of *Lecture Notes in Computer Science*, pages 304–312. Springer, 2019. URL https://doi.org/10.1007/978-3-030-57043-9_28.
344. Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Carlos Gañán, Tom Grasso, Michael Levi, Tyler Moore, Stefan Savage and Marie Vasek. "Measuring the Changing Cost of Cybercrime". In *Workshop on the Economics of Information Security*. 2019. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/cost_of_cybercrime.pdf.
345. James T. Graves, Alessandro Acquisti and Ross Anderson. "Perception Versus Punishment in Cybercrime". *Journal of Criminal Law and Criminology*, **109**, 2019. URL https://scholarlycommons.law.northwestern.edu/jclc/vol109/iss2/4/.
346. Ilia Shumailov, Xitong Gao, Yiren Zhao, Robert D. Mullins, Ross Anderson and Cheng-Zhong Xu. "Sitatapatra: Blocking the Transfer of Adversarial Samples", 2019. URL https://arxiv.org/abs/1901.08121.
347. Ilia Shumailov, Laurent Simon, Jeff Yan and Ross Anderson. "Hearing your touch: A new acoustic side channel on smartphones", 2019. URL https://arxiv.org/abs/1903.11137.

348. Ilia Shumailov, Yiren Zhao, Robert Mullins and Ross Anderson. "The Taboo Trap: Behavioural Detection of Adversarial Samples", 2019. URL https://arxiv.org/abs/1811.07375.

349. Sophie van der Zee, Richard Clayton and Ross Anderson. "The gift of the gab: Are rental scammers skilled at the art of persuasion?", 2019. URL https://arxiv.org/abs/1911.08253.

350. Sophie van der Zee, Ronald Poppe, Paul J. Taylor and Ross Anderson. "To freeze or not to freeze: A culture-sensitive motion capture approach to detecting deceit". *PLoS ONE*, **14**(4), 2019. URL https://eprints.lancs.ac.uk/id/eprint/132789/.

351. Yiren Zhao, Ilia Shumailov, Robert D. Mullins and Ross Anderson. "To Compress Or Not To Compress: Understanding The Interactions Between Adversarial Attacks And Neural Network Compression". In Ameet Talwalkar, Virginia Smith and Matei Zaharia (Editors), *Proceedings of the Second Conference on Machine Learning and Systems*, pages 230–240. 2019. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/sysml2019-127.pdf.

352. Ross Anderson. *Security Engineering – A Guide to Building Dependable Distributed Systems*. Wiley Computer Publishing. John Wiley & Sons, 2020.

353. Ilia Shumailov, Yiren Zhao, Robert D. Mullins and Ross Anderson. "Towards Certifiable Adversarial Sample Detection". In Jay Ligatti and Xinming Ou (Editors), *ACM Workshop on Artificial Intelligence and Security*, pages 13–24. 2020. URL https://www.repository.cam.ac.uk/items/780196a7-f41a-4568-821c-88cfe36db52b.

354. Almos Zarandy, Ilia Shumailov and Ross Anderson. "BatNet: Data transmission between smartphones over ultrasound", 2020. URL https://arxiv.org/abs/2008.00136.

355. Almos Zarandy, Ilia Shumailov and Ross Anderson. "Hey Alexa what did I just type? Decoding smartphone sounds with a voice assistant", 2020. URL https://arxiv.org/abs/2012.00687.

356. Yiren Zhao, Ilia Shumailov, Han Cui, Xitong Gao, Robert D. Mullins and Ross Anderson. "Blackbox Attacks on Reinforcement Learning Agents Using Approximated Temporal Information". In *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops*, pages 16–24. 2020. URL https://core.ac.uk/download/pdf/345610289.pdf.

357. Yiren Zhao, Ilia Shumailov, Robert D. Mullins and Ross Anderson. "Nudge Attacks on Point-Cloud DNNs", 2020. URL https://arxiv.org/abs/2011.11637.

358. Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague and Carmela Troncoso. "Bugs in our Pockets: The Risks of Client-Side Scanning", 2021. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/bugs21.pdf.

359. Ross Anderson. *Confidentiality in Remote Clinical Practice*. International Psychoanalytical Association, 2021. URL https://www.ipa.world/IPA/IPA_DOCS/Consultancy%20report%20by%20Professor%20Ross%20Anderson%20FRS.pdf.

360. Ross Anderson, Rainer Böhme, Richard Clayton and Ben Collier. "Silicon Den: Cybercrime is Entrepreneurship". In *Workshop on the Economics of Information Security*. 2021. URL https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-anderson.pdf.

361. Ross Anderson and Ilia Shumailov. "Situational Awareness and Adversarial Machine Learning – Robots, Manners, and Stress", 2021. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/situational-awareness2021.pdf.
362. David Khachaturov, Ilia Shumailov, Yiren Zhao, Nicolas Papernot and Ross Anderson. "Markpainting: Adversarial Machine Learning meets Inpainting". In Marina Meila and Tong Zhang (Editors), *International Conference on Machine Learning (ICML)*, volume 139 of *Proceedings of Machine Learning Research*, pages 5409–5419. PMLR, 2021. URL http://proceedings.mlr.press/v139/khachaturov21a.html.
363. Ilia Shumailov, Zakhar Shumaylov, Dmitry Kazhdan, Yiren Zhao, Nicolas Papernot, Murat A. Erdogdu and Ross Anderson. "Manipulating SGD with Data Ordering Attacks". In Marc'Aurelio Ranzato, Alina Beygelzimer, Yann N. Dauphin, Percy Liang and Jennifer Wortman Vaughan (Editors), *Advances in Neural Information Processing Systems 34 (NeurIPS 2021)*, pages 18021–18032. 2021. URL https://papers.neurips.cc/paper_files/paper/2021/file/959ab9a0695c467e7caf75431a872e5c-Paper.pdf.
364. Ilia Shumailov, Yiren Zhao, Daniel Bates, Nicolas Papernot, Robert D. Mullins and Ross Anderson. "Sponge Examples: Energy-Latency Attacks on Neural Networks". In *IEEE European Symposium on Security and Privacy*, pages 212–231. IEEE, 2021. URL https://ieeexplore.ieee.org/document/9581273.
365. Mansoor Ahmed-Rengers, Diana A. Vasile, Daniel Hugenroth, Alastair R. Beresford and Ross Anderson. "CoverDrop: Blowing the Whistle Through A News App". *Proceedings Privacy Enhancing Technologies*, **2022**(2):47–67, 2022. URL https://petsymposium.org/2022/files/papers/issue2/popets-2022-0035.pdf.
366. Ross Anderson. "Chat Control or Child Protection?", 2022. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/chatcontrol.pdf.
367. Ross Anderson and Sam Gilbert. "Legislating for Online Safety". *Intermedia*, **50**(2):8–12, 2022. URL https://www.iicom.org/intermedia/vol-50-issue-2/regulating-online-safety/.
368. Ross Anderson, Sam Gilbert and Diane Coyle. *The Online Safety Bill*. Bennett Institute for Public Policy, 2022. URL https://www.bennettinstitute.cam.ac.uk/publications/online-safety-bill/.
369. Nicholas Boucher and Ross Anderson. "Keynote: Trojan Source and Bad Characters: Invisible Hacks and Reluctant Patching". In *LangSec*. 2022. URL https://www.youtube.com/watch?v=nXCEuHekt-0.
370. Nicholas Boucher and Ross Anderson. "Talking Trojan: Analyzing an Industry-Wide Disclosure". In Santiago Torres-Arias, Marcela S. Melara and Laurent Simon (Editors), *ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses*, pages 83–92. 2022. URL https://doi.org/10.1145/3560835.3564555.
371. Nicholas Boucher, Ilia Shumailov, Ross Anderson and Nicolas Papernot. "Bad Characters: Imperceptible NLP Attacks". In *IEEE Symposium on Security and Privacy*, pages 1987–2004. 2022. URL https://ieeexplore.ieee.org/document/9833641.
372. Jusop Choi, Wonseok Choi, William Aiken, Hyoungshick Kim, Jun Ho Huh, Taesoo Kim, Yongdae Kim and Ross Anderson. "Attack of the Clones: Measuring the Maintainability, Originality and Security of Bitcoin 'Forks' in the Wild", 2022. URL https://arxiv.org/abs/2201.08678.

373. Ildiko Pete, Jack Hughes, Andrew Caines, Anh V. Vu, Harshad Gupta, Alice Hutchings, Ross Anderson and Paula Buttery. "PostCog: A tool for interdisciplinary research into underground forums at scale". In *IEEE European Symposium on Security and Privacy*, pages 93–104. IEEE, 2022. URL https://www.cl.cam.ac.uk/~ah793/papers/2022postcog.pdf.
374. Ross Anderson and Nicholas Boucher. "If It's Provably Secure, It Probably Isn't: Why Learning from Proof Failure Is Hard". In Frank Stajano, Vashek Matyáš, Bruce Christianson and Jonathan Anderson (Editors), *Security Protocols XXVIII*, volume 14186 of *Lecture Notes in Computer Science*, pages 199–204. Springer, 2023. URL https://doi.org/10.1007/978-3-031-43033-6_19.
375. Ross Anderson and Nicholas Boucher. "If It's Provably Secure, It Probably Isn't: Why Learning from Proof Failure is Hard (Transcript of Discussion)". In Frank Stajano, Vashek Matyáš, Bruce Christianson and Jonathan Anderson (Editors), *Security Protocols XXVIII*, volume 14186 of *Lecture Notes in Computer Science*, pages 205–210. Springer, 2023. URL https://doi.org/10.1007/978-3-031-43033-6_20.
376. Jenny Blessing and Ross Anderson. "One Protocol to Rule Them All? On Securing Interoperable Messaging". In Frank Stajano, Vashek Matyáš, Bruce Christianson and Jonathan Anderson (Editors), *Security Protocols XXVIII*, volume 14186 of *Lecture Notes in Computer Science*, pages 174–192. Springer, 2023. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/interoperability-spw23.pdf.
377. Jenny Blessing, Partha Das Chowdhury, Maria Sameen, Ross Anderson, Joseph Gardiner and Awais Rashid. "Towards Human-Centric Endpoint Security". In Frank Stajano, Vashek Matyáš, Bruce Christianson and Jonathan Anderson (Editors), *Security Protocols XXVIII*, volume 14186 of *Lecture Notes in Computer Science*, pages 211–219. Springer, 2023. URL https://bpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/1/670/files/2023/10/Towards-Human-Centric-Endpoint-Security.pdf.
378. Nicholas Boucher and Ross Anderson. "Automatic Bill of Materials", 2023. URL https://arxiv.org/abs/2310.09742.
379. Nicholas Boucher and Ross Anderson. "Trojan Source: Invisible Vulnerabilities". In Joseph A. Calandrino and Carmela Troncoso (Editors), *32nd USENIX Security Symposium*, pages 6507–6524. 2023. URL https://www.usenix.org/system/files/sec23fall-prepub-151-boucher.pdf.
380. Nicholas Boucher, Jenny Blessing, Ilia Shumailov, Ross Anderson and Nicolas Papernot. "When Vision Fails: Text Attacks Against ViT and OCR", 2023. URL https://arxiv.org/abs/2306.07033.
381. Nicholas Boucher, Luca Pajola, Ilia Shumailov, Ross Anderson and Mauro Conti. "Boosting Big Brother: Attacking Search Engines with Encodings". In *International Symposium on Research in Attacks, Intrusions and Defenses, RAID*, pages 700–713. ACM, 2023. URL https://doi.org/10.1145/3607199.3607220.
382. David Khachaturov, Yue Gao, Ilia Shumailov, Robert D. Mullins, Ross Anderson and Kassem Fawaz. "Human-Producible Adversarial Examples", 2023. URL https://arxiv.org/abs/2310.00438.
383. Anh V. Vu, Alice Hutchings and Ross Anderson. "A Case Study in Censorship". *Cambridge Cybercrime Centre Briefing Paper*, 2023. URL https://anhvvcs.github.io/static/media/vu2024no-briefing.pdf.
384. Anh V. Vu, Alice Hutchings and Ross Anderson. "Defacement Attacks on Israeli Websites". *Cambridge Cybercrime Centre Briefing Paper*, 2023. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/gaza.pdf.

385. Anh V. Vu, Lydia Wilson, Yi Ting Chua, Ilia Shumailov and Ross Anderson. "ExtremeBB: A Database for Large-Scale Research into Online Hate, Harassment, the Manosphere and Extremism". In *Workshop on Online Abuse and Harms (WOAH)*. 2023. URL https://www.repository.cam.ac.uk/items/dbd78f16-82cb-4d81-8842-8a8dc1e8deb0.
386. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague and Carmela Troncoso. "Bugs in our pockets: the risks of client-side scanning". *Journal of Cybersecurity*, **10**(1), 2024. URL https://www.schneier.com/wp-content/uploads/2024/01/Bugs_in_Our_Pockets.pdf.
387. Jenny Blessing, Daniel Hugenroth, Ross Anderson and Alastair R. Beresford. "SoK: Web Authentication in the Age of End-to-End Encryption", 2024. URL https://arxiv.org/abs/2406.18226.
388. Eleanor Clifford, Ilia Shumailov, Yiren Zhao, Ross Anderson and Robert D. Mullins. "ImpNet: Imperceptible and blackbox-undetectable backdoors in compiled neural networks". In *IEEE Conference on Secure and Trustworthy Machine Learning, SaTML*, pages 344–357. 2024. URL https://doi.org/10.1109/SaTML59370.2024.00024.
389. Pranav Dahiya, Ilia Shumailov and Ross Anderson. "Machine Learning needs Better Randomness Standards: Randomised Smoothing and PRNG-based attacks". In Davide Balzarotti and Wenyuan Xu (Editors), *33rd USENIX Security Symposium*. 2024. URL https://www.usenix.org/system/files/sec24summer-prepub-920-dahiya.pdf.
390. Partha Das Chowdhury, Maria Sameen, Jenny Blessing, Nicholas Boucher, Joseph Gardiner, Tom Burrows, Ross Anderson and Awais Rashid. "Threat models over space and time: A case study of end-to-end-encrypted messaging applications". *Software: Practice and Experience*, 2024. URL https://doi.org/10.1002/spe.3341.
391. Ronald Poppe, Sophie van der Zee, Paul J. Taylor, Ross Anderson and Remco C. Veltkamp. "Mining Bodily Cues to Deception". *Journal of Nonverbal Behavior*, **48**(1):137–159, 2024. URL https://doi.org/10.1007/s10919-023-00450-9.
392. Ilia Shumailov, Zakhar Shumaylov, Yiren Zhao, Nicolas Papernot, Ross Anderson and Yarin Gal. "AI models collapse when trained on recursively generated data". *Nature*, **631**(8022):755–759, 2024. URL https://www.nature.com/articles/s41586-024-07566-y.
393. Anh V. Vu, Alice Hutchings and Ross Anderson. "No Easy Way Out: the Effectiveness of Deplatforming an Extremist Forum to Suppress Hate and Harassment". In *IEEE Symposium on Security and Privacy*, pages 717–734. IEEE Computer Society, 2024. URL https://www.cl.cam.ac.uk/archive/rja14/Papers/vu2023no.pdf.
394. Anh V. Vu, Daniel R. Thomas, Ben Collier, Alice Hutchings, Richard Clayton and Ross Anderson. "Getting Bored of Cyberwar: Exploring the Role of Low-level Cybercrime Actors in the Russia-Ukraine Conflict". In Tat-Seng Chua, Chong-Wah Ngo, Ravi Kumar, Hady W. Lauw and Roy Ka-Wei Lee (Editors), *ACM Web Conference (WWW)*, pages 1596–1607. 2024. URL https://www.repository.cam.ac.uk/items/1b98a653-bd54-4c84-ad1b-8d1c441979f6.

Former PhD students supervised by Ross Anderson

Compiled by Markus G. Kuhn

University of Cambridge

We contacted all former doctoral students who graduated with Ross as their supervisor, to find out what they have been up to since.

The first year in brackets is that of matriculation and the second is that in which the PhD was approved. This is followed by the title of the dissertation. This information comes from the database of the Degree Committee of the Department.

1 **Charalampos Manifavas** (1995 – 2002)

Micropayment transaction costs

Harry began his career in an investment bank while pursuing his PhD. After completing his doctorate, he transitioned to academia. He is currently affiliated with FORTH, a Greek research institute, where he works on EU-funded projects in digital forensics, cybercrime, post-quantum cryptography, quantum key distribution, and security operations centers. He has taught multiple cybersecurity courses at various universities, most recently at the University of Crete.

2 **Fabien A. P. Petitcolas** (1996 – 1999)

Information hiding and its application to copyright protection

Fabien joined Microsoft Research after completing his PhD with Ross. He held various roles there before joining OneSpan where he led a small research team. Today he researches various computer security topics on behalf of Belgian social security.

3 **Henry Jong-Hyeon Lee** (1996 – 2000)

Designing a reliable publishing framework

After completing his PhD under Ross, Henry Jong-Hyeon Lee founded two security tech startups: FILOSAFE Corporation and Filonet Korea, Inc. Henry then transitioned to public service and became the Director of Information Security (CISO) for the Justice Sector in British Columbia, Canada. His expertise led him to Samsung Electronics, where he served as Corporate Senior Vice President, overseeing Mobile Security (Samsung Mobile) and then Network Security (Samsung Networks). Most recently, Henry joined Amazon, where he led device security for Amazon devices.

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

4 **Markus G. Kuhn** (1997 – 2002)
Compromising emanations: eavesdropping risks of computer displays

After his PhD with Ross, Markus stayed with the Security Group as associate professor, teaching Security, Cryptography and Digital Signal Processing. He worked on side-channel security, video eavesdropping, distance-bounding protocols, the security of RFID and navigation systems, and other aspects of signal security, and much enjoyed graduating nine brilliant PhD students so far: Piotr Zieliński, Steven Murdoch, Gerhard Hancke, Saar Drimer, Andrew Lewis, Marios Omar Choudary, Christian O'Connell, Shih-Chun You, Dimitrije Erdeljan.

5 **Frank Stajano** (1998 – 2001)
Security for ubiquitous computing

Like Ross, Frank did his PhD as a mature student, submitted it in three years—as early as the regulations allowed—and then turned it into a book for Wiley, *Security for Ubiquitous Computing*. He owns Cambridge Cyber Ltd, he is Fellow of Trinity College and Professor of Security and Privacy at Cambridge, where he teaches the undergraduate course on cybersecurity and a graduate course on DeFi and digital money. In 2015, with MIT, he founded the C2C CTF, still ongoing, to raise a new generation of cyber defenders. His current research is on the financial infrastructure for the digital society. He is also 5th dan in kendo (Japanese swordsmanship) and has led the Cambridge dojo for over 20 years.

6 **Ulrich Lang** (1998 – 2003)
Access policies for middleware

Ulrich co-founded ObjectSecurity during his PhD with Ross (and Dieter), spinning out research from his thesis to develop the company's first product. For over two decades, ObjectSecurity has been a leader in cybersecurity innovation and is nowadays headquartered in San Diego, CA, USA. The company's flagship products include BinLens, an innovative automated binary vulnerability analysis tool, and an AI/ML-powered vulnerability analysis product. Additionally, ObjectSecurity conducts fast-track R&D and commercialization—funded by the U.S. SBIR program—on topics such as binary analysis, AI/ML security, supply chain risk analysis, 5G vulnerability analysis, and fine-grained access control.

7 **Susan Pancho** (1998 – 2003)
Contributions of formal security proofs

Susan returned to the Philippines after completing her PhD and started introducing Computer Security courses and research projects at the University of the Philippines. Today, she is a Professor at the same university, and also does computer security research for various companies, universities, and government agencies in the Philippines.

8 **Jianxin Yan** (1999 – 2003)
Security for online games

Jeff went on to become a lecturer in computer security at Newcastle University, and later Professor of Cyber Security at the University of Southampton.

9 **Sergei Skorobogatov** (2000 – 2005)
Semi-invasive attacks – a new approach to hardware security analysis

After completing his PhD Sergei stayed as a Postdoctoral researcher at the Computer Laboratory, until 2023. His areas of research covered Hardware Security of microcontrollers, FPGAs, smartcards and Secure Elements. Since 2023 Sergei has worked in a local research company as R&D director in the area of security vulnerabilities analysis of embedded systems.

10 **George Danezis** (2000 – 2004)
Better anonymous communications

After completing his PhD on anonymity and peer-to-peer system, he headed to KU Leuven to learn more cryptography and then Microsoft Research Cambridge to do privacy related research. He then took a faculty position at University College London, where he is now Professor of Security and Privacy Engineering – a title chosen as an homage to his supervisor. In 2018 he got interested in scaling blockchains, and founded Chainspace, which was acquired by Facebook (now Meta) to work on the Libra / Diem project. Now he is a cofounder of Mysten Labs, acting as Chief Scientist, and builds modern secure peer-to-peer transaction systems, like Sui and Walrus. He regularly credits the Eternity Service, along with a healthy distrust of traditional banking, as an enduring inspiration for his work.

11 **Michael Bond** (2000 – 2004)
Understanding security APIs

Mike Bond worked on software attacks on Hardware Security Modules, on banking security and security of EMV chip card payment systems. He continued the field that Ross opened with "Why Cryptosystems Fail" and co-published with Ross, Steven Murdoch, Jolyon Clulow, Saar Drimer, George Danezis and others over a 15 year period. After the lab, Mike worked at a specialist crypto vendor Cryptomathic under Peter Landrock for a decade and then in the FinTech industry in London, at G-Research, where he remains to date.

12 **Richard Clayton** (2000 – 2005)
Anonymity and traceability in cyberspace

Richard Clayton did his PhD as a mature student and stayed on in the Lab on various projects "because it is more fun than working". He was the founding Director of the Cambridge Cybercrime Centre in 2015 – setting it on its course to not only do first class work on cybercrime, but to collect datasets and make them available to other academics, perhaps even before anyone in Cambridge had looked at the data. He continues to work part-time for the CCC, spending

the rest of the week helping the Yahoo anti-spam team keep unwanted email out of user inboxes.

13 **Jolyon Clulow** (2003 – 2007)
On the security of real-world devices

Jolyon returned to industry, working first in consulting with Deloitte, before going client side with a sequence of banks: Tesco Bank, Deutsche Bank, Barclays UK and TSB, holding the role of Chief Information Security Officer at the latter two. He is currently the Group Chief Information Security Officer for Sky.

14 **Andy Ozment** (2003 – 2007)
Vulnerability discovery & software security

Andy went on to serve as the deputy cybersecurity czar in the Obama White House. He then led the cybersecurity parts of the organization that became the U.S.' Cyber and Infrastructure Security Agency (CISA). Andy left the U.S. government in 2017 to serve as a partner and the Chief Information Security Officer (CISO) at Goldman Sachs. He is currently the Chief Technology Risk Officer (CTRO) at Capital One. Andy and his wife Ragnhild live in Washington, DC and have two daughters, ages 6 and 8.

15 **Shishir Nagaraja** (2003 – 2008)
Robust covert network topologies

Shishir holds the Chair of Cybersecurity at Newcastle University, where he co-leads the UK National Edge-AI Hub. His PhD on network security was supervised by Ross and Jon. It established a link between evolutionary game theory and complex networks, with applications to network security. His current work uses data-driven methods to explore autonomy, decentralised planning, and side-channels, in network security.

16 **Feng Hao** (2004 – 2007)
On using fuzzy data in security mechanisms

Feng Hao is now a Professor of Security Engineering in the Department of Computer Science, at the University of Warwick. His research covers the design and analysis of security protocols for real-world applications, e.g., key exchange, e-voting, e-auction and secure multi-party computation.

17 **Tyler Moore** (2004 – 2008)
Cooperative attack and defense in distributed networks

Tyler is now a Professor of Cyber Studies and Computer Science at the University of Tulsa. He is inaugural department chair for the School of Cyber Studies, an interdisciplinary academic unit focused on security and privacy. Tyler's research continues to focus on security economics and cybercrime measurement.

18 **Robert Watson** (2005 – 2011)
New approaches to operating system security extensibility

Robert Watson is now Professor of Systems, Security, and Architecture in the Department of Computer Science and Technology at the University of Cambridge. He leads an international collaboration around the CHERI instruction-set architecture, an idea arising at the tail end of his PhD with Ross. He has recently initiated a new policy effort around memory-safety standardisation, addressing market failures in the deployment of technologies that would prevent 70% of critical software security vulnerabilities, strongly influenced by Ross's work in security economics.

19 **Hyoungshick Kim** (2008 – 2012)
Complex network analysis for secure and robust communications

Hyoungshick Kim is a professor in the Department of Computer Science at Sungkyunkwan University. He previously worked at Samsung Electronics before pursuing his PhD at the University of Cambridge. He also gained research experience at UBC and CSIRO Data61. His research focuses on data-driven security and measurement, with a recent emphasis on investigating security issues in AI systems.

20 **Joseph Bonneau** (2008 – 2012)
Guessing human-chosen secrets

Joseph Bonneau is now an Associate Professor of Computer Science at New York University. In Cambridge as a Gates Scholar, he worked with Ross on human authentication (especially passwords) and privacy in social networks. After being introduced to the Bitcoin white paper by Ross, Joe later went on to work extensively in cryptocurrencies during postdoctoral fellowships at Princeton, Stanford and the Electronic Frontier Foundation. Inspired by Ross, he co-wrote the textbook *Bitcoin and Cryptocurrency Technologies* which has become standard for university-level courses on cryptocurrency. He has also won the Caspar Bowden PET award for his work introducing key transparency to encrypted messaging systems, and has helped launch five startups as an advisor.

21 **Shailendra Fuloria** (2009 – 2012)
Robust security for the electricity network

After completing his PhD, Shailendra joined ABB in India to lead multiple client-facing and R&D projects in security for industrial automation and control systems. He then joined Eaton to lead their global product security lab focusing on security for hardware and software used in the electrical infrastructure, smart homes, smart vehicle and aerospace industry. He currently works as the CISO of Nagarro, helping to secure the company's systems across 30 countries.

22 **Wei Ming Khoo** (2009 – 2013)
Decompilation as search

Wei Ming is a Principal Member of Technical Staff at DSO National Laboratories, since 2016, where he leads research in software security and binary analysis.

23 **Rubin Xu** (2010 – 2015)
Improving application trustworthiness on stock Android

After completing his PhD, Rubin went on to work for Google UK, where he is responsible for improving security and manageability for enterprises in the Android OS.

24 **Dongting Yu** (2010 – 2016)
Access control for network management

Dongting moved to San Francisco, USA, after completing his PhD. He works at B2B startups as a security engineer and occasionally does some consulting on the side. Aside from security, the network knowledge that he gained during his PhD is also frequently helpful when troubleshooting network and cloud infrastructure problems.

25 **Laurent Simon** (2012 – 2016)
Exploring new attack vectors for the exploitation of smartphones

After completing a PhD with Ross, Laurent Simon joined Samsung Research America as a security researcher. Laurent now works at Google as a security engineer.

26 **Kumar Sharad** (2012 – 2016)
Learning to de-anonymize social networks

After finishing his PhD, Sharad joined NEC Laboratories, Heidelberg as a Research Scientist working on securing ML systems. Sharad now works at Splunk as a Senior Threat Researcher where he leads the development of ML based SIEM solutions.

27 **Khaled Baqer** (2014 – 2018)
Resilient payment systems

Khaled Baqer has been a Senior Principal Product Security Engineer at Entrust (formerly nCipher Security), since January 2019. He is the lead security architect for the entire product line of Hardware Security Modules (HSMs), working on embedded systems' security. His PhD thesis was focused on the security and resilience of electronic payment systems.

28 **Alexander Michael Vetterl** (2016 – 2020)
Honeypots in the age of universal attacks and the Internet of Things

After completing his PhD, Alexander worked briefly as a Postdoc at the Cambridge Cybercrime Centre. He has since moved outside academia and is now a project leader with BCG.

29 **Mansoor Ahmed** (2017 – 2021)
Decentralised computer systems

After completing his PhD, Mansoor worked briefly as a postdoc under Jon Crowcroft before starting his own company, OpenOrigins, where he works on provable content authenticity.

30 **Ilia Shumailov** (2017 – 2022)
On security of machine learning

After completing a PhD with Ross, Ilia Shumailov joined Google DeepMind, where he currently leads research in Security and Privacy.

31 **Nicholas Boucher** (2020 – 2024)
Deception and defense from machine learning to supply chains

Nicholas Boucher completed his PhD shortly before Ross' passing in 2024. He has since continued his work at Microsoft, with which he was affiliated throughout his studies, where he leads a team securing commerce systems.

Ross Anderson's PhD ancestors

Compiled by Frank Stajano

University of Cambridge

Sir Maurice Wilkes, who led the effort to built EDSAC (the first stored-program computer to go into regular use), was the Head of our Department from 1945 to 1980. Ross Anderson, like a majority of our faculty members until at least the turn of the millennium, was an academic descendant of Sir Maurice, in his case through David Wheeler and Roger Needham. But from whom did Sir Maurice himself descend? From no less than Galileo and Newton, it turns out, which means that so did Ross—as well as all of his former students listed in the previous chapter, together with their own students.

The following information comes from the database of the Mathematics Genealogy Project at `https://mathgenealogy.org`.

- Ross John Anderson's advisor was Roger Michael Needham.
- Roger Michael Needham's advisor was David John Wheeler.
- David John Wheeler's advisor was Maurice Vincent Wilkes[1].
- Maurice Vincent Wilkes's advisor was John Ashworth Ratcliffe.
- John Ashworth Ratcliffe's advisor was Edward Victor Appleton[2].
  Edward Victor Appleton's advisors were Joseph John Thomson[3] and Ernest Rutherford[4] (Now we're branching out non-linearly... We follow Joseph John Thomson for brevity.)
- Joseph John Thomson's advisor was John William Strutt (Lord Rayleigh)[5].
- John William Strutt (Lord Rayleigh)'s advisors were Edward John Routh, George Gabriel Stokes and James Clerk Maxwell. (We follow James Clerk Maxwell.)
- James Clerk Maxwell's advisor was William Hopkins.
- William Hopkins's advisor was Adam Sedgwick.
- Adam Sedgwick's advisors were Thomas Jones and John Dawson. (We follow Thomas Jones.)
- Thomas Jones's advisors were Thomas Postlethwaite and John Cranke. (We follow Thomas Postlethwaite.)
- Thomas Postlethwaite's advisor was Stephen Whisson.
- Stephen Whisson's advisor was Walter Taylor.
- Walter Taylor's advisor was Robert Smith.
- Robert Smith's advisor was Roger Cotes.
- Roger Cotes's advisor was **Isaac Newton**.

[1] Turing Award.
[2] Nobel Prize in Physics.
[3] Nobel Prize in Physics.
[4] Nobel Prize in Chemistry.
[5] Nobel Prize in Physics.

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

- Isaac Newton's advisors were Isaac Barrow and Benjamin Pulleyn. (We follow Isaac Barrow.)
- Isaac Barrow's advisors were Vincenzo Viviani and Gilles Personne de Roberval. (We follow Vincenzo Viviani.)
- Vincenzo Viviani's advisors were **Galileo Galilei** and Evangelista Torricelli. (We follow Galileo Galilei.)
- Galileo Galilei's advisor was Ostilio Ricci.
- Ostilio Ricci's advisor was Niccolò Fontana Tartaglia.
- The advisor of Niccolò Fontana Tartaglia is unknown.

Those of a curious nature might now backtrack, exploring the other branches of the graph we did not visit, and discover other famous academic ancestors of Ross.

Part II

Festschrift

Revisiting the Limits of Steganography

Rainer Böhme

University of Innsbruck, Austria

Abstract. I select five key ideas from Ross Anderson's first paper on steganography and show how they have influenced the state of the art. The ideas are: content-adaptive steganography, the selection channel, the diminishing secure rate, generative steganography, and epistemic limits.

Keywords: Information Hiding · Steganography · Ross Anderson.

1 Hiding and Freedom

In 1996, Ross Anderson brought together researchers from five different subfields who had a common interest in hiding some information in other data (or noise) to achieve a security objective. This marked the beginning of a series of first bi-annual, then annual workshops on "Information Hiding" (IH), which continue to this day. The 2024 edition was held in Baiona, Spain and the 2025 edition will be held in San Jose, California. Incidentally, the forerunner of PETS[1] was also born out of this workshop series. Ross's own contribution to the first edition of IH was a short essay on "Stretching the Limits of Steganography" [2]. An extended journal version [3], co-authored with his student Fabien A. Petitcolas, is now Ross's third most cited paper.

Among other things, digital steganography was of interest in the first "crypto wars" [1] as an argument against restricting the use of cryptography. If a technology exists that allows undetectable secret communication, it becomes pointless to enforce laws that prohibit secret communication. Many of the cutting-edge technologies discussed at the workshop have societal implications. Sender anonymity supports freedom of expression, while watermarking for digital rights management enables applications that may deprive users of their autonomy.

For this piece, I re-read Ross's original work on steganography and point out striking technical insights that have led to the development of whole strands of literature, as well as some "rediscoveries," that are now linked to Ross's ideas. His 1996 paper appears surprisingly fresh after almost 30 years, and I would like to share some of my observations with the readers.

2 Groundbreaking Ideas for Digital Steganography

Recall that digital steganography aims to hide a secret message undetectably in inconspicuous cover objects. The sender and recipient share a key, and no

[1] Privacy Enhancing Technologies Symposium, `https://petsymposium.org`

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

one else should be able to tell whether an object contains any secret message or not [24]. The task is to find or modify an object so that it contains the message under the key and is indistinguishable from typical objects on the channel.

2.1 Content-Adaptive Steganography

Since finding a stego object by sampling quickly becomes inefficient for larger messages, the common approach for the sender is to sample a single cover object and modify it carefully. To reduce the risk of detection, local modifications should take into account the surrounding content. Ross described this for images in the spatial domain:[2]

> "Of course, not every pixel may be suitable for encoding ciphertext: changes to pixels in large fields of monochrome colour, or that lie on sharply defined boundaries, might be visible. So some systems have an algorithm that determines whether a candidate pixel can be used [...]"

All relevant embedding function today build on this observation and are content-adaptive. Nowadays suitability is no longer binary. Researchers are developing and comparing distortion functions that approximate the effect on detectability of changing an element in the cover [22]. What remains challenging is dealing with non-additive distortion, for example in cases where two or more pixels should better be changed together or not at all [23].

2.2 Selection Channel

Content-adaptive embedding makes the extraction more difficult. How does the recipient know where to look for the message? Simply applying the same suitability metric may not be successful, as the result may not be the same for the received object that has been modified during embedding. Ross's idea of a selection channel was to find an encoding that would not even require the recipient to know where the embedding was taking place:

> "We will use our keystream generator to select not one pixel but a set of them, and embed the ciphertext bit as their parity. This way, the information can be hidden by changing whichever of the pixels can be changed least obtrusively."

This idea became a game changer when it was generalized in *wet paper coding* [11], and later combined with syndrome coding [9]. In Ross's original scheme, it was difficult to find the right set size k. If it was too large, the capacity was reduced to $1/k$ of the available elements. If you make it too small, you increase the risk that at least one of the many sets doesn't have a good option for making an embedding change, and you get caught. Codes with low-density parity check matrices allow for larger overlapping sets, but require the sender to solve a system of equations. Doing this efficiently [10] while satisfying statistical properties of the change vector [17] is an open problem.

[2] For completeness, the idea can be found in an earlier (German) source [19] for audio, but the concept is less general there and the source is not widely available.

2.3 Diminishing Secure Rate

Ross also reflected on the secure capacity of a channel. He had the right intuition that steganography should not be thought of as a one-shot game, because the adversary accumulates evidence.

> "Thanks to the Central Limit Theorem, the more covertext we give the warden, the better he will be able to estimate its statistics, and so the smaller the rate at which [the sender] will be able to tweak bits safely. The rate might even tend to zero."

The result that every (marginally) imperfect sender will be caught in the long run, and thus the secure rate is zero, was formalized in the *square root law* [14], first for the asymptotic case of $n \to \infty$ independent objects, and later empirically established for objects of varying sizes [16]. In the best case, a sender who can choose a cover object of size n must limit the number of embedding changes proportional to $\sqrt{n}$ in order to keep the risk of detection constant. The applicability of this law to content-adaptive embedding is an open problem [15].

Conversely, a strictly positive secure rate can only be attained if the steganography is perfect, i. e., the distributions of the cover and stego objects are identical.

2.4 Generative Steganography

There are channels where this is possible in principle because the distribution of objects is defined, e. g., by a generative language model or a generative adversarial network [12]. If you assume such a channel, it becomes possible to make stego objects indistinguishable from covers and thus attain a positive secure rate [13]. But why would such channels exist in the first place? Wouldn't it be easier to exchange the latent space of the model and 'decompress' it at the recipient's end? Ross clearly saw the link between perfect compression and undetectability:

> "Information theorists assume that any signal can in theory be completely compressed. But if this could ever be done in practice, then the steganography problem would become trivial: [The sender] can just 'uncompress' her ciphertext getting a comprehensible message, and [the adversary] would have to pass the result."

With recent developments in learned large language models and neural image compression [4], it may be within reach to iterate over the values of the latent space in order to generate objects close enough to the channel distribution to be indistinguishable from real objects. Similarly, setting the latent space to the (encrypted) message should result in a secure stego object. What remains a challenge is to exactly retrieve the latent space from the generated object, as the generation involves floating-point operations and rounding losses. Until this problem is solved, coding is required to make the message extractable [20].

2.5 Epistemic Limits

The assumption of a channel with a defined distribution, even if it is encoded in an incomprehensible way in billions of trained parameters, is arguably an escape from solving a steganographic problem.[3] One could also imagine a channel where mathematicians exchange random numbers, so any encryption scheme would provide secure steganography in this channel.

Ross acknowledged that the channel distribution is not under our control and is generally not fully understood. What is known about it needs to be captured in models:

> "Performance of [the adversary's] job depends on his having a model of the source, and the danger to Alice and Bob is that his model might be better than theirs."

Today's models are inferred from data. Detecting stego objects with learned classifiers was proposed in 2003 [18] and is now the standard. Machine learning is also increasingly used on the sender's side [6]. The race for the better (trained) model turns into a race for access to more and better training data, and for efficient ways to closely approximate the underlying distributions. This is a problem common to many fields, most notably machine learning.

One difference is that approximation errors are not just "challenging cases" to be buried in supplementary material, but security vulnerabilities. When discovered, the system is "broken." Good designs provide evidence of their absence.

To me, this shows how fundamental steganography research is. It is about the ability to decide on hypotheses, to learn about reality from incomplete observations, including understanding what information is lost during processing, and to do all this efficiently and, if possible, with guarantees. Because every gap gives an advantage to the adversary. Moreover, the scope is not limited to message exchange. Making something artificial indistinguishable from something real appears in many corners of security [21]. Steganography remains fascinating.

3 Concluding Remarks

In this area, as in many others, Ross did what he liked best, doing groundbreaking research "with shovels". This paved the way for others to fill in the details "with pincers", including myself with a dissertation on the epistemic limits of steganography [7,8]. Ross also brought people together and created a community. I recommend that readers attend a future edition of the (now) *ACM Workshop on Information Hiding and Multimedia Security*.[4]

Working on this contribution to the Festschrift has reminded me of the value of reading original work. I encourage all researchers to trace ideas back to their source by following the citation trail (and finding ways to fill in the gaps).

[3] The GPT-2 channel assumed in [13] was distinguishable from real text at the time the paper was written: `https://huggingface.co/openai-detector/` (accessed: July 2021). Neural compression can be distinguished from conventional compression [5].

[4] `https://www.ihmmsec.org/`

References

1. Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benalob, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller and Bruce Schneier. "The Risks of Key Recovery, Key Escrow, and Trusted Third-party Encryption". *World Wide Web Journal*, **2**(3):241–257, 1997.
2. Ross J. Anderson. "Stretching the Limits of Steganography". In Ross J. Anderson (Editor), *Information Hiding (1st International Workshop)*, volume 1174 of *Lecture Notes on Computer Science*, pages 39–48. Springer, 1996.
3. Ross J. Anderson and Fabien A. P. Petitcolas. "On the Limits of Steganography". *IEEE Journal on Selected Areas in Communications*, **16**:474–481, 1998.
4. Johannes Ballé, David Minnen, Saurabh Singh, Sung Jin Hwang and Nick Johnston. "Variational Image Compression with a Scale Hyperprior". In *International Conference on Learning Representations (ICLR)*. OpenReview.net, 2018. URL `https://openreview.net/forum?id=rkcQFMZRb`. (accessed: December 2024).
5. Sandra Bergmann, Denise Moussa, Fabian Brand, André Kaup and Christian Riess. "Forensic Analysis of AI-Compression Traces in Spatial and Frequency Domain". *Pattern Recognition Letters*, **180**:41–47, 2024.
6. Solène Bernard, Patrick Bas, John Klein and Tomás Pevný. "Backpack: A Backpropagable Adversarial Embedding Scheme". *IEEE Transactions on Information Forensics and Security*, **17**(9):3539–3554, 2022.
7. Rainer Böhme. *Improved statistical steganalysis using models of heterogeneous cover signals*. Ph.D. thesis, Technische Universität Dresden, Department of Computer Science, Dresden, Germany, 2008.
8. Rainer Böhme. "An Epistemological Approach to Steganography". In Stefan Katzenbeisser and Ahmad-Reza Sadeghi (Editors), *Information Hiding (IH)*, volume 5806 of *Lecture Notes in Computer Science*, pages 15–30. Springer, 2009.
9. Ron Crandall. "Some Notes on Steganography". Mimeo posted to a mailing list, 1998. Online available at `http://dde.binghamton.edu/download/Crandall_matrix.pdf` (accessed: November 2024).
10. Tomáš Filler, Jan Judas and Jessica Fridrich. "Minimizing Additive Distortion in Steganography Using Syndrome–Trellis Codes". *IEEE Transactions on Information Forensics and Security*, **6**(3-2):920–935, 2011.
11. Jessica Fridrich, Miroslav Goljan and David Soukal. "Perturbed Quantization Steganography with Wet Paper Codes". In Jana Dittmann and Jessica J. Fridrich (Editors), *ACM Multimedia and Security Workshop (MM&Sec)*, pages 4–15. ACM, 2004.
12. Jamie Hayes and George Danezis. "Generating Steganographic Images via Adversarial Training". In *Advances in Neural Information Processing Systems*, pages 1954–1963. 2017.
13. Gabriel Kaptchuk, Tushar M. Jois, Matthew Green and Aviel D. Rubin. "Meteor: Cryptographically Secure Steganography for Realistic Distributions". In Yongdae Kim, Jong Kim, Giovanni Vigna and Elaine Shi (Editors), *ACM Conference on Computer and Communications Security (CCS)*, pages 1529–1548. ACM, 2021.
14. Andrew Ker. "Batch Steganography and Pooled Steganalysis". In Jan Camenisch, Christian Collberg, Neil Johnson and Phil Sallee (Editors), *Information Hiding (IH)*, volume 4437 of *Lecture Notes in Computer Science*, pages 265–281. Springer, 2007.
15. Andrew Ker. "The Square Root Law of Steganography: Bringing Theory Closer to Practice". In Matthew C. Stamm, Matthias Kirchner and Sviatoslav

Voloshynovskiy (Editors), *ACM Workshop on Information Hiding and Security Workshop (IH&MMSec)*, pages 33–44. ACM, 2017.
16. Andrew Ker, Tomáš Pevný, Jan Kodovský and Jessica Fridrich. "The Square Root Law of Steganographic Capacity". In Andrew Ker, Jana Dittmann and Jessica Fridrich (Editors), *ACM Multimedia and Security Workshop (MM&Sec)*, pages 107–116. ACM, 2008.
17. Olaf Markus Köhler, Cecilia Pasquini and Rainer Böhme. "On the Statistical Properties of Syndrome Trellis Coding". In Christian Krätzer, Yun-Qing Shi, Jana Dittmann and Hyoung-Joong Kim (Editors), *Digital Forensics and Watermarking (IWDW)*, volume 10431 of *Lecture Notes in Computer Science*, pages 331–346. Springer, 2017.
18. Siwei Lyu and Hany Farid. "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines". In Fabien A. P. Petitcolas (Editor), *Information Hiding (IH)*, volume 2578 of *Lecture Notes in Computer Science*, pages 340–354. Springer, 2003.
19. Steffen Möller, Andreas Pfitzmann and Ingo Stierand. "Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist *[Computer-based steganography: how it works and why any regulation of encryption is therefore nonsensical]*". *Datenschutz und Datensicherung*, **18**(6):318–326, 1994.
20. Tamio-Vesa Nakajima and Andrew D. Ker. "The Syndrome-Trellis Sampler for Generative Steganography". In *IEEE Workshop on Information Forensics and Security (WIFS)*. IEEE, 2020.
21. Cecilia Pasquini, Pascal Schöttle and Rainer Böhme. "Decoy Password Vaults: At Least As Hard As Steganography?" In Sabrina De Capitani di Vimercati and Fabio Martinelli (Editors), *ICT Systems Security and Privacy Protection (IFIP SEC)*, volume 502 of *IFIP Advances in Information and Communication Technology*, pages 327–340. Springer, 2017.
22. Tomáš Pevný, Tomáš Filler and Patrick Bas. "Using High-Dimensional Image Models to Perform Highly Undetectable Steganography". In Rainer Böhme, Philip Fong and Reihaneh Safavi-Naini (Editors), *Information Hiding (IH)*, volume 6387 of *Lecture Notes in Computer Science*, pages 161–177. Springer, 2010.
23. Tomás Pevný and Andrew D. Ker. "Exploring Non-Additive Distortion in Steganography". In Rainer Böhme, Cecilia Pasquini, Giulia Boato and Pascal Schöttle (Editors), *ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec)*, pages 109–114. ACM, 2018.
24. Gustavus J Simmons. "The Prisoners' Problem and the Subliminal Channel". In David Chaum (Editor), *Advances in Cryptology, Proceedings of CRYPTO '83*, pages 51–67. Plenum Press, 1984.

Acknowledgements

I would like to thank Benedikt Lorch for useful comments on a draft of this work, and the organizing team, especially Frank Stajano, for their efforts in putting together the Rossfest Symposium.

Observations on Focused Workshops: One of Ross's Many Services to the Field; Illustrated by a Discussion of the Origins of IHW

John McHugh[0000-0003-2900-1966]

Assurance Labs, Inc. Gaithersburg, MD 20886 USA
https://www.assurancelabs.tech info@assurancelabs.tech

Abstract. In Ross Anderson's CV is a section entitled "Research mentoring and management" in which Ross mentions the four conference series that he started. The purpose of this note is to examine these series, with special attention to the Information Hiding series where a paper of mine appears to be the spark that ignited the flame. I believe that the workshop series have been especially effective at advancing niche areas within the general field of computer security and advocate the establishment of similar series as a way to advance research in other specialized segments of the area. The paradigm seems to be especially effective in bringing practitioners and researchers together and in promoting interdisciplinary collaborations.
The first Information Hiding Workshop (IHW) took place in 1996 in Cambridge but its origin probably goes back to work that I did in the early 1990s and an "accidental" paper from 1992. I believe that it was this paper that sparked Ross's interest in the area of information hiding. It is worth examining the chain of events that led to the first IHW because this provides insight into the ways in which Ross created communities and their impact on the field of computer security. In addition to establishing the field of information hiding, it led to a friendship that was cut short by Ross's untimely death.

Keywords: Information Hiding · Research Process · Personal History

1 Winning friends (or at least influencing people)

Ross started four workshop series, Fast Software Encryption (1993), Information Hiding (1996), the Workshop on Economics and Information Security (2002) and the Workshop on Security and Human Behaviour (2008). Each of these is ongoing and each has engendered a research community and, more importantly, each has resulted in substantial interaction between practitioners and researchers. There is an important lesson to be learned here.

Much of the academic computer science community operates in a vacuum, isolated from the real world where people want to use computers to solve their real problems. This definitely applies to computer security. For example, much of

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

the recent academic literature in malware analysis focuses on evasion techniques but there is a substantial mismatch between the techniques that are the focus of research and those encountered by analysts in the field [16]. Some years ago, I participated in a study of security operations centers, SOCs, that attempted to discover why they were generally ineffective. We trained analysts in the anthropological technique of "Participant Observation" and embedded them in a series of SOC operations. In general, the results [15,2] are encouraging but, in a sense, disheartening in that while many SOCs are dysfunctional the reasons vary widely. Nonetheless, having researchers function as practitioners tends to focus the research on real problems.

Focused workshops such as the ones that Ross founded are another way to bring research and user communities together. He organized the first Fast Software Encryption workshop in 1993. It continues to this day. I attended the first IHW in 1996. It merged with the Multimedia Security workshop in 2013 and continues in that form. I presented a paper at the first Workshop on Economics and Information Security in 2002. The series continues to this day as does the Security and Human Behavior series started in 2008. Based on my experiences with the two series in which I have participated, these workshops attract a better mix of practitioners and researchers than most more general conferences in the security field. In addition, the academic participants tend to be more interdisciplinary than is the case for more general conferences. I believe that this is desirable and should be encouraged. The operative question is how. Ross managed this on multiple occasions and I hope that discussions with the participants of this meeting will provide insight into the process and provide guidance for those of us who hope to emulate it.

2 Workshops as Community Builders

Each of the focused workshops that Ross organized has flourished, at least in part because they brought together a diverse group of people united by a common interest and a need to make progress in a specific area. In the case of IHW, the field quickly grew far beyond my initial contribution, described in section 5, below. Building a community is a complicated process. The presentation of papers is only a small part of it. Community requires substantial interaction between individual members of the community. This often involves extra-curricular social activities. The first IHW included a field trip to Bletchley Park with a tour guided by the late Tony Sale [13]. Most subsequent IHWs featured social activities for the group as well, often walking excursions, that offered additional opportunities for community formation. A relaxed schedule with the talks spread over several days, ample time for presentations and discussions aided the process, as well. As far as I can tell, most of the workshops that Ross started have operated as stand alone events. While this complicates the logistics and requires the host (individual or institution) to advance funding and take on financial risk, the stand alone format generally encourages participation by those who are seriously interested in the subject. While many major conferences provide venues for

associated workshops, these are often limited to a single day or even half a day; a format that is not as conducive to community formation although it may work to sustain an established community. They also tend to attract people who are attending the main event and who have only a casual interest in the specialty. In my experience, the presence of a substantial group of non-participants dilutes the interactions.

3 Workshops as Career Builders

In academic circles, workshop publications tend to be discounted, but they are often critical in starting or advancing careers. I was the organizer for the 2001 (fourth) IHW. In addition to a controversial paper that did not appear [4], the workshop helped to advance the careers of several participants. We accepted a practical application paper [14] from a young man, Toby Sharp, who had built an image steganography system to allow a friend to communicate successfully from a repressive country. The author was able to obtain a grant for air fare from England, but had no other support. My wife and I hosted him in our house. Subsequently, he asked me to write a letter of recommendation when he applied for a position at Microsoft's research facility in Cambridge, UK. He is now a senior researcher in the Computer Vision and Augmented Reality fields at Google.

A student author, Ahmad-Reza Sadeghi, presented a paper [1] on his own at the workshop and was co-author of another [12]. He is now a full professor with the System Security Lab at the Technical University of Darmstadt. He came despite considerable difficulties in getting a US visa to attend and extensive interrogation by the immigration authorities when he arrived at Dulles Airport where I met him.

Several of the student authors of [4] have also done well although the paper did not get presented at IHW due to legal challenges from the Secure Digital Music Initiative (SDMI). Scott Craver has enjoyed a successful career at Binghamton University in New York. Dan Wallach is a full professor at Rice University in Houston, TX, and is currently on leave to serve as a program manager at DARPA.

On the other hand, no good deed goes unpunished. Ira Moskowitz who served as the program Chair for the workshop and I were included in the legal actions threatened by the SDMI. Carnegie Mellon University, where I held a position at the Software Engineering Institute, supported me and said that they would fight any action against me. The Naval Research Lab, where Ira worked, essentially repudiated Ira's role, offering no support. Ira subsequently withdrew from professional activities.

4 The Origins of IHW

At the time I wrote the paper that apparently sparked Ross's interest in information hiding, the topic was far from my mind. I got my PhD at The University

of Texas in 1983 with a dissertation that examined potential code optimizations enabled by the presence of formal specifications and a reasonably powerful (for its day) theorem prover. The Gypsy group, of which I was a member, built one of three tools (the GVE) suitable for analyzing code to be evaluated at the B3 and A1 levels of the Trusted Computing Systems Evaluation Criteria [5] (TCSEC or "Orange Book"). The Gypsy group became Computational Logic, Inc. (CLI) and I became the Vice President of CLI in charge of applications support. CLI supported the GVE under contract to our friends at Ft. Meade and obtained funding from DARPA. My office in North Carolina worked on verification related contracts including a DARPA funded software engineering process research project with TRW [10]. When my office closed, I kept the TRW project because of a "key personnel" clause in the contract and moved it to UNC where I obtained a research faculty position.[1]

The process model was a variation on Barry Boehm's risk driven spiral model [3] with security considerations being the primary risk drivers. The second phase of the TRW project required us to apply the process model developed in the first phase to a sample development. We chose to attempt a TCSEC B3 version of X Windows [6,7], a popular windowing system for Unix. The prototype was implemented on Sun 3 workstations and its performance was "sluggish but usable". One of the team, Jeremy Epstein, thought that TRW should turn it into a product and sell it to the trusted systems development community. Although TRW was not a product company, Jeremy got a bit of funding and took the prototype on the road. He came back enthusiastic, but with a caveat.

Jeremy: They really like it, but it needs a downgrader.
Me: You mean that they want to look at an image on the screen, say "nothing classified here," push a button and the image file moves to the low side?
Jeremy: Yes, yes! that's what they want.
Me: They are out of their f*****g minds.

5 A Cautionary note...

Earlier, I had done a bit of work on a downgrader for text files [11] and knew some of the pitfalls. Back at UNC, I posed the problem to a colleague who threw it out in a meeting of the graphics research group. Charles Kurak, a graduate student who had been a computer software analyst while in the Navy understood the problem and, in a matter of hours, ginned up a demo program for low order bit(s) image embedding in uncompressed grayscale images using available libraries and a bit of glue code. When he brought me some examples, I was thrilled and told him that he should write it up for publication. He said that he was too busy studying for qualifying exams to write a paper, so I wrote the paper [9] (listing him as first author) and, with his permission, sent it to ACSAC where I presented it in December of 1992. As I recall, it was well received, but no one got excited.

[1] If you can bring in funding, you can pay yourself a salary.

In May of 1993, I attended the IEEE Security and Privacy conference in Oakland and Ross, who I knew slightly at the time, caught me during a break and asked about the paper. Buried in the paper is a conjecture that the information carrying capacity of an image is related to the difference in size between the base image compressed with the best available lossless compression technique and the size of the file compressed with a lossy compression technique that results in an image that when decompressed is subjectively identical to the original. Ross asked if I had a proof and I admitted that I did not, but that the conjecture seemed reasonable. Note that the conjecture is relatively loose as it depends on the ability of the viewer to see small differences and on the display to show them accurately. Nonetheless, the conjecture seems reasonable as it captures the essence of the situation: how much can you get away with given a human operator and a less than perfect display.

Several years passed before I again met Ross and he reported that one of his students had proven the conjecture after considerable effort. Subsequently, Ross invited me to attend the first Information Hiding Workshop. I was able to include a stop in Cambridge in another trip and made it to the second and third days of the first IHW.

6 The Rest Is History, Public and Personal

I got to know Ross better at the workshop and we met regularly at various conferences and other events. My late wife, Ruth, accompanied me on a number of these trips as Shireen often accompanied Ross. We were at their house for the publication party they held when the first edition of Ross's "Security Engineering" was published. I was honored to be one of the readers for portions of the book. The copy that he gave me remains a prized possession. I find the inscription telling (see Figure 1 in Appendix A) because it captures Ross's general inquisitiveness, which I share, along with a wicked sense of humor (or a degree of ambiguity when it suits the purpose).

Over the years, I remained involved in the information hiding community, presenting papers, attending the workshop, and chairing the 2001 workshop.

We visited Ross and Shireen on a number of occasions outside Cambridge and they visited us at our place in the North Carolina mountains. Ruth and I both cooked and we cooked with Shireen on several occasions, including a memorable dinner in their apartment in the hotel in St. Lucia where Ross was participating in Financial Crypto 2011. Ross's interests covered many areas, including many aspects of the National Health Service. Ruth had a PhD in Public Health and they had interests in common. Any gathering that included either of them could be counted on for both good conversation as well as good food and drink.

Twenty nine years later, in 2021, the paper got a "Test of Time Paper Award" from ACSAC. The images used in the original paper are long gone, but I re-implemented the algorithm from the paper and made new images, e.g. Figure 2 in Appendix A. Much to my surprise, the paper is still being cited, typically as the first published paper in digital steganography. At the time of the award, Ross

noted a revival of interest in the area, "thanks to the mania for neural-network applications." mentioning [8] in passing.

A Figures

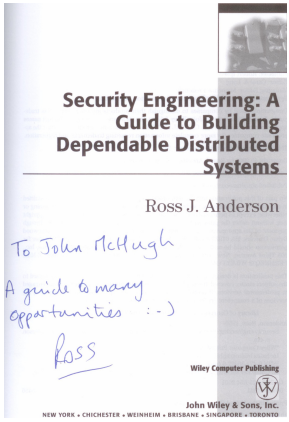

Fig. 1. Title Page from "Security Engineering"

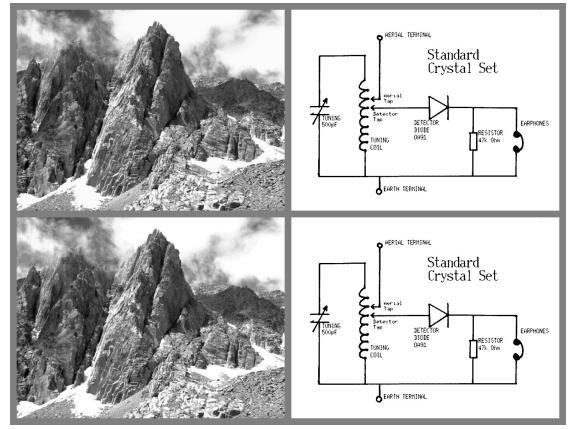

Fig. 2. Low Order Bit IH: 8 bit cover, 3 bit embed / modified image, 3 bit extracted

References

1. Andre Adelsbach and Ahmad-Reza Sadeghi. "Zero-Knowledge Watermark Detection and Proof of Ownership". In Ira Moskowitz (Editor), *Fourth International Workshop on Information Hiding*, number 2137 in LNCS, pages 273–288. 2001.
2. "Argus Cyber Security Lab", 2024. This site contains numerous references on "Bringing Anthropology into Cybersecurity".
3. B. W. Boehm. "A spiral model of software development and enhancement". *Computer*, **21**(5):61–72, 1988. `https://doi.org/10.1109/2.59`.
4. Scott A. Craver, Min Wu, Bede Liu, Ben Swartzlander, Dan S. Wallach, Drew Dean and Edward W. Felten. "Reading Between the Lines: Lessons from the SDMI Challenge". In *10th USENIX Security Symposium (USENIX Security 01)*. USENIX Association, Washington, D.C., August 2001. URL `https://www.usenix.org/conference/10th-usenix-security-symposium/reading-between-lines-lessons-sdmi-challenge`.
5. Department of Defense. *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985. DOD 5200.28-STD (supersedes CSC-STD-001-83).
6. Jeremy Epstein, John McHugh, Hilarie K. Orman, Rita Pascale, Ann B. Marmor-Squires, Bonnie P. Danner, Charles R. Martin, Martha A. Branstad, Glenn S. Benson and D. Rothnie. "A High Assurance Window System Prototype". *J. Comput. Secur.*, **2**(2-3):159–190, 1993. `https://doi.org/10.3233/JCS-1993-22-306`.

7. Jeremy Epstein, John McHugh, Rita Pascale, Charles Martin, Douglas Rothnie, Ann Marmor-Squires Hilarie Orman, Martha Branstad and Bonnie Danner. "Evolution of a Trusted B3 Window System Prototype". In *IEEE Symposium on Security and Privacy*. 1992.
8. David Khachaturov, Ilia Shumailov, Yiren Zhao, Nicolas Papernot and Ross Anderson. "Markpainting: Adversarial Machine Learning meets Inpainting", 2021. URL `https://arxiv.org/abs/2106.00660`.
9. Charles Kurak and John McHugh. "A Cautionary Note on Image Downgrading". In *Computer Security Applications Conference*. Dec 1992.
10. Ann Marmor-Squires, John McHugh, Martha Branstad, Bonnie Danner, Lou Nagy, Pat Rougeau and Dan Sterne. "A Risk Driven Process Model for the Development of Trusted Systems". In *Computer Security Applications Conference*. Tucson, Az, Dec 1989.
11. John McHugh. *Computer and Network Security*, chapter An EMACS Based Downgrader for the SAT, pages 228–237. IEEE Computer Society Press, 1986.
12. Ahmad-Reza Sadeghi. "How to Break a Semi-Anonymous Fingerprinting Scheme". In Ira Moskowitz (Editor), *Fourth International Workshop on Information Hiding*, number 2137 in LNCS, pages 384–394. 2001.
13. `https://www.theguardian.com/theguardian/2011/aug/31/tony-sale-obituary`, August 2011.
14. Toby Sharp. "An implementation of key-based digital signal steganography". In Ira Moskowitz (Editor), *Fourth International Workshop on Information Hiding*, number 2137 in LNCS, pages 13–26. 2001.
15. Sathya Chandran Sundaramurthy, John McHugh, Xinming Simon Ou, S. Raj Rajagopalan and Michael Wesch. "An Anthropological Approach to Studying CSIRTs". *IEEE Security & Privacy*, **12**(5):52–60, 2014. `https://doi.org/10.1109/MSP.2014.84`.
16. Miuyin Yong Wong, Matthew Landen, Frank Li, Fabian Monrose and Mustaque Ahamad. "Comparing Malware Evasion Theory with Practice: Results from Interviews with Expert Analysts". In *Proceedings of the Twentieth Symposium on Usable Privacy and Security*, pages 61 – 80. Usenix, August 2024. Presentation at `https://www.usenix.org/conference/soups2024/presentation/yong-wong`.

The Loss of a Force of Nature: Memories of Ross Anderson

Susan Landau

Tufts University, Medford, MA 02155
susan.landau@privacyink.org

Some days a force of nature is a sudden, strong gust that takes the large pile of leaves you have carefully accumulated, tossing the fronds to the four winds. Other times it is the thundering river enlarged by a spring melt, creating destinations and vistas as it carves a new path to the sea. Its most notable feature is not the potential of its destructive power but rather its creative energy. That was the essence of my friend and colleague, Ross Anderson. To those whose policies Ross found inimical, I'm sure he appeared to be that unpredictable and sometimes devastating gust. To those who largely saw eye-to-eye with Ross's ends—though not necessarily his means—Ross was forever carving new paths to the sea and creating new destinations and vistas.

Where and when Ross and I met is lost in the sands of time; it was sometime during Crypto Wars I. By Crypto Wars II, Ross and I were fighting the battles together. In between, Ross had taken on many others: copyright, Cambridge University's retirement-age policy, the US government's policy on transit passengers, and multiple others. It wasn't that Ross was deliberately argumentative, but rather that he could not accept injustice whenever he encountered it. Strategy was rarely part of Ross's decision to take on a battle; Ross took issues on because he simply couldn't bear the injustice that he saw taking place. Making progress in so many battles requires a person to be of inexhaustible energy, tremendous certainty, and smart. Ross was all three.

Working with Ross tossed one into a storm of exciting ideas, important social struggle, and for many of us, periodic exhaustion. There was also enormous mental stimulation and a challenge to sharpen your thinking. And there was one more challenge: you never knew when you would be met with Ross's Scottish obstreperousness. But it was worth it. To spend time with Ross was to be with someone with great imagination, humor, and a zest for life.

A hallmark of Ross's working style was to be all in. If he was working on encryption policy, he would be simultaneously working on encryption algorithms, related security problems, papers on problems regarding the government's stance on encryption. If that weren't enough, Ross would find a policy organization to put out whitepapers, write op-eds, appear on panels, and galvanize the opposition. And if there weren't institutions to support his projects, Ross would create them.

The Santa Barbara CRYPTO meeting was where everyone used to go for anything cryptographic (or crypto, as we used to call the field in the days before blockchain became a household word). Ross realized that, great as the meeting was, CRYPTO was largely missing out on the workhorse of cryptography:

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

symmetric-key systems. So while still a graduate student, Ross started the Fast Software Encryption conference (FSE) in 1992. The result was an energetic research community focused on symmetric-key primitives. Work at FSE influenced the Advanced Encryption Standard, lightweight cryptographic algorithms, and other standards.

By the late 1990s, the US had a small but robust set of civil-society organizations focusing on the digital world; due to different funding mechanisms across the pond, the UK and Europe did not. Forces of nature are not waylaid by barriers. Seeing threats to online freedom and privacy, in 1998 Ross and Caspar Bowden founded the Foundation for Information Policy Research (FIPR), which jumped right into battle. Tackling the proposed Regulation of Investigatory Powers Act (RIPA), FIPR fought the bill's proposed warrantless collection of browsing information and corporate criminal liability due to failure to decrypt. FIPR won; these and other freedom-infringing aspects of RIPA were removed prior to passage.

Perhaps starting FIPR gave Ross enthusiasm for starting organizations, or perhaps that zest was always present in him. In any case, it became manifest afterwards, to the great intellectual benefit of many of us and to the field of cybersecurity.

By the late 1990s, many of us began to realize that cybersecurity was not just a technical problem. Ross decided to do something about it. After a fruitful sabbatical with Hal Varian at Google, Ross went on to create the Workshop in Economics of Information Security (WEIS), a venue in which computer scientists and economists could tackle the externalities of (the lack of) computer security, hone their arguments, and then publish the polished work in the appropriate venue for their field. It's where students in the field could try their arguments as well, rubbing shoulders with eminent economists and forward-thinking computer-security professionals. WEIS has now provided an outlet for multiple generations of researchers in the economics of information security. In bringing together these two disciplines the meetings have had tremendous value; we now have a far greater understanding of the barriers in adopting security solutions as well as a body of work analyzing which solutions are more likely to be valuable. Without WEIS as a conduit for such discussions, our grasp of the problems would be far less.

Ross, being Ross, didn't stop there. His next conference adventure was the informal but carefully structured Security and Human Behaviour Workshop (SHB), in which a hand-picked group of social scientists, computer scientists, and random others mixed and mingled and gave brief talks about their own work. The real purpose was to stretch minds among people who often have been looking at the same problems in far different ways from different disciplines. At this meeting, just as at WEIS, Ross blogged the talks in real time, thus sharing the ideas with a far wider audience. Ross's ability to synthesize the talks from quite diverse areas—psychology, economics, sociology, cybersecurity—and blog about them in real time was just amazing. It was also very valuable: many who

couldn't attend the meeting nonetheless got great value by learning what was being discussed.

Ross didn't create FSE, FIPR, WEIS, or SHB by himself. Ross leaned on colleagues and brought others in. He also brought in his students. Here's where I note that Ross promoted his students and colleagues, sometimes giving them professional tasks to do earlier than some might have, but in the process, ensuring that they got to meet movers and shakers in their area. Ross was caring and generous towards his students, ensuring that they had many professional opportunities from early on in their work.

By the time Ross created WEIS, I was already doing interdisciplinary work. Rather than economics and the social sciences, my focus was on legal issues related to privacy and surveillance. By the mid 2000s I'd moved into writing law-review articles (if you're going to impact policy, you need to write where the policy audience is). WEIS added a new perspective for me. Even though I didn't directly work on the economics of information security, I began regularly attending WEIS; the viewpoint the meeting provided enhanced my approach to policy issues.

Ross's willingness to stretch boundaries of fields was a critical aspect of enabling the interdisciplinary research community that Ross was seeking to foster for cybersecurity. Although the economists seek to focus on the economic issues of information security, the computer scientists on the security aspects, the sociologists on social impacts, etc., the fact is that the research is strongest when it pulls on all these different modes of thinking. That's because all shed light on why cybersecurity is so hard to achieve or what an appropriate policy solution might be.

Ross's insistence on breaking down the barriers between the different fields was really important. And yes, sometimes he did rediscover the wheel without knowing that another field had already figured out the same solution. But, of course, it is far better to think broadly than to focus too narrowly on a field and solve a small problem instead of tackling the broad overriding issue. Ross did not think small either in his own research nor in where the field should go.

Ross was a person of bountiful energy, which explains his productivity and reach across so many different fields, as well as the multiple versions of *Security Engineering* (I use the earlier ones to elevate my desktop computer to the right height; seeing their bindings as I type provides wonderful reminders of technical issues I need to consider). One example of his productivity stands out to me. We were in the middle of writing "Bugs in Our Pockets" [1] when, during a Friday afternoon call, Ross said he wouldn't do any writing over the next several days as he had to take the weekend off to write an op-ed. Sure enough, a draft of the op-ed appeared in our mailboxes on Sunday afternoon awaiting our comments.

Ross's force-of-nature approach to life was most visible on political issues, where he would not let go if he thought a situation was amiss. This could be thoroughly exhausting. But hand-in-hand with this aspect of Ross was that you always knew where you stood with him. There was no dissembling with Ross, which was a very good thing.

When I first met Ross, I was Whit Diffie's co-author on *Privacy on the Line: The Politics of Wiretapping and Encryption*. I was a female theoretical computer scientist thrust suddenly into a den of noisy and aggressive male cryptographers. Ross was among the less easy of those I met. Ross could take up lots of space and yet, at the time, it wasn't on for a woman researcher to try to do the same back. I had to learn how to hold my ground with Ross, and that personal learning curve took me some time.

In addition, my training as a mathematician had taught me to be very precise (the same is true of the law-review articles I was turning to writing). Ross had a different approach to work. His tendency was to move forward even if not all the pieces were yet in place. Ross would then come back to fill in the arguments—or not. Such behavior is really anathema to a mathematician. So there was also a professional learning curve I had to master in order to work successfully with Ross. Eventually I learned that one too. Sometimes several of us would work together fixing a joint piece of work to get the messy part precise and correct, then share the polished result with Ross. Such an approach almost always worked out just fine.

We all change and grow. When I first knew Ross, there were no other women researchers in the room. A decade ago, Alice Hutchings came to the Cambridge Computer Laboratory. Other women also arrived. Ross changed. A mail came from Ross telling me to read Crash Override: "It's about how misogyny, homophobia and toxic masculinity drove gamergate." Then Ross added words that have stayed with me ever since: "We should listen to actual victims rather than just other academics."

The world had shifted from the time when I had met Ross in the 1990s. Ross had changed. I had changed. Our relationship became a collaboration in which I could both learn from Ross, he could learn from me, and we could argue with one another. Most importantly, I could laugh with him. When you can laugh with a colleague, you can work together.

When I learned last March that Ross had died, I was in the midst of running a student workshop about machine learning and ensuring contestability, the ability of a person to contest a decision that an automated system makes about individuals. Empowering students to take on the machine is very much of a Ross kind of thing, and the news of his death stayed with me all through that day. My first reaction was shock. Ross was always so alive a human being that it was hard to imagine him no longer with us.

My second, third, and remaining thoughts have focused on Ross's irreplaceability. Ross Anderson was an argumentative, irascible Scot with a fine intellect, an inability to let a problem go, an endless energy to match, and a love of the world and for his beloved Shireen. We will not see his like again. And that is a tremendous loss for all of us.

References

1. Harold Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G Neumann, Ronald L Rivest,

Jeffrey I Schiller, Bruce Schneier, Vanessa Teague and Carmela Troncoso. “Bugs in our pockets: the risks of client-side scanning”. *Journal of Cybersecurity*, **10**(1):1–18, 01 2024. ISSN 2057-2085. https://doi.org/10.1093/cybsec/tyad020.

Ross Anderson's Contributions to Secure Healthcare Information Systems

William Yurcik[1][0009-0004-8453-3898] and
John McHugh[2][0000-0003-2900-1966]

[1] Centers for Medicare & Medicaid Services (CMS), Baltimore MD 21244, USA
[2] Assurance Labs, Inc. Gaithersburg, MD 20886 USA
William.Yurcik@cms.hhs.gov
mchugh@cs.unc.edu

Abstract. Ross Anderson greatly influenced many issues surrounding the security and privacy of healthcare information systems through his research, advocacy, and recommendations that have been adopted worldwide. In particular, the issues he addressed within the UK National Health Service (NHS) have direct parallels with other healthcare systems internationally. In this paper we comprehensively summarize his body of work highlighting many individual efforts culminating in an overall legacy contribution.
Ross Anderson argued that health data should be kept at the provider, not in large central databases vulnerable to attack. In this context he postulated what has come to be known as "Anderson's Rule". The NHS had a long history of privacy abuses which were exposed in his work. Ross Anderson advocated that patients be notified every time their health data is shared with another provider for secondary use and that we must be willing to draw "red lines" not to be crossed with health data. Most importantly, Ross Anderson argued that clinical healthcare data should move from one of opt-out/opt-in to active veto, which inspired more in-depth analysis of how we can more meaningfully balance technology advances with patient and medical staff privacy rights.

Keywords: clinical systems security · ethical issues in healthcare · health data privacy · national databases · NHS cryptography · NHS National Programme for IT · patient records · re-identification · summary care records

1 Introduction

Ross Anderson was a leader we celebrate in many aspects of security engineering, however it is underappreciated that one of these aspects is as the original trailblazer for secure healthcare information systems. In this paper we highlight Anderson's game-changing legacy in securing healthcare systems based on primary sources.

Ross Anderson's earliest work on IT system failure modes established a basis for evidence-based threat models for a wide range of applications [14,23,26].

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

However, Anderson did not confine his research to technical security techniques but rather embraced the wider context exploring the implications of system failure modes in healthcare [25,12,13,17,4,8,15,19,46]. In 1998 Anderson created the Foundation for Information Policy Research (FIPR) to study the connections between IT systems, government agencies and businesses [18,16,17,29]. He continued his research while advising the British Medical Association on clinical information systems in the 1990s [1,7] and the U.K. Information Commissioner's Office on Children's Databases in 2006 [29].

In addition to individual academic research paper contributions, Anderson authored four books, each with varying content on healthcare IT systems: *Database State* [30], *Security Engineering: A Guide to Building Dependable Distributed Systems* [14,23,26] (three editions), *Personal Medical Information* [5] (an edited compilation), and *The Global Trust Register* [31].

The remainder of this paper highlights Ross Anderson's healthcare research threads ending with a reflection on his incredible legacy in the healthcare context.

2 Healthcare IT System Hazards

The collection and use of data in healthcare IT systems has the potential for violation of individual privacy, as sensitive health information can be easily identifiable and misused when linked across multiple data sources, raising concerns about unauthorized access, disclosure, and potential discrimination against individuals based on their health data [46]. Accidental or malicious errors in medical records could lead to incorrect diagnosis and treatments causing harm or death; making healthcare information available via the Internet creates vulnerability to data breaches; and the move from paper to electronic records introduces chain-of-custody issues [46].

Ross Anderson focused on informed consent in that he trusted individuals to make decisions how their own healthcare data should be collected, used, and shared; with options to opt-in, opt-out, and/or restrict data usage [20,25,30,45]. 'Opt-in' means the default is non-participation in data collection requiring patients to actively agree to data collection, while 'opt-out' means the default is participation in data collection requiring patients to actively refuse data collection. Anderson goes one step beyond 'opt-in' and 'opt-out' by arguing that (maintaining the default being non-participation in data collection) rather than patients only having the right to consent to the use of their health data, they should also have the active right to refuse the use of their health data thus ensuring an active response from patients [20,25,30,45].

3 The UK National Health Service

The National Health Service (NHS) is the umbrella term for the publicly-funded healthcare systems of the United Kingdom, comprising the NHS in England, Scotland and Wales. In 2024, the NHS workforce was 1.5M making it the seventh largest employer and second largest non-military public organization in the

world.[3] For such a large system, productivity and effectiveness are issues to be continuously addressed.

3.1 National Programme for IT

In 2002, NHS embarked on an ambitious project called "the National Programme for IT (NPfIT)" with the goal of implementing a unified digital patient record system across all its facilities in order to improve the quality of patient care and service delivery. The NPfIT project was the largest public-sector IT program ever attempted in the UK and one of the largest civilian IT projects ever in the world [47,3,4,19,32,37,36,38]. Unfortunately the result was almost complete failure due to significant cost overruns and implementation issues, a cautionary tale commonly studied as a case in business schools [37,38,40,41,43].

For this paper, the significance of NPfIT was not in its business failure but more importantly in the security/privacy issues it raised for clinical IT systems. Anderson studied NPfIT for protecting integrity with only authorized users able to access and modify data, enforcing privacy/confidentiality with access controls and authentication, data governance, and protection against data breaches and availability outages [2,20,21,25,11,13,16,47,3,22,6,1,24,15,19,7,32].

BBC News has reported an average of about 2,500 NHS data breaches each year [34]. Some doctors warn that data breaches and data abuse were so rampant and routine within NHS systems that it could jeopardize patient trust [17,3,22,27,4,6,1,15,19,35,42,44]. Anderson's work on exposing these problems and addressing the challenges of managing sensitive medical information within the large, complex NHS healthcare system has proven to stand the test of time as seminal work [2,20,21,25,11,13,16,47,3,22,6,1,24,15,19,7,32].

3.2 Anderson's Rule

As the result of his work with NHS NPfIT, Anderson formulated the principle that you cannot construct a database system with scale, functionality and security in the same instance. What has come to be known as "Anderson's Rule" can be stated as:

> *Database systems that handle sensitive personal information involve a trilemma of security, functionality, and scale, of which you can only choose two.*

For example, (1) a database system that scales to have information on many patients and to which many people require access is hard to secure unless its functionality is restricted, or (2) for a system with rich functionality to be secure, you have to restrict the number of patients in the system and the number of people with access, or accept that some information will leak [44]. Anderson, and many others, have successfully applied this rule for many instances and no counter-examples have emerged.

[3] NHS website, `https://www.nhs.uk/`

3.3 Data Confidentiality for both Patients and Clinical Staff

Anderson advocated that in order for the NHS to have a secure patient healthcare IT system, patients and medical staff should be able to access data locally without requiring a national database [2,25,11,13,47,3,22,4,30,32]. Healthcare data can be distributed at NHS providers, not communicating over insecure wide area networks to a database vulnerable to attack. In the special cases where patient data needs to be shared within NHS, secure communications channels can be established. This decentralized approach also avoids the interoperability challenge of connecting all types of medical systems. As FIPR Chairman, Anderson states: "... no one in central government ... should have access to identifiable health information on the whole UK population" [16].

3.4 NHS Anonymization, Pseudonymization, and Cryptography

The NHS developed a patient identification system in the 1990s. This enabled the anonymization of medical records and the integration of information hosted on different systems. This information was added to a national data "spine" hosting data on every citizen. In 2003 the NHS proposed a centrally-controlled individual electronic care record (IECR) for all patients in order to combine hospital and general practioner records. By 2006, more than 90 percent of general practices in England were computerized, and one-third held electronic patient medical records [36].

For research purposes, NHS patient data was anonymized by removing all personal indicators from records. However other data was pseudonymized such that it retained some personal indicators while other personal indicators were replaced with pseudonyms. Anderson communicated that pseudonymized data can be linked to individuals when paired with other linkable records such as insurance claims [47,17,15,39,45,46].

For patient data confidentiality, NHS sought encryption algorithms and in 1996 a simplified block cipher algorithm called "Red Pike" was created for the NHS by the UK intelligence community [8,33,48]. Red Pike is a 64-bit block cipher using simple bitwise operations, no S-boxes, no key scheduling, no look-up tables, and can be implemented in a few lines of code [8,33,48]. Anderson evaluated the Red Pike algorithm and reported that he had serious reservations about the method based on the algorithm's RC-5 derived roots, S-boxes should be used, and that it was susceptible to the "glitch" attack [8,33,48]. In retrospect the issues pointed out by Anderson soon became unimportant relative to the 64-bit key size as CPU speeds dramatically increased.

4 Healthcare Databases Worldwide

Security and privacy issues in healthcare systems are not unique to the UK. Other countries, such as Austria, Netherlands, and New Zealand confronted similar problems when attempting to centralize healthcare data. For example,

New Zealand maintains a database called the National Medical Data Set which contains most citizens' health records identified by an encrypted social security number [9].

4.1 Icelandic Health Database

Iceland proposed a national healthcare database and claimed that the use of encryption and pseudonyms would protect personal information from being discoverable [10,9,12]. On behalf of the Icelandic Medical Association, Anderson evaluated that the Icelandic proposal to encrypt personal identity numbers into pseudonyms was inadequate [10,9,12]. Based on Anderson's Rule, he stated that the Icelandic Health Database could not be secured without more limited access to a smaller number of users and rejection of queries returning fewer than six patients [10,9,12].

4.2 UK Children's Database

Anderson was vigilant to the collection and use of data from vulnerable populations, such as children, to ensure their rights and interests are protected [28]. In his role as FIPR Chairman, Anderson provided a safety and privacy analysis of the UK Government's proposals to create a database for all UK children [29].

Anderson stated while it may be appropriate for privacy rules to be broken in serious cases where children were at risk, building a database for all UK children breaks many privacy protection laws without good reason and would make children's personal information vulnerable to a variety of attacks [29].

5 Ross Anderson's Legacy in Secure Healthcare IT Systems

It has been challenging to summarize Ross Anderson's contributions to secure healthcare IT systems within the constraints of this paper, as his contributions were wide-ranging and pervasive. As healthcare IT continues to evolve, especially given recent advances in AI, we must continue to re-examine the tenets Ross gave us: informed consent; Anderson's Rule; healthcare data protection via anonymization and cryptography; the hazards of national databases; and the privacy protection of vulnerable populations. With legacy defined as the positive impact a person has on others through their actions and accomplishments, one legacy of Ross Anderson will be the future healthcare IT systems we design given the important lessons he gave us.

Acknowledgments. This paper is the result of countless interactions both authors have had with Ross Anderson both directly and indirectly through research forums he created.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this paper.

References

1. Ross Anderson. "Security in Clinical Information Systems". `https://www.cl.cam.ac.uk/archive/rja14/#Med` as of 30 December 2024. This is a section in Ross's home page at Cambridge which has been archived.
2. Ross Anderson. "Clinical System Security — Interim Guidelines". *British Medical Journal*, **312**(7023):109–111, January 1996.
3. Ross Anderson. "NHS-wide Networking and Patient Confidentiality". *British Medical Journal*, **310**(6996):5–6, July 1996.
4. Ross Anderson. "Patient Confidentiality — at Risk from NHS Wide Area Networking". In *Proceedings of Healthcare 96*. March 1996.
5. Ross Anderson (Editor). *Personal Medical Information — Security, Engineering, and Ethics. Proceedings of Personal Information Workshop*. Springer-Verlag, Berlin, June 1996.
6. Ross Anderson. "Security in Clinical Information Systems". `https://www.cl.cam.ac.uk/archive/rja14/policy11/policy11.html` or `https://www.cl.cam.ac.uk/archive/rja14/Papers/policy11.pdf` as of 30 Dec 2024, January 1996.
7. Ross Anderson. "An Update on the BMA Security Policy". In *Cambridge Workshop on Personal Information — Security Engineering and Ethic*, pages 233–250. Springer Verlag, Berlin, 1996.
8. Ross Anderson. "Problems with the NHS Cryptography Strategy". `https://www.cl.cam.ac.uk/archive/rja14/Papers/zergo-critique.pdf` or `https://www.cl.cam.ac.uk/archive/rja14/zergo/zergo.html` as of 31 Dec 2024, October 1997.
9. Ross Anderson. "The DeCODE Proposal for an Icelandic Health Database". *The Icelandic Medical Journal*, **84**(11):874, November 1998.
10. Ross Anderson. "Comments on the Security Targets for the Icelandic Health Database". `https://www.cl.cam.ac.uk/ftp/users/rja14/iceland-admiral.pdf`, 1999.
11. Ross Anderson. "Healthcare Protection Profile — Comments". `https://www.cl.cam.ac.uk/archive/rja14/Papers/healthpp.pdf`, October 1999. These Comments were for a Panel *Health Care Protection Profile Initiative* at the 22nd National Information Systems Security Conference (NISSC).
12. Ross Anderson. "Iceland's Medical Database is Insecure". *British Medical Journal (BMJ)*, **319**(7201):59, 1999.
13. Ross Anderson. "Information Technology in Medical Practice: Safety and Privacy Lessons from the United Kingdom". *Medical Journal of Australia*, **170**(4):181–184, February 1999.
14. Ross Anderson. *Security Engineering — A Guide to Building Dependable Distributed Systems, 1st edition*. John Wiley & Sons, first edition, 2001.
15. Ross Anderson. "Undermining Data Privacy in Health Information". *British Medical Journal*, **322**(7284):442–443, February 2001.
16. Ross Anderson. "NHS Confidentiality Consultation — FIPR Response". `https://www.cl.cam.ac.uk/archive/rja14/fiprmedconf.html`, January 2005.
17. Ross Anderson. "NHS Systems Fail to Protect Patient Confidentiality". Foundation for Information Policy Research `https://www.fipr.org/press/030205NHS.html`, March 2005.
18. Ross Anderson. "Healthcare IT in Europe and North America". National Audit Office, 2006.

19. Ross Anderson. "Under Threat: Patient Confidentiality and NHS Computing". *Drugs and Alcohol Today*, **6**(4):13–17, December 2006.
20. Ross Anderson. "Confidentiality and Connecting for Health". *British Journal of General Practice*, **58**(547):75–76, February 2008.
21. Ross Anderson. "Connecting for Health". *British Journal of General Practice*, **8**(549):279–280, April 2008. Available at `DOI:10.3399/bjgp08X279823` as of 7 January 2025.
22. Ross Anderson. "Patient Confidentiality and Central Databases". *British Journal of General Practice*, **58**(547):75–76, February 2008.
23. Ross Anderson. *Security Engineering — A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, second edition, 2008.
24. Ross Anderson. "Security Policy Model for Clinical Information Systems". In *Proceedings of IEEE Symposium on Security and Privacy*, pages 30–43. 2008.
25. Ross Anderson. "Do Summary Care Records Have the Potential To Do More Harm Than Good? Yes". *British Medical Journal*, **340**, June 2010. Available at `https://doi.org/10.1136/bmj.c3020`.
26. Ross Anderson. *Security Engineering — A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, third edition, 2020.
27. Ross Anderson. "Patient Confidentiality in Remote Consultations". `https://www.lightbluetouchpaper.org/2021/05/27/patient-confidentiality-in-remote-consultations/`, May 2021.
28. Ross Anderson. "Chat Control or Child Protection?" *arXiv Computers and Society*, October 2022. URL `https://arxiv.org/abs/2210.08958`.
29. Ross Anderson, I Brown, R. Clayton, T. Dowty, D. Korff and E. Munro. "Children's Databases — Safety and Privacy — A Report for the Information Commissioner". `https://www.cl.cam.ac.uk/archive/rja14/Papers/kids.pdf` as of 31 December 2024. Foundation for Information Policy Research, Information Commissioner's Office, November 2006.
30. Ross Anderson, I Brown, T. Dowty, W. Heath, P. Inglesant and A. Sasse. *Database State*. The Garden House, Water End, York UK, 2009.
31. Ross Anderson, B. Crispo, J-H. Lee, C. Manifavas, V. Matyáš Jr. and FAP. Petitcolas. *The Global Internet Trust Register*. The MIT Press, 1999.
32. Ross Anderson, Rudolf Hanka and Alan Hassey. "Clause 67, Medical Research and Privacy: the Options for the NHS". `https://www.cl.cam.ac.uk/archive/rja14/Papers/hcbillc67.pdf` as of 31 December 2024, April 2001.
33. Ross Anderson and Markus Kuhn. "Improved Differential Fault Analysis". `cryptome.org/jya/akdfa.txt` as of 31 December 2024.
34. BBC News. "NHS has Repeated Data Breaches". `https://www.bbc.com/news/health-30037938` as of 31 December 2024, November 2014.
35. A. Browne. "Lives Ruined as NHS Leaks Patients' Notes". *The Guardian*, June 2000. On line at `https://www.theguardian.com/society/2000/jun/25/futureofthenhs.health` as of 31 December 2024.
36. Chantler C., T. Clarke and R. Granger. "Information Technology in the English National Health Service". *The Journal of the American Medical Association*, **296**(18):2255–2258, 2006.
37. Oliver Campion-Awwad, Alexander Hayton, Leila Smith and Mark Vuaran. "The National Programme for IT in the NHS — A Case History". `https://www.cl.cam.ac.uk/archive/rja14/Papers/npfit-mpp-2014-case-history.pdf` as of 31 December 2024, February 2014.

38. W. Currie, N. Pouloudi and E. Whitley. "Entangled Stakeholder Roles and Perceptions in Health Information Systems: a Longitudinal Study of the UK NHS N3 Network". *Journal of the Association for Information Systems*, **17**(2):107–161, 2016.
39. Ian Denley and Simon Weston Smith. "Privacy in Clinical Information Systems in Secondary CarE". *British Medical Journal*, **318**(7194):1328–1331, May 1999.
40. House of Commons, Committee of Public Accounts. "The Dismantled National Programme for IT in the NHS, Nineteenth Report of Session 2013–14". `https://publications.parliament.uk/pa/cm201314/cmselect/cmpubacc/294/294.pdf` as of 31 December 2024, July 2013.
41. T. Justinia. "The UK's National Programme for IT: Why Was It Dismantled?" *Health Services Management Research*, **30**(1):2–9, 2017.
42. V. Matyáš Jr. "Protecting Doctors' Identity in Drug Prescription Analysis". *Health Informatics Journal*, **4**(3-4):205–209, September 1998.
43. A. Maughan. "Six Reasons Why the NHS National Programme for IT Failed". *Computer Weekly*, September 2010. On line at `https://www.computerweekly.com/opinion/Six-reasons-why-the-NHS-National-Programme-for-IT-failed` as of 31 December 2024.
44. H. Porter. "Nine Sacked for Breaching Core ID Card Database". *The Guardian*, August 2009. On line at `https://www.theguardian.com/commentisfree/henryporter/2009/aug/10/id-card-database-breach` as of 31 December 2024.
45. L. Presser, M. Hruskova, H. Rowbottom and Kancir J. "Care data and Access to UK Health Records: Patient Privacy and Public Trust". *Technology Science*, August 2015. On line at `https://techscience.org/a/2015081103/` as of 31 Dewcember 2024.
46. M. Richards, Ross Anderson, S. Hinde, J. Kaye, A. Lucassen, PM. Matthews, M. Parker, MV. Shotter, G. Watts, GE. Wallace and J. Wise. "The Collection, Linking, and Use of Data in Biomedical Research and Health Care: Ethical Issue". `https://cdn.nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data-report.pdf` as of 31 December 2024, February 2015.
47. et al Ross Anderson. "The NHS's National Programme for Information Technology (NPfIT) — A Dossier of Concerns". `https://homepages.cs.ncl.ac.uk/brian.randell/Concerns.pdf`, September 2010.
48. Zergo Limited. "The Use of Encryption and Related Services with the NHSnet". NHS Executive — a copy is available at `http://www.cypherspace.org/adam/ukexport/zergo.html` as of 31 December 2024, April 1996.

The Long Shadow of the Computer Fraud and Abuse Act: Exploring User Discussions on the Legality of Vulnerability Research on Reddit

Yangheran Piao(✉), Harita Lolla, and Daniel W. Woods

School of Informatics, University of Edinburgh, Edinburgh, UK
{lawrencepiao,s2523563,daniel.woods}@ed.ac.uk

Abstract. To explore the legal uncertainties related to cybersecurity and the role of informal legal advice in online forums, we analyzed user discussions about the legality of vulnerability research. We collected a dataset of 73 queries and 228 responses from Reddit. Our analysis revealed two broad types of legal concerns: proactive, addressing hypothetical vulnerability research in the future; and reactive, involving actions that have already taken place. Both types of concerns were associated with negative emotions, such as confusion, fear, and regret, especially in reactive cases. We also found that, in response, users provided advice ranging from warnings about legal consequences and the possibility of prosecution to mitigation strategies like consulting a lawyer, participating in bug bounty programs, and using practice environments. Despite the informal nature of these discussions, the community appears to play a positive role in offering advice, especially for novices.

Keywords: Cybersecurity law · Bug hunting · Content analysis · Vulnerability disclosure · Security and privacy discourse

1 Introduction

In 1986, the US introduced the Computer Fraud and Abuse Act (CFAA), a broad computer-related law designed to ensure that authorities could prosecute emerging cybercrimes as technology evolved [16]. While this future-proofing approach offered flexibility for law enforcement, it created legal ambiguity regarding legitimate activities, such as bug bounty hunting and responsible vulnerability research [2,4]. Anderson *et al.* [5] highlighted that public perceptions of cybercrime severity often diverge from the sentencing factors used in the CFAA. Similarly, our work finds that vulnerability researchers, particularly amateur hackers and beginners, still face uncertainty and emotional stress four decades on.

Our study focuses on exploring how users discuss these legal risks in a naturalistic setting that captures real-world uncertainties and advice. Additionally, we examine how these discussions reflect broader concerns within the online forum. We focus on two research questions:

- **RQ1:** What legal uncertainties do users face in vulnerability research?
- **RQ2:** What advice do users provide on the legality of vulnerability research?

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

2 Background

The CFAA criminalizes unauthorized access to computer systems, and also allows for civil actions [2,14]. The language used in this law is ambiguous, particularly when it comes to defining terms such as "access" and "authorization" [12]. This has led to criticisms that the CFAA has potentially criminalized benign computer interactions [11]. Despite the Department of Justice committing to not prosecuting good faith research, how to define a hacker's intent remains vague and open to subjective interpretation [9,15]. This leads to a situation where the relevant provisions are not always aligned with the positive aspects of finding and fixing vulnerabilities, which exposes researchers to both criminal and civil liability risks, creating a chilling effect that could stifle security research [3,16].

One route to authorization is through bug bounty programs, which can reduce the risk of legal consequences for ethical hackers and researchers [1]. However, some companies deliberately use obscure language in their vulnerability disclosure policies, giving them the discretion to initiate lawsuits arbitrarily [4]. This becomes even more uncertain across multiple jurisdictions [8,10]. For instance, under the UK's Computer Misuse Act (CMA), merely owning any hacking tools could be considered a crime [6,17]. This has raised concerns that even with safe harbor permission for responsible vulnerability disclosure, hacking may still be illegal [7,16]. All of the above demonstrates that, especially for beginners, hackers still face challenges when understanding and dealing with related laws.

3 Methodology

Data Collection. We collect data from Reddit, which is a common data source for understanding how users discuss security and privacy [10,13]. This study was approved by our Research Ethics Committee and we ensured that no personally identifiable information was collected or stored. Using Reddit's API, we gathered 73 questions and 228 comments from cybersecurity-related subreddits across two iterations. We collected data from 13 different subreddits, with the majority in `r/legaladvice` and `r/AskNetSec` (see Figure 2 in Appendix B).

Thematic Analysis. We first built a codebook around the research questions by iteratively adding and merging terms. A researcher then broke the text into analytic units that captured distinct meanings related to the themes. Two researchers independently coded 175 units and calculated the Cohen's Kappa ($k = 0.83$), indicating a high level of agreement. One researcher then coded the remaining data. The codebook can be found in Appendix A.

Limitations. The Reddit API is convenient for real-time data scraping but has limitations in retrieving consistent historical data, managing large datasets, and handling rate limits efficiently. Although our study reached thematic saturation during coding, we did not analyze all relevant user discussion. For example, we only analyzed posts in English, and we did not analyze questions and discussion found in the comments of posts that are not about legal issues. This suggests our study surfaced the main qualitative themes, although the quantitative prevalence of themes is influenced by various biases.

4 Results

4.1 RQ1: Questions about Vulnerability Research Legality

We identified that the majority of questions are posted by students (41%) and amateurs (37%). For example, a user notes "*I am a complete novice*" apart from a "*pentesting class I took last semester*". Such users express motivation to acquire hacking skills without triggering legal issues. There was also questions from contractors and professional penetration testers (10%), as well as questions where this information was not provided. Most questions can be divided into proactive and reactive types:

Proactive Questions concern the legality of hypothetical future actions (42%). Users seek to clarify the legal boundaries, with less focus on specific behaviors or detailed scenarios. For example:

> Q17: "*I was wondering how people test for exploits to simply help people keep their systems more secure without any legal ramifications*"

Some proactive questions are framed more in terms of ethics than legality (10%), like "*Is it ethical to try if these passwords work on email accounts?*", which indicates that ethical correctness is sometimes regarded as a factor influencing the justification of hacking activities.

Reactive Questions pertain to historic activities, where the questioner has already engaged in or attempted some form of vulnerability research (44%). We altered some direct quotes from reactive queries to protect user privacy. These questions tend to focus on minimizing legal risks after the fact:

> Q47: "*I did not even realize what I did until last minute and stopped the scan... I'm terrified and have no idea what to do*"

We also found that both types of questions are accompanied by negative emotions, especially reactive ones, which often involve confusion, fear, or regret, due to concerns about the uncertainty of legal consequences:

> Q4: "*I am scared that by making the report they will see that I exploited the bug too much and put them in danger or something like that...*"

21% of questions mentioned users' location and jurisdiction, with the majority being from the U.S. Moreover, 16% of the questioners mentioned bug bounty programs, but most of them stated that they had already checked that the target assets or vendors had no relevant bug bounty programs in place.

Additionally, the questions related to geopolitics (9%) include inquiries about hacking activities within the context of hostility or war, and questions about the legality of attacking websites engaged in illegal activities or on the "dark web".

> Q28: "*I'm wondering if it is legal to perform a hack on a illegal website...*"
> Q62: "*Let's say I found some vulnerabilities to harm the Russian government. What are the legalities in acting on them in the US*"

These discussions sparked extended ethical debates, with users invoking: "*. . . taking down illegal websites would make me the batman of hacking?*" and "*If you kill a killer, the number of killers in the world remains the same*".

4.2 RQ2: Advice on Vulnerability Research Legality

We identified three main types of advice: legal, prosecution, and mitigation, as shown in Figure 1, which respectively focus on the legality of actions, the likelihood and conditions of facing prosecution, and solutions to reduce risks or act responsibly.

Legal Advice. A large portion of legal advice appears in the form of warnings (61%), where respondents emphasize that the original post (OP)'s actions could lead to adverse legal consequences, warning the OP to be cautious, though no evidence or explanation is provided, such as "*NO! And please don't even try. . .*". When it comes to advice on whether specific actions are legal, the advice tends to be conservative, i.e., the actions violate the law (21%).

> "*The rule of thumb is generally if you are trying to compromise something offered by a service provider it is almost always illegal*"

Additionally, many users express uncertainty (10%), stating that the situation falls into a grey zone where the laws are ambiguous, for instance: "*Be careful, or stop doing what you're doing. . . you're in a very grey area*".

Prosecution. Reactive questions are always accompanied by concerns about the severity of the consequences. In the responses to these questions, the possibility of being prosecuted is frequently discussed. 51% of the related responses mentioned that whether someone gets prosecuted depends on whether their actions caused any damage or the jurisdiction in which it occurred, such as "*. . . depending on where you are located the laws vary as does the liklihood you will be pursued and prosecuted*". Some users opined that simple bug finding may only result in a warning email because formal prosecution incurs significant costs. For example, one user said:

> "*They'd have to either sue you in Georgia. . . and try to get a Canadian court. . . That's a lot of work for not much payoff*"

Mitigation. For proactive questions, 40% of the responses recommend participating in bug bounty programs, such as "*If you legally want to do things like this you should look into bug bounty programs*". Moreover, users suggest practicing on dedicated testing environments or virtual machines.

> "*If you want to practice this stuff in a safe environment. . . Play in a VM*"

Other advice also encourages users to seek prior approval or authorization, such as "*White Hat Hackers only hack with written permission*". These before-the-fact recommendations for proactive queries provided safe and legal ways to practice and apply hacking skills.

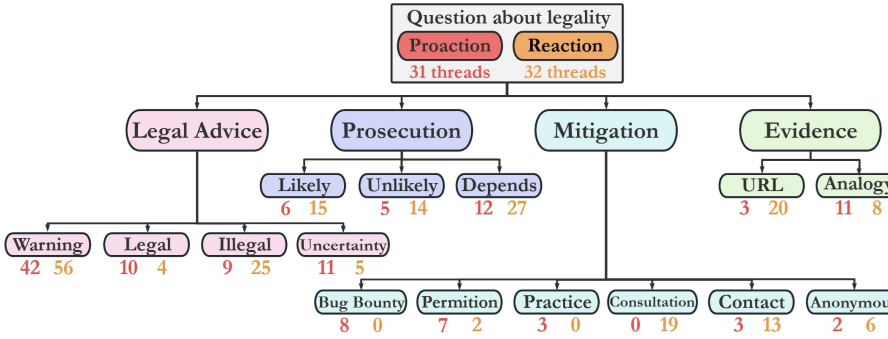

Fig. 1. The types of questions and advice. Red and orange numbers show the occurrence of advice for proactive and reactive questions, respectively.

For reactive questions, users always offered numerous mitigation strategies intended to reduce or eliminate risk factors. The most common suggestion is to consult a lawyer specializing in cybersecurity law (44%). The next most common advice is to contact official disclosure channels, such as computer emergency response team (CERT) or the target vendor's email. Another common suggestion is anonymous disclosure, which is usually recommended if no response is received after contacting official channels. Examples of each can be seen in the following:

"*My advice is to email another security contact at Microsoft*"
"*If you've gotta do something, find some way to anonymously report it*"
"*. . . but I think you would be better off talking to a lawyer*"

Supporting Evidence. As supplementary support, 10% of the advice provided corroboration for their viewpoints, primarily by sharing URLs, that link to: 1) law documents; 2) news or reports of similar cases; and 3) explanatory or defense videos. Moreover, 8% of the suggestions contained analogies to aid in understanding and explanation, such as "*. . . driving around with a garage door opener, seeing if there's a door that might actually open*".

5 Conclusion

Our research identifies the main forms of questions and advice related to the legality of vulnerability research on Reddit. We found that many users expressed confusion and fear regarding the legality of their actions. This demonstrates the influence that broad computer security laws and uncertain enforcement could have on legitimate activity. Deterring experimentation, particularly among beginners, may have unseen consequences on the cybersecurity skills pipeline, as would-be security practitioners are discouraged at the first step.

Despite the initial uncertainty, many users offer valuable mitigation strategies. One positive aspect of these discussions is the frequent recommendation of

responsible approaches to hacking, such as participating in bug bounty programs and practicing hacking techniques in controlled environments. This demonstrates a proactive effort by the community to guide less experienced researchers toward safer environments with less legal risk. Future work should explore how cybersecurity law professionals handle consultations and advice requests. This could help identify the gap between informal advice found on forums and expert legal counsel, ultimately contributing to the development of clearer guidelines for bounty hunters and researchers.

References

1. C. P. Beretas. "Analysis of White and Black Hat Hacker Roles, Practices and Techniques, Considering Ethical and Legal Issues, Including Bug Bounty Programs". *SunText Review of Economics & Business*, **4**:1–13, 2023. https://doi.org/10.51737/2766-4775.2023.095.
2. S. A. Constant. "The Computer Fraud and Abuse Act: A prosecutor's dream and a hacker's worst nightmare—The case against Aaron Swartz and the need to reform the CFAA". *Tulane Journal of Technology and Intellectual Property*, **16**:231, 2013. URL https://journals.tulane.edu/TIP/article/view/2622.
3. O. van Daalen. "In defense of offense: Information security research under the right to science". *Computer Law & Security Review*, **46**:105706, 2022. https://doi.org/10.1016/j.clsr.2022.105706.
4. A. Gamero-Garrido, S. Savage, K. Levchenko *et al.* "Quantifying the pressure of legal risks on third-party vulnerability research". In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1501–1513. Springer, Heidelberg, 2017. https://doi.org/10.1145/3133956.3134047.
5. J. T. Graves, A. Acquisti and R. Anderson. "Perception versus punishment in cybercrime". *The Journal of Criminal Law and Criminology*, **109**(2):313–364, 2019. URL https://scholarlycommons.law.northwestern.edu/jclc/vol109/iss2/4/.
6. A. Guinchard. "The Computer Misuse Act 1990 to support vulnerability research? Proposal for a defence for hacking as a strategy in the fight against cybercrime". *Journal of Information Rights, Policy and Practice*, **2**(2), 2017. https://doi.org/10.21039/irpandp.v2i2.36.
7. HackerOne. "Review of the Computer Misuse Act 1990: Consultation and response to call for information", 2023. URL https://www.hackerone.com/sites/default/files/2023-04/[SubmissionCopy]HackerOne-CMA-OpenConsultationLetter.pdf.
8. F. Hantke, S. Roth, R. Mrowczynski *et al.* "Where are the red lines? Towards ethical server-side scans in security and privacy research". In *IEEE Symposium on Security and Privacy (SP)*, pages 1–13. IEEE, Los Alamitos, CA, 2024. https://doi.org/10.1109/SP54263.2024.00104.
9. S. Hourican. "CFAA and Van Buren: A half-measure for a whole-ly ineffective statute". *Seton Hall Legislative Journal*, **47**(3):30–54, 2023. URL https://scholarship.shu.edu/shlj/vol47/iss3/2.
10. T. Hrle, M. Milad, J. Li *et al.* "'Just a tool, until you stab someone with it": Exploring Reddit users' questions and advice on the legality of port scans". In *European Workshop on Usable Security (EuroUSEC)*. Karlstad, Sweden, 2024. https://doi.org/10.1145/3688459.3688469.

11. O. S. Kerr. "Vagueness challenges to the Computer Fraud and Abuse Act". *Minnesota Law Review*, **94**, 2009. URL https://scholarship.law.umn.edu/mlr/508.
12. O. S. Kerr. "Focusing the CFAA in Van Buren". *The Supreme Court Review*, **2021**:155–184, 2022. https://doi.org/10.1086/720376.
13. J. Li, K. Sun, B. S. Huff *et al.* "'It's up to the Consumer to be Smart": Understanding the security and privacy attitudes of smart home users on Reddit". In *IEEE Symposium on Security and Privacy (SP)*, pages 2850–2866. IEEE, Heidelberg, 2023. https://doi.org/10.1109/sp46215.2023.10179344.
14. S. Park and K. Albert. "A researcher's guide to some legal risks of security research", 2020. URL https://clinic.cyber.harvard.edu/wp-content/uploads/2020/10/Security_Researchers_Guide-2.pdf.
15. W. Thomas. *Supporting data-driven software development life-cycles with bug bounty programmes.* Ph.D. thesis, University of Oxford, 2023. URL https://ora.ox.ac.uk/objects/uuid:4a828bbb-8ff4-4cac-9e09-5699b30c6d52.
16. Q. H. Wang, R. Geng and S. H. Kim. "Chilling effect of the enforcement of Computer Misuse Act: Evidence from publicly accessible hack forums". *Information Systems Research*, **35**(3):1195–1215, 2024. https://doi.org/10.1287/isre.2019.0346.
17. K. Wilson. *Computer (mis)use and the law: What's wrong with the CMA?* Ph.D. thesis, University of Oxford, 2019. URL https://ora.ox.ac.uk/objects/uuid:f44d4182-a52f-4842-aee0-28faa8b2acc8.

Appendix A Codebook

- **Questions** - Questions or concerns posed by the user in the original post.
  - **Actor** - Who are questioners or participants in vulnerability research?
    - **Educational** - Students affiliated with an educational institution.
    - **Hobbyist** - Newcomers who are interested in hacking or security.
    - **Professional Pentester** - Penetration tester employed by firms.
    - **Contractor** - Experienced hackers hired for specific periods or projects.
  - **Motives** - Why do actors conduct vulnerability research?
    - **For-Profit** - Financial rewards, recognition and brand building.
    - **Non-Profit** - Hacking to improve security infrastructure.
    - **Accidental** - Unintentionally finding a bug in unrelated tasks.
    - **Learning** - Practice to improve skills or acquire knowledge.
    - **Geopolitics** - Hacking in the context of war or diplomatic tensions.
  - **Timing** - When actions or inquiries are addressed?
    - **Reactive** - Issues related to actions that have already taken place.
    - **Proactive** - Questions about future actions before they occur.
  - **Legal Framework** - Ties the technical and moral aspects with legalities.
    - **Offensive Security** - Legality of good-faith intrusion.
    - **Bug Bounty** - Issues about the bug bounty programs.
    - **Information Gathering** - Concerns related to web scraping.
    - **Ethics** - Worries related to moral conduct and social responsibility.
    - **Disclosure** - Issues about responsible or public disclosure of bugs.
    - **Policy Violation** - Concerns about breaches of terms or regulations.
  - **Jurisdiction** - Actor's region of operation.

    - **USA** - Actors or targets are located in USA or involve its regulations.
    - **EU** - Actors or targets are located in EU or involve its regulations.
    - **UK** - Actors or targets are located in UK or involve its regulations.
    - **Others** - Other countries or regions.
- **Technology** - Legitimacy of tools, techniques, and functional attributes.
- **Emotion** - The sentiment displayed by the user during questioning.

- **Responses** - Advice and suggestions given by users in threads.
  - **Legal Support** - Suggestions related to legality or regulation.
    - **Legal Advice** - Distinguishing between legal and illegal activities.
      - **Warning** - Warnings about possible legal risks or consequences.
      - **Ambiguity** - It is a grey area and the regulations are ambiguous.
      - **Legality** - Suggestions where users say something is legal.
      - **Illegality** - Suggestions where users say something is illegal.
    - **Mitigation** - Suggestions that intend to reduce or eliminate the risk.
      - **Anonymity** - Hiding identify during hacking and disclosure.
      - **Official Contact Channel** - How to communicate or report?
      - **Prior Approval** - Getting approval from the authorities.
      - **Policy Compliance** - Complying with policies laid by vendors.
      - **Consult Lawyer** - Talking to cyber law attorneys.
      - **Bug Bounty Programs** - Reporting via official disclosure.
    - **Prosecution** -Advice that discusses the legal proceedings.
  - **Non-Legal Support** - Suggestions other than the above.
    - **General** - Anything off-topic or irrelevant.
    - **Insufficient Information** - Anything that are difficult to interpret.
    - **Miscellaneous** - Anything not related to the research question.

Appendix B Data Distribution

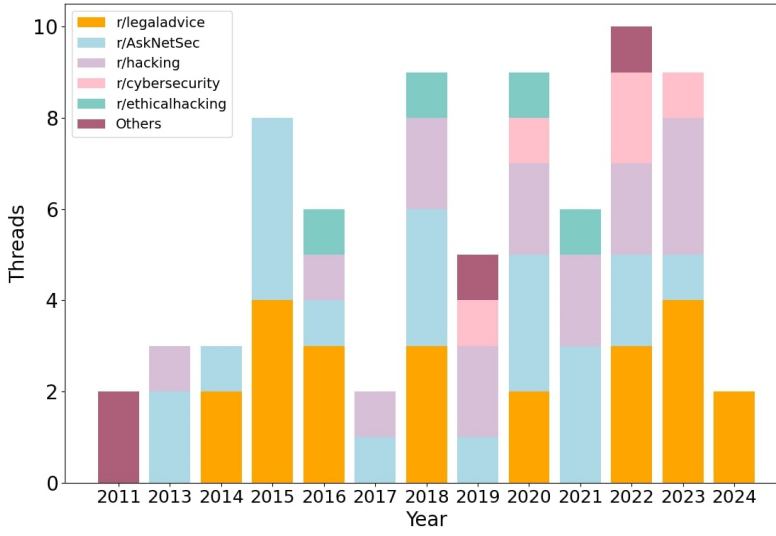

Fig. 2. Data distribution of Reddit threads.

The posts were made between 2011 and April 2024, with approximately 50% of the queries recorded after 2020.

Technologists Setting De-facto Policy

Marie Vasek and Kyle Beadle

University College London
{m.vasek,kyle.beadle.22}@ucl.ac.uk

Abstract. Policy is slow to adapt to the increasingly rapid pace of technology and social norms. We investigate two case studies here: gender and cryptocurrency. We show how technologists have updated their systems reflecting social norms not yet embedded in policy. This has implications for uniformity as well as future governance of said systems.

1 Introduction

Ross Anderson advocated vociferously in his lifetime for "sensible regulation" which kept pace with technological innovation. In his textbook, *Security Engineering*, Ross considered early megacorporations like IBM and Microsoft who set the standards for computing in these days which were then reflected in policy [3]. Ross was similarly critical towards self-governance mechanisms [1] and generally considered the psychological acceptability of mechanisms by technologists [3].

We consider other recent cases where technologists set de-facto policy. We outline the trade-offs here. On one hand, we do not want to wait for governments to bicker in order for technology to evolve, particularly to reflect evolutions in society. On the other, technologists rolling out new changes are often doing so based on their own (often American) lens and then outsourcing those norms to other countries.

We see this in the current roll out of AI. Technologists are making what they see as "purely technical" or "logical" choices. However, technology is inherently political. Choices to surveil social media to "train models" or embed technology in politically charged areas like warfare necessarily are political choices. The *rightness* or *wrongness* of these choices is not the point – rather, the fact that technologists are making these policy choices which act like de-facto policy. In turn, when governments write regulation to consider the effects of this technology on the world, it might be impossible to overturn decisions made in the making of the technological space. The governmental policy builds upon the choices made by the initial technologists.

Less studied are the effects of technologists on gender recognition and cryptocurrency exchange regulation. Technologists in social networks rolled out gender options other than male or female starting with Facebook in 2014 while only 2 countries in the world recognised more than 2 genders. While this decision reflected cultural change, it likely helped accelerate the roll out of nonbinary genders to more countries worldwide by providing visibility in a similar manner to how the main factors in the acceptance of gay people was visibility of

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

gay friends and family [9]. Cryptocurrency exchanges have been patchily regulated since their start in 2010 with Bit Market. Despite facilitating money transfers, most serious cryptocurrency regulatory efforts started after the collapse of Mt Gox in 2014.

Policy scholars consider **platform governance** which navigates how corporations are acting more like nation states and make decisions amongst themselves considering their users, third parties (like ad platforms), and governments [8]. Our work extends theirs, considering how the early adopting individual technologist exerts disproportionate power over the eventual policy in two case studies.

2 Gender Recognition

Until 2003, countries only officially recognised two genders: male and female. However, a spectrum of genders has been recognised in various forms before then from the Incan Qariwarmi to the Inuit 'third gender'. We draw a distinction between a person's legal gender as recognised by their government of residence and their gender as recognised by the person themself. Legal gender matters to different degrees in different places: e.g., in the UK a person can use a bathroom of their gender, but legal gender is on their taxes each year. Iceland is rolling out regulations requiring access to gender neutral toilets after implementing a legal third gender option in 2021. In the US, legal gender is implemented state by state; 22 states and Washington DC recognise a legal non-binary gender (X).

Back in 2014, Facebook introduced 58 gender options augmented by a custom option if those options weren't sufficient to represent a users' gender [7]. This was considered radical at the time. In 2014, the only countries that recognised genders other than male or female was Germany and Australia who allowed an "indeterminate" gender. In the US, Oregon was the first state to recognize nonbinary genders in 2016. The first US nonbinary passport was granted in 2021.

Bivens outlines how, despite allowing a diversity of gendered options, these all boil down to three essential genders (male, female, and undefined) which allows them to satisfy their advertisers need for genders that fit into their existing models [4]. She shows how choices determined on, e.g., pronouns or gender before a custom option was chosen, determines the gender shown in their API. This demonstrates the inherent tension in adopting new technological features in existing platforms by adopting them to the old, existing technological framework. Platforms are complex and rely on ad money for monetisation. This adaptation also shows how cheap it can be to add new features to allow a broader spectrum of genders for their users. We argue that the gender displayed to others amongst the platform is more impactful than that shown to advertisers. By allowing gender to be updated this way shows that there is not a legitimate business case to not make these changes.

While Facebook's decision was lauded for its inclusivity [7], along with revoking its real name policy [10], gender options have real-world privacy implications. Facebook's popularity means that gender options are available in markets where it is dangerous to be non-binary – and even more dangerous to be open about

it. Notably, the feature enables surveillance of a user's gender identity. The feature's all-in nature (you are either one gender or another) flattens a user's gender transition journey and unnecessarily requires a user to explain themselves to discriminating family members [6]. The gender option feature may also lead to surveillance among queer individuals as they adapt their identity to be more acceptable among their online, queer friends [14]. Meanwhile, Facebook has since translated these options for countries across the world where state actors are actively imprisoning and killing LGBTQ+ people [15].

While some platforms (often aimed at young people) offer wide spectrums of gender to chose from, other platforms, particularly governmental ones have been slow to adopt, even after new gender options are legalised. Spiel conducts an auto-ethnography on their experience navigating registering their gender for various platforms in Germany [13]. Despite Germany recognising nonbinary genders for a decade prior to Spiel's journey, they received a lot of resistance. Particularly relevant to this paper, they received a lot of "computer says no"-type of resistance. Spiel sometimes resorts to using GDPR to force organisations to reflect their gender in their system via GDPR's ability to request accurate information be reflected by others' systems.

It is often unclear how to adapt gender to a system serving a wide variety of people and interpret gender to many. There have been a wide spectrum of implementations over the years. These fall into three broad camps: forcing all users into male or female, a short number of options including male and female, or a write-in option. Some systems integrate trans status and gender. There's broad guidance given to technologists, but even under complaints, without any government mandate, changes are rare. It can also commingle users who identify as neither male nor female with users who prefer not to state for other reasons. These are frequently made with the best of intentions. However, the mishmash of gendered options throughout platforms indicates the need for more streamlined governance. Collier and Cowan, though, warn against overly reductive categories towards general case norms which don't fit the narrow context in which the question is needed [5].

3 Cryptocurrencies

Satoshi Nakamoto created Bitcoin as an alternative to the government-backed monetary system. Since then, the industry has tried to self govern. This historically looked like individual operators making decisions about payments on their platforms without any external oversight. However, by 2013, 45% of cryptocurrency exchanges failed [12]. These frequent failures indicates the lack of adherence to a suitable security practice within exchanges.

Despite this, the industry has repeatedly pushed back against governmental regulation to protect users, crying out against surveillance. Cryptocurrency exchanges have tried all sorts of tricks to evade regulators, from declaring themself to be a "decentralised company" not based in any country, to moving their opera-

tions out of countries that discuss regulation, to simply not filing any paperwork to require governments to actively come after them.

We consider technologists decisions in the early days of cryptocurrencies, particularly Bitcoin, and their effects on the potential governance issues now. Satoshi and other early technologists in the space made a lot of microdecisions when designing Bitcoin and the surrounding ecosystem, some of which eventually caused problems.

Nakamoto consensus works when consistently mining on only one machine. It makes a lot of sense given the sheer amount of time that only Satoshi or a group smaller than four were mining. However, the ecological resources required for this proof-of-work based consensus mechanism has proved to be likely way higher than expected.

Mt Gox secured their users' bitcoin by putting them on a small number of omnibus accounts. These were then subsequently compromised and stolen. The industry learned a partial story here – particularly, to encrypt wallets so even if they are stolen, the money cannot be recovered by a random third party. However, this is not the sole fatal flaw. The use of omnibus accounts or intermingling customer funds, might decrease complexity, but it also makes a single target more attractive to attackers and reduces transparency which could increase the likelihood of insolvency. Many exchanges today still use this method to store their users' funds.

Satoshi considered privacy in the creation of Bitcoin. While the whitepaper warns people to use a new key pair for each transaction, this behaviour was not required or encouraged in code. This decision to allow users to reuse addresses despite being aware of the risks, has deanonymised thousands of users [11].

In April 2013, there were 7 coins trading for nonzero amounts of money, according to CoinMarketCap. It took a considerable amount of energy in this time period to launch an altcoin. Even DogeCoin, the copy of Litecoin with a delightful meme attached for attractive marketing, required days of programming in order to launch this effort in December 2013. But, there was a major shift in January 2014 when the service coingen was launched. This service allowed anybody to pay a small amount of money to create a new altcoin codebase of their own with personalised parameters. From this point forward, the code homogeneity in new projects increased substantially. While this project shut down afterwards, the effects have lingered in the vast array of copied codebases littered throughout the listings of altcoins. While consumers might expect that a new currency might need an interesting amount of original content and might trust a coin just for the engineering work needed to launch a coin, technologies like coingen break this trust model. Afterwards, the industry has not built adequate resources to display to consumers whether a project contains any new innovation or is just an empty copy of existing work with a few changed constants.

4 Discussion and Conclusion

Technologists are not a great representation of broader culture. In the US, technologists skew towards wealthier white and asian men between the ages of 20 and 50. These are groups with divergent beliefs and norms from the wider world. Allowing this group of people to set de-facto policy without being beholden to a broader group has consequences for how technology grows.

Currently, while there is a wide scale uncertainty about the representation of gender in systems, this uncertainty is reflected in the uneven presentation of gender in computer systems. To some degree there's a tradeoff – it can be hard to adapt older users to new norms around gender and allowing users to type in arbitrary text can be confusing to those users. Options on a drop down menu can be confusing and if transgender status is comingled, this can potentially out a user unnecessarily if the trans status information is not needed for the system. Recommendations from activists can be seen as unreasonable to update systems around. However, as we saw with Facebook, it can be possible to implement new genders for users to display within the extremely binary gendered advertising framework. Hopefully, as the world settles around a consistent way of recognising people existing outside the gender binary, systems will be updated in turn.

In the world of cryptocurrencies, we have seen how small engineering decisions have caused major changes impacting the potential governance of the ecosystem. We currently need to be considering the implementation of technology around new regulation to ensure compliance with not only the letter of law, but also the spirit. There similarly needs to be surveillance by adequately trained technologists in order to ensure compliance. While regulation will change with the rapid pace of technology, there's a need to ensure the technology component works now in order to set the stage for future compliance.

Ross Anderson publicly bemoaned the cryptocurrency industry. His paper Bitcoin Redux [2] outlined what a threat he thought it was, from the ecological implications to off-chain transactions turning cryptocurrency exchanges into a "shadow banking system". *"In the absence of effective regulation, the cryptocurrency bubble is somewhat like a teenage party that's got a bit rowdy, and it's time for the grown-ups to take the punch bowl away."* Our work agrees with the broader sentiment and explains how the harms he outlined (and others) occur through the decisions of only a few technologists setting de-facto policy.

References

1. Ross Anderson and Tyler Moore. "Information security economics – and beyond". In *Annual international cryptology conference*, pages 68–91. Springer, 2007.
2. Ross Anderson, Ilia Shumailov, Mansoor Ahmed and Alessandro Rietmann. "Bitcoin redux". In *The 17th Annual Workshop on the Economics of Information Security (WEIS 2018)*. 2018.
3. Ross J Anderson. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.

4. Rena Bivens. "The gender binary will not be deprogrammed: Ten years of coding gender on Facebook". *New Media & Society*, **19**(6):880–898, 2017.
5. Ben Collier and Sharon Cowan. "Queer conflicts, concept capture and category co-option: The importance of context in the state collection and recording of sex/gender data". *Social & Legal Studies*, **31**(5):746–772, 2022.
6. Stefanie Duguay. "'He has a way gayer Facebook than I do": Investigating sexual identity disclosure and context collapse on a social networking site". *New media & society*, **18**(6):891–907, 2016.
7. Kashmira Gander. "Facebook's new gender options: 50 new categories include trans and intersex". URL `https://www.independent.co.uk/tech/facebook-adds-new-gender-options-50-new-categories-include-trans-and-intersex-9127209.html`.
8. Robert Gorwa. "What is platform governance?" *Information, communication & society*, **22**(6):854–871, 2019.
9. Gregory M Herek. "Anti-equality marriage amendments and sexual stigma". *Journal of Social issues*, **67**(2):413–426, 2011.
10. Amanda Holpuch. "Facebook adjusts controversial 'real name' policy in wake of criticism". URL `https://www.theguardian.com/us-news/2015/dec/15/facebook-change-controversial-real-name-policy`.
11. Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker and Stefan Savage. "A fistful of bitcoins: characterizing payments among men with no names". In *Proceedings of the 2013 Internet Measurement Conference*, pages 127–140. 2013.
12. Tyler Moore and Nicolas Christin. "Beware the middleman: Empirical analysis of Bitcoin-exchange risk". In *Financial Cryptography and Data Security*, pages 25–33. Springer, 2013.
13. Katta Spiel. "'Why are they all obsessed with Gender?" – (Non)binary Navigations through Technological Infrastructures". In *Proceedings of the 2021 ACM Designing Interactive Systems Conference*, pages 478–494. 2021.
14. Ashley Marie Walker and Michael A DeVito. "'' 'More gay' fits in better": Intracommunity Power Dynamics and Harms in Online LGBTQ+ Spaces". In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–15. 2020.
15. Rasha Younes. "'All This Terror Because of a Photo": Digital Targeting and Its Offline Consequences for LGBT People in the Middle East and North Africa". Human Rights Watch. URL `https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt`.

~~Security-by-design~~ Securing a compromised system

Awais Rashid[1][0000-0002-0109-1341],
Sana Belguith[1][0000-0003-0069-8552],
Matthew Bradbury[2][0000-0003-4661-000X],
Sadie Creese[3][0000-0002-2414-9657],
Ivan Flechais[3][0000-0002-3620-0843], and
Neeraj Suri[2][0000-0003-1688-1167]

[1] University of Bristol, UK
[2] Lancaster University, UK
[3] University of Oxford, UK

Abstract. Digital infrastructures are seeing convergence and connectivity at unprecedented scale. This is true for both current critical national infrastructures and emerging future systems that are highly cyber-physical in nature with complex intersections between humans and technologies, e.g., smart cities, intelligent transportation, high-value manufacturing and Industry 4.0. Diverse legacy and non-legacy software systems underpinned by heterogeneous hardware compose on-the-fly to deliver services to millions of users with varying requirements and unpredictable actions. This complexity is compounded by intricate and complicated supply-chains with many digital assets and services outsourced to third parties. The reality is that, at any particular point in time, there will be untrusted, partially-trusted or compromised elements across the infrastructure. Given this reality, and the societal scale of digital infrastructures, delivering secure and resilient operations is a major challenge. We argue that this requires us to move beyond the paradigm of security-by-design and embrace the challenge of *securing-a-compromised-system*.

Keywords: Security · Convergence · Cyber physical systems

1 Introduction

The security of infrastructures, architectures, and mechanisms is built on assumptions. This includes speculations or approximations about context, usage, threat models or interactions with other systems. Even when correct, these assumptions may only hold at a particular point in time and are often shaped by additional assumptions about the system's lifespan and that the designed security approaches will mitigate against vulnerabilities over that lifespan. These assumptions do not survive contact with the reality of deployed systems.

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

In practice, a system involves a range of other sub-systems several of which are not in the purview of the developers or the organisation deploying the system—in many instances assets and services are outsourced to third parties with security breaches having major knock-on effects on a wide array of systems and users [6]. Even where these sub-systems are within the development or administrative control of the system owner, there are complex technology stacks with a plethora of third party libraries, hardware, software components and diverse development practices – including often misplaced assumptions about threat models [7,20]. Furthermore, threat actors evolve quickly in terms of their capabilities, motivations and tactics, techniques and procedures, for example using generative AI techniques to create malware [13]. Systems, particularly large-scale ones that underpin societal scale infrastructures, e.g., water, power, digital services for citizens, do not evolve as rapidly. It takes time and money to change a system and, where such change is enacted, for example, for a power system or railway infrastructures, it is a major investment of hundreds of millions or billions of pounds involving rearchitecting the system, upgrading hardware and software systems, testing for safety and uptime, and retraining of staff. In some cases, it is even not possible to upgrade legacy systems to state-of-the-art security mechanisms due to real-time requirements or the need to formally prove safety and dependability related properties.

Furthermore, digital infrastructures have complex interdependencies and intersections with human users who are an integral part of the work and information flows. Often, human interactions with the systems catalyse dynamic composition of services which create new interactions and dependencies across systems at runtime. Usability of security mechanisms is paramount [23] not only to ensure that security does not create significant overheads but also to mitigate against shadow security practices [18] by users. Security mechanisms typically aim to address specific threats or vulnerabilities. For example, the Digital Security by Design (DSbD) programme is making key advances to eliminate memory vulnerabilities at the hardware-level [9]. While this holds great promise, there remain risks of developer-induced vulnerabilities [28] or constraining assumptions as to who the threat actor is, e.g., one aiming to extract data from RAM after super cooling it [29].

The reality is that it is *impossible* to secure all aspects of a system by design. Measuring security – and its *goodness* – is an open problem and polling *goodness* of a system cannot perfectly determine if the system's behaviour is good. The best one can do is probabilistic [4]. The reality is that systems will become compromised or will always have untrusted, partially trusted, or compromised elements. Pragmatic considerations mean also that one cannot simply shutdown a whole transportation infrastructure because, say, a traffic signal is compromised, or disconnect large parts of the power grid because specific components are under attack. How we ensure that the system continues to operate within specified bounds of safety and resilience – albeit potentially at reduced capacity – is critical, as is the capability to limit impacts of partial breaches including cascading effects across interconnected infrastructures. *We, therefore, posit that*

research needs to move beyond the paradigm of security-by-design and embrace the challenge of securing-a-compromised-system. This requires scientific advances in four key dimensions. We discuss these next to present a research agenda for the research community.

2 Research Challenges

2.1 Predictability

Predictability is an inherent goal in security: knowing what can and will happen, what can be done to mitigate it and the extent to which any mitigation is effective. Predictability requires *measuring security* which is a hard problem in any system. It is compounded in digital infrastructures as complexity is paramount: mix of technology (legacy and non-legacy), uncertainty about threats and effectiveness of controls, emergent behaviour, interactions between security and other system goals, trustworthiness of people and organisations and divergence from rules (shadow practices).

A large body of work has focused on developing metrics. Reference sources such as NIST 800-55 [5] and ISO 27004 [15] adopt a catalogue approach: reference metrics classified into categories and documented with scenarios and examples. However, the contextualisation of metrics relies on arbitrary examples and use cases, limiting their expressiveness and hence their ability to address the complexity and inherent uncertainty. Others promote a more structured way of designing security measurements [12,17,11]. However, they presume that one knows a priori what is pertinent to measuring security and that instrumenting all elements is feasible—not the case given the dynamism and opaqueness in contemporary and future digital infrastructures.

Standards such as NIST SP 800-160 Volumes 1 and 2 [21,22] offer guidance on engineering trustworthy secure and resilient systems. However, such standards are based on the premise that the problem, solution and trustworthiness contexts can be established *a priori* and that systems can be architected with a high degree of control over their components. These assumptions do not hold in large-scale infrastructures. There are systems about which one can collect relevant metrics (e.g., a sub-system into which deep instrumentation can be deployed) and for others one can not. Uncertainty also comes from what is unseen, e.g., shadow practice. So modelling the dependencies and deriving relevant metrics to understand the security implications of those dependencies is a major scientific challenge.

2.2 Composition

Composing security provision in any system is a hard problem. For instance, a longstanding principle is that of *secure distributed composition* which states that when multiple sub-systems or components are composed, the resulting system does not weaken the security policies enforced by its components. Security policy enforcement approaches typically take an organisation- or network-centric view of security, e.g., [10,26]. These tend to be either obligation-driven

or authorisation-driven [26]. In the former case, policies are enforced actions in response to particular events or stimuli within a system while, in the latter, they provide access control rules specifying whether a particular subject can legitimately access (or not) a particular object. Such approaches assume that the system, whether distributed or not, is within a single administrative control and even where platform or geographical boundaries are crossed, this happens within the control of a single organisation or a federated security management framework [8]. This is not the case for digital infrastructures under discussion in this paper, which are globally interconnected open-ended networked environments.

The challenge is further compounded by the cyber-physical nature of many constituent systems where legacy hardware and software are abound and security assurances can vary widely—from poorly designed network protocol stacks to access control models that do not enforce privileges at suitable levels. Furthermore, such environments are not static. Devices, systems and services can dynamically (and, increasingly, automatically) compose based on context and locality. Human actors are integral to the dynamics, and often catalyse dynamic composition and delivery of services, e.g., through wearables that bridge multiple systems simultaneously. Consequently, security orchestration can be, at best, delivered through service-level agreements (SLAs). However, violation of such SLAs is often only detected post-hoc. Furthermore, in a large set of scenarios, e.g., those involving untrusted or partially-trusted third party systems, specification, agreement and enforcement of an SLA is impossible.

2.3 Continual Assurance

For well-structured systems (e.g., control systems, database/transactional systems) with clearly specified security requirements on a) interactions and dependencies across sub-systems, services and components, and b) the expected threats, research has developed a variety of sophisticated capabilities to monitor and analyse their security posture to assert (with varying levels of confidence and accuracy) the requisite levels of security assurances [1,14,19]. This is not the case for globally interconnected open-ended networked heterogeneous environments where a complete awareness of all dependencies and knowledge of all operational paths is not viable. This becomes even more challenging in an ultra-large scale environment where conjunctions of secure and unsecure, trusted and untrusted, and reliable and unreliable elements are present.

For instance, for complex and dynamically interconnected systems, the consequent lack of a) complete and stable system and security specifications including the threats, and b) complete and stable dependency and interface specifications, make provisioning of continual assurance a challenge. Such systems are typically heterogeneous couplings of structured, unstructured, synchronous and asynchronous elements and services. This precludes a single system model invariably considered in state-of-the-practice/art approaches [25].

2.4 Incident Response

Over the past 20 years significant progress has been made to mature and develop incident response and recovery capacity, whether delivered by in-house security operations centres (SOCs) or by third party managed service providers. This is supported by automation and tooling, often in the form of Security Information and Event Management (SIEM) systems that provide real-time information to human operators in a SOC. However, selecting the best response and recovery actions remains a largely human task [2]. Orchestrating incident response on an infrastructure-scale requires research into the appropriate balance between human-machine decision-making.

Existing standards such as ISO/IEC 27035-2:2023 [16] offer guidelines on how to plan, prepare and learn lessons from any incidents, both in terms of system defences and the incident response approach. Given the high-level nature of such guidance, operationalisation happens through *playbooks*, acting as recipes on steps and actions to take during incident response. However, playbooks remain very much a manual setup, often taking the format of natural language texts or flow charts—typically in printed format placed in SOCs. Recent works have argued for more systematic model-based representations of playbooks [24], and have highlighted the lack of a) usability studies of playbooks, and b) specificity even for highly rated playbooks for completeness and correctness by experts [27].

In the infrastructures under discussion, each constituent system will have its own playbook unlikely to be formalised into any structured or systematic common model [24]. Orchestrating a globally coordinated incident response on this scale is, therefore, a major research challenge. It is made even more challenging by the dynamism—systems composing with the infrastructure or leaving. Furthermore, constituent systems' playbooks will change in response to incidents over time. So one cannot start from the assumption that the playbooks are convergent or will remain so over time. The complexity is further compounded because contextual information is a challenge in SIEMs as SOC workers are not involved in the design choices, configurations and operation of specific organisational assets from where telemetry is fed into the SOC. Where contextual information is communicated, this happens informally and thus remains tacit and not formally documented [3].

3 In Conclusion

Advancing the paradigm of *securing-a-compromised-system* will require a *systems* approach that addresses the aforementioned four dimensions. We need new ways to elicit, specify, and validate security assurances for service composition in the presence of uncertainty, dynamism, and human behaviour. New mechanisms to compose and orchestrate security provision across diverse and heterogeneous evolving infrastructures with legacy and non-legacy elements will be critical in this regard. Alongside, it is paramount that the research community develops ways to reason about the security state at runtime in order to provide continuity of oversight and trust in the presence of partially trusted, under attack,

vulnerable, or compromised elements. Last, but by no means least, it is essential that we address how we may orchestrate incident response that accounts for heterogeneous incident response practices in constituent systems and provides situational awareness at the necessary pace and resolution for optimal human-machine decision-making.

Acknowledgments. This research is supported by the Engineering and Physical Sciences Research Council grant SCULI: Securing Convergent Ultra-large Scale Infrastructures [EP/Z531315/1].

References

1. Abiodun Ayodeji, Mokhtar Mohamed, Li Li, Antonio Di Buono, Iestyn Pierce and Hafiz Ahmed. "Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors". *Progress in Nuclear Energy*, **161**:104738, 2023. ISSN 0149-1970. https://doi.org/10.1016/j.pnucene.2023.104738.
2. Maria Bada, Sadie Creese, Michael Goldsmith, Chris Mitchell and Elizabeth Phillips. "Computer security incident response teams (CSIRTs): An overview". *The Global Cyber Security Capacity Centre*, 2014.
3. Sandeep N. Bhatt, Pratyusa K. Manadhata and Loai Zomlot. "The Operational Role of Security Information and Event Management Systems". *IEEE Secur. Priv.*, **12**(5):35–41, 2014. https://doi.org/10.1109/MSP.2014.103.
4. Matthew Bradbury, Arshad Jhumka and Tim Watson. "Trust Trackers for Computation Offloading in Edge-Based IoT Networks". In *40th IEEE Conference on Computer Communications, INFOCOM 2021, Vancouver, BC, Canada, May 10-13, 2021*, pages 1–10. IEEE, 2021. https://doi.org/10.1109/INFOCOM42981.2021.9488844.
5. Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown and Will Robinson. "Performance Measurement Guide for Information Security", July 2008. https://doi.org/10.6028/NIST.SP.800-55r1. NIST SP 800-55 Rev. 1.
6. Partha Das Chowdhury, Karen V. Renaud and Awais Rashid. "When Data Breaches Happen, Where Does the Buck Stop ... and Where Should it Stop?" In *Proceedings of New Security Paradigms Workshop (NSPW)*. 2024. https://doi.org/10.1145/3703465.3703474.
7. Partha Das Chowdhury, Maria Sameen, Jenny Blessing, Nicholas Boucher, Joseph Gardiner, Tom Burrows, Ross J. Anderson and Awais Rashid. "Threat Models over Space and Time: A Case Study of E2EE Messaging Applications". *Software: Practice & Experience*, **54**:2316–2335, 2024.
8. Maarten Decat, Bert Lagaisse and Wouter Joosen. "Middleware for efficient and confidentiality-aware federation of access control policies". *Journal of Internet Services and Applications*, **5**(1), 2014. https://doi.org/10.1186/1869-0238-5-1.
9. "Digital Security by Design (DSbD)", 2024. URL https://www.dsbd.tech/. Accessed On: 2024-11-15.
10. Antonis M. Hadjiantonis, M. Charalambides and G. Pavlou. "A Policy-Based Approach for Managing Ubiquitous Networks in Urban Spaces". In *IEEE International Conference on Communications*, pages 2089–2096. 2007. https://doi.org/10.1109/ICC.2007.346.

11. Lance Hayden. *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*. McGraw Hill, 2011.
12. Debra S. Herrmann. *Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI*. CRC Press, 2007.
13. HP Wolf Security. "Threat Insights Report: September 2024", September 2024. URL `https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-september-2024/`. Accessed On: 2024-11-15.
14. Aleksandar Hudic, Paul Smith and Edgar R. Weippl. "Security assurance assessment methodology for hybrid clouds". *Computers & Security*, **70**:723–743, 2017. `https://doi.org/10.1016/j.cose.2017.03.009`.
15. ISO/IEC JTC 1/SC 27. "Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation". Standard, ISO/IEC, 2016. URL `https://www.iso.org/standard/64120.html`. ISO/IEC 27004:2016, Edition 2.
16. ISO/IEC JTC 1/SC 27. "Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response". Standard, ISO/IEC, 2023. URL `https://www.iso.org/standard/78974.html`. ISO/IEC 27035-2:2023.
17. Andrew Jaquith. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley Professional, 1st edition, March 2007. ISBN 9780321349989.
18. Iacovos Kirlappos, Simon E. Parkin and M. Angela Sasse. "'Shadow security" as a tool for the learning organization". *SIGCAS Comput. Soc.*, **45**(1):29–37, 2015. `https://doi.org/10.1145/2738210.2738216`.
19. Tyson Macaulay and Bryan L Singer. *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2011.
20. Awais Rashid. *Developer-Centred Security*. Springer, 2021. `https://doi.org/10.1007/978-3-642-27739-9_1578-1`.
21. Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau and Rosalie Mcquaid. "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach", December 2021. URL `https://doi.org/10.6028/NIST.SP.800-160v2r1`. NIST Special Publication 800-160, Volume 2, Revision 1.
22. Ron Ross, Mark Winstead and Michael McEvilley. "Engineering Trustworthy Secure Systems", November 2022. URL `https://doi.org/10.6028/NIST.SP.800-160v1r1`. NIST Special Publication (SP) NIST SP 800-160v1r1.
23. M. Angela Sasse and Awais Rashid. *The Cyber Security Body of Knowledge v1.1.0, 2021*, chapter Human Factors. University of Bristol, 2021. URL `https://www.cybok.org/`. KA Version 1.0.1.
24. Avi Shaked, Yulia Cherdantseva and Pete Burnap. "Model-Based Incident Response Playbooks". In *ARES 2022: The 17th International Conference on Availability, Reliability and Security, Vienna, Austria, August 23–26, 2022*, pages 26:1–26:7. ACM, 2022. `https://doi.org/10.1145/3538969.3538976`.
25. Ankur Shukla, Basel Katt, Livinus Obiora Nweke, Prosper Kandabongee Yeng and Goitom Kahsay Weldehawaryat. "System security assurance: A systematic literature review". *Computer Science Review*, **45**:100496, August 2022. `https://doi.org/10.1016/j.cosrev.2022.100496`.
26. Morris Sloman. "Policy Driven Management for Distributed Systems". *Journal of Network and Systems Management*, **2**(4):333–360, 1994. `https://doi.org/10.1007/BF02283186`.
27. Rock Stevens, Daniel Votipka, Josiah Dykstra, Fernando Tomlinson, Erin Quartararo, Colin Ahern and Michelle L. Mazurek. "How Ready is Your Ready? Assessing the Usability of Incident Response Playbook Frameworks". In *CHI '22:*

CHI Conference on Human Factors in Computing Systems, New Orleans, LA, USA, 29 April 2022 - 5 May 2022, pages 589:1–589:18. ACM, 2022. https://doi.org/10.1145/3491102.3517559.

28. Sami Ullah and Awais Rashid. "Porting to Morello: An In-depth Study on Compiler Behaviors, CERT Guideline Violations, and Security Implications". In *9th IEEE European Symposium on Security and Privacy, EuroS&P 2024, Vienna, Austria, July 8-12, 2024*, pages 381–397. IEEE, 2024. https://doi.org/10.1109/EuroSP60621.2024.00028.
29. Yuanzhe Wu, Grant Skipper and Ang Cui. "Cryo-Mechanical RAM Content Extraction Against Modern Embedded Systems". In *2023 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, May 25, 2023*, pages 273–284. IEEE, 2023. https://doi.org/10.1109/SPW59333.2023.00030.

How Shifting Liability Explains Rising Cybercrime Costs

Tyler Moore

School of Cyber Studies, College of Engineering & Computer Science,
The University of Tulsa, OK, USA tyler-moore@utulsa.edu

Abstract. The extent and cost of cybercrime has grown substantially in recent years. One underappreciated reason why is that for many such crimes, intermediaries such as banks have successfully avoided liability for fraud. Using a case study and data from the FBI's Internet Crime Complaint Center, this paper demonstrates how the financial losses arising from cybercrimes where liability is assigned to financial institutions are dwarfed by crimes where it is not. The paper then discusses circumstances under which liability for these cybercrimes should be assigned to parties other than individual victims.

1 Introduction

In his seminal paper "Why cryptosystems fail", Anderson observed that US and UK bank regulation differed in terms of who was ultimately held responsible for paying for ATM card fraud [1]. In the US, the rules were clear: banks are liable for ATM fraud. In the UK, banks could frequently require customers to shoulder the costs of fraud. In technological respects, UK and US banks were quite similar. This policy difference led to vastly different outcomes, with UK banks experiencing higher overall fraud losses per capita. This early insight about the importance of incentives contributed to the emergence of the security economics as a subdiscipline of cybersecurity [2].

In the decades since, many new forms of cybercrime have proliferated. While the composite magnitude of the costs imposed by these cybercrimes have proven difficult to measure [3,4], it is clear that some categories cause much greater financial losses than others. This paper will argue that whenever intermediaries, such as banks, technology platforms and payment service providers, are held liable for cybercrime costs, they do a pretty good job managing the risk and minimizing overall fraud losses. Cybercrimes in this category includes phishing attacks and payment card fraud. However, when intermediaries can avoid liability for losses and instead place the burden of cybercrime on individuals and smaller enterprises, cybercrime costs have exploded. In fact, I argue that this is a natural reflection of the incentives at play for attackers and defenders alike. Cybercriminals are naturally drawn to attacks that avoid the ire of banks and technology platforms, as these attacks are more profitable and face less resistance. Defenders meanwhile do not place as much emphasis on countering such threats for the simple reason that they do not bear the cost of the attacks.

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

2 Case Study: PayPal Fraud

The following case study experienced by the author illustrates the problem. On April 26, 2024, I received a payment request through PayPal from "Loretta Simmons" for $789.99. Such a request is not unusual. My PayPal account is shared with my spouse. She collects vintage goods and occasionally purchases items from people she interacts with online. When requests like these arrive, we communicate through an out-of-band channel to verify whether the payment request is expected. In this case, she texted me, "Did you see that PayPal money request?", to which I replied with the details of the transaction. I misinterpreted this communication as confirmation that the transaction was valid, so I completed payment, using the "friends and family" option.

The next evening over dinner when I asked about what she had bought, she told me that she did not buy anything through PayPal. That is when I realized we had miscommunicated earlier and I had been scammed. What followed illustrates how when liability for fraud falls on consumers, it is easily ignored by intermediaries.

I called PayPal. I initiated a dispute through the automated system. A case was opened at 8:46PM. At 9:04PM, I received another email notifying me that my case had been closed, and they "determined there was no unauthorized use". They suggested I contact the seller (i.e., the scammer) to try to resolve my dispute. I immediately called PayPal again, only to find that the call center closed for the day at 9PM. I got through to a human operator on April 29, who again advised me to contact the seller to resolve the dispute. When I explained that the seller was in on the fraud, I was told to contact my bank to try to stop the payment. I immediately contacted the bank and disputed the transaction; unfortunately, the payment cleared at 4AM on April 29 and the bank refused reimbursement, stating that I should seek restitution from PayPal. Ultimately, neither PayPal nor the bank reimbursed me for the fraud.

What lessons can be learned from this experience? One is that PayPal's own processes are not optimized to assist customers who experience fraud initiated on its platform. The messaging and investigation focused on mediating disputes between legitimate buyers and sellers, as well as account takeovers. PayPal's investigation confirmed that I initiated the payment (which I never disputed doing), and then used that information to determine that they were not liable.

When payments are made to bank accounts controlled by scammers, acting quickly is essential to reversing fraudulent payments. Yet PayPal's initial messaging, both when I opened the dispute investigation and when it was quickly closed, made no recommendation that I contact my bank to dispute the transaction. Because the payment did not post until more than 24 hours after those communications, a faster response would likely have foiled the fraud. PayPal is not incentivized to assist customers in this manner, as the liability for fraud had been determined to lie with the customer.

Additionally, neither of the two operators I spoke with encouraged me to file a police report. When I asked if I should do so, I was told that is up to me and was something they could not assist with.

3 Liability and Self-Reported Cybercrime Losses

	2023		2022		2021	
	#	$ Loss	#	$ Loss	#	$ Loss
Cybercrime Categories Where Intermediaries are Usually Liable						
Credit Card/Check Fraud	13718	173.6M	22985	264.1M	16750	173.0M
Identity Theft	19778	126.2M	27922	189.2M	51629	278.3M
Non-Payment/Non-Delivery	50523	309.6M	51679	281.8M	82478	337.5M
Phishing/Spoofing	298878	18.7M	321136	160.0M	342494	126.4M
Total (Liable)	382897	628.2M	423722	895.1M	493351	915.1M
Cybercrime Categories Where Intermediaries are Usually Not Liable						
Advanced Fee	8045	134.5M	11264	104.3M	11034	98.7M
BEC	21489	2946.8M	21832	2742.4M	19954	2396.0M
Confidence Fraud/Romance	17823	652.5M	19021	735.9M	24299	956.0M
Employment	15443	70.2M	14946	52.2M	15253	47.2M
Extortion	48223	74.8M	39416	54.3M	39360	60.6M
Investment	39570	4570.3M	30529	3311.7M	20561	1455.9M
Lottery/Sweepstakes/Inheritance	4168	94.5M	5650	83.6M	5991	71.3M
Overpayment	4144	38.3M	6183	33.4M	6108	
Ransomware	2825	59.6M	2385	34.4M	3729	49.2M
Real Estate	9521	145.2M	11727	396.9M	11578	350.3M
Tech Support	37560	924.5M	32538	806.6M	23903	347.7M
Total (Not Liable)	299996	11489.4M	290828	9912.8M	253468	6666.3M

Table 1. Cybercrime losses from 2021–2023 according to the FBI IC3.

The US FBI operates the Internet Crime Complaint Center (IC3), which collects reports of cybercrimes experienced by individuals and organizations. Each year the IC3 releases a report detailing cybercrime incidents and financial losses, split by various categories [11,12,13].

Table 1 reports the figures for cybercrime categories that generate financial losses. It does not include categories of harms where no explicit financial loss is experienced, such as harassment, stalking, and crimes against children. I have also excluded infrastructure crimes such as botnets and malware.

The cybercrimes are split into two categories. At the top are crimes where fraud liability rests with intermediaries such as financial institutions. At the bottom are crimes where responsibility typically falls on the individuals involved.

In terms of the number of incidents reported, cybercrimes where individuals are not usually liable outnumber those where individuals are responsible, with 400–500K reports annually compared to 250–300K reports. These totals are heavily skewed by phishing, which accounts for the majority of all reports where banks are liable.

Despite a higher incidence of crimes, the amount of money lost to scams is much higher in cases where individuals are liable. In 2023, for example, losses due to these frauds totaled $11.5 billion, compared to $628 million for cases where banks and other intermediaries are liable. A similar trend holds for 2022 and 2021 as well – frauds where intermediaries avoid liability report an order of magnitude more financial losses than crimes where they foot the bill.

What drives these differences? Incentives provide the simplest explanation. When banks and other financial intermediaries are responsible for managing cybercrime risks, they do a respectable job reining in losses. For example, I have seen in the past two decades significant investment in countermeasures to combat phishing [8,9]. Consequently, while the number of phishing attacks remains high, reported losses are quite small (roughly $100 million annually according to IC3 data).

For crimes whose losses are borne directly by the victims, losses are much higher. For example, business-email compromise (BEC) reports annual losses of $2–3 billion. Here, firms are duped into paying fake invoices worth hundreds of thousands of dollars to scammers. While banks do cooperate with investigations and try to block these payments from clearing, they often fail. And when they fail, it's the bank's customer who pays.

The "least-cost avoider" principle from tort law which holds that liability should be assigned to the party that can avoid harm for the lowest cost [5]. It is clear that for phishing, identity theft and credit-card fraud, payment intermediaries can avoid the costs of these crimes more efficiently than individuals and organizations could. This is because the intermediaries have greater technical expertise and visibility into the crimes targeting their customers.

What about the other crime categories listed in Table 1 where intermediaries are not currently liable? In most cases, they are in a much better position to counter cybercrime risks than victim individuals and organizations. Take BEC. Each year, tens of thousands of organizations are targeted. While these organizations can and should invest in efforts to tighten protocols around payments to vendors, victims typically have never experienced these attacks until they are targeted. By contrast, financial institutions have been dealing with BEC attacks targeting their customers for years. They have access to transaction data, which can reveal anomalous patterns. They can purchase software from third-party vendors to identify suspected BEC scams. Put simply, banks are the least-cost avoider for BEC.

Also key to assigning liability responsibility is the extent to which an intermediary can be aware of the attack taking place and how their platform is utilized in the attack. These concepts are often interrelated. For example, in many advanced fee frauds, the cash-out mechanism is a money-services business like Western Union or Moneygram. Here, the operator typically does not know what the payment is being used for. In this case, it is not clear that the payment processor is in a strong position to detect and block the fraud.

The PayPal case study from Section 2 nicely illustrates how payment platforms may be utilized and aware of crimes they help facilitate. In contrast to

advanced fee frauds, lottery scams, BEC, and others, the platform itself was utilized to initiate the scam. I received a valid payment request initiated through PayPal by an illicit user. PayPal permitted "Loretta Simmons" to sign up for an account, associate a bank account, and submit payment requests (of which I was likely only one of many recipients). Hence, PayPal's platform was integral to several stages of the scam's operation. Moreover, this integration also ensures that PayPal has good awareness to the scam, and by extension, is in a strong position to mitigate the harms. The fact that it failed to detect or counter the attack (after being notified) can best be explained by the fact that they were not held financially responsible.

Finally, it is worth noting that there can be cases where no payment intermediary exists. Most ransomware attacks are monetized through Bitcoin payments. Victims pay directly to addresses established by cybercriminals. A similar approach is utilized in so-called "pig butchering" schemes. While these scams may appear to leverage a fully decentralized payment infrastructure, in practice they often hold accounts at one of the centralized cryptocurrency exchanges [6,10]. Hence, even in these cases intermediaries may be available where pressure could be applied if desired.

4 Discussion and Concluding Remarks

Experience has demonstrated that the harms resulting from cybercrime can be mitigated to a socially-acceptable level. The key is to get the incentives right. I have shown that when liability for cybercrimes is placed on the party in the best position to defend against attacks, harms are lower. Unfortunately, cybercriminals often behave rationally. Many have shifted their efforts away from crimes that banks and other platforms are focused on reducing. Instead, criminals have turned their attention to scams where such well-resourced intermediaries are not liable and therefore are not devoting as much effort to stop.

What are the policy implications? If reducing overall societal harm is the goal, then responsibility for more cybercrimes need to shift away from individual victims to the intermediaries in the best position to take precautions. Such an approach may not always be popular, particularly when intermediaries could argue that they are not the ones responsible for insecure or otherwise poor decisions taken by their customers. Yet the principle of indirect intermediary liability does not require liability to be placed on the party most responsible [7]. It holds that the party in the best position to counter the risk should be the one assigned responsibility for doing so.

One way to honor Ross Anderson's legacy is to continue to fight for the many individuals who fall victim to cybercrimes and are held financially responsible even when responsibility should lie elsewhere. This paper has shown one strategy for doing so.

References

1. Ross Anderson. "Why Cryptosystems Fail". In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93, pages 215 – 227. Association for Computing Machinery, New York, NY, USA, 1993. ISBN 0-89791-629-8. https://doi.org/10.1145/168588.168615. URL https://doi.org/10.1145/168588.168615.
2. Ross Anderson. "Why information security is hard — an economic perspective". In *Seventeenth Annual Computer Security Applications Conference*, pages 358–365. 2001. https://doi.org/10.1109/ACSAC.2001.991552.
3. Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michael van Eeten, Michael Levi, Tyler Moore and Stefan Savage. "Measuring the Cost of Cybercrime". In *11th Workshop on the Economics of Information Security (WEIS)*. 2012. URL https://tylermoore.utulsa.edu/weis12.pdf.
4. Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Carlos Gañán, Tom Grasso, Michael Levi, Tyler Moore, Stefan Savage and Marie Vasek. "Measuring the Changing Cost of Cybercrime". In *18th Workshop on the Economics of Information Security (WEIS)*. 2019. URL https://tylermoore.utulsa.edu/weis19cost.pdf.
5. Guido Calabresi and A. Douglas Melamed. "Property Rules, Liability Rules, and Inalienability: One View of the Cathedral". *Harvard Law Review*, **85**(6):1089, April 1972. ISSN 0017811X. https://doi.org/10.2307/1340059. URL https://www.jstor.org/stable/1340059?origin=crossref.
6. John M. Griffin and Kevin Mei. "How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering", February 2024. https://doi.org/10.2139/ssrn.4742235. URL https://papers.ssrn.com/abstract=4742235.
7. Tyler Moore. "The economics of cybersecurity: Principles and policy options". *International Journal of Critical Infrastructure Protection*, **3**(3):103–117, December 2010. ISSN 1874-5482. https://doi.org/10.1016/j.ijcip.2010.10.002. URL https://www.sciencedirect.com/science/article/pii/S1874548210000429.
8. Tyler Moore and Richard Clayton. "Examining the impact of website take-down on phishing". In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, eCrime '07, pages 1–13. Association for Computing Machinery, New York, NY, USA, October 2007. ISBN 978-1-59593-939-5. https://doi.org/10.1145/1299015.1299016. URL https://doi.org/10.1145/1299015.1299016.
9. Adam Oest, Penghui Zhang, Brad Wardman, Eric Nunes, Jakub Burgis, Ali Zand, Kurt Thomas, Adam Doupé and Gail-Joon Ahn. "Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale". In *USENIX Security Symposium*, pages 361–377. 2020. ISBN 978-1-939133-17-5. URL https://www.usenix.org/conference/usenixsecurity20/presentation/oest-sunrise.
10. Marilyne Ordekian, Antonis Papasavva, Enrico Mariconti and Marie Vasek. "A sinister fattening: Dissecting the tales of pig butchering and other cryptocurrency scams". In *2024 Symposium on Electronic Crime Research (eCrime 2024)*. 2024.
11. US Federal Bureau of Investigation. "Internet Crime Report", 2021. URL https://www.ic3.gov/AnnualReport/Reports/2021_IC3Report.pdf.
12. US Federal Bureau of Investigation. "Internet Crime Report", 2022. https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf.
13. US Federal Bureau of Investigation. "Internet Crime Report", 2023. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf.

'Nothing about us without us'* Towards Equitable Cybersecurity Capabilities

Partha Das Chowdhury**

University of Bristol

Abstract. Security & privacy provisioning exercises should not only recognize the heterogeneity of individual needs but also systematically capture them. Prior research proposed a shift from *utilitarian usability* to adopt Amartya Sen's *capability approach* to capture individual needs, interests and circumstances. In this position paper we argue that *capability approach* based systems provisioning can also end up being exclusory unless *capabilities* are adequately granular.

1 Introduction

The ability to exercise security & privacy online can unlock significant human rights, yet remains a privilege exclusive to individuals in better circumstances than others. There is an inescapable reality – every individual is not equally disposed to securely and safely participate in a digital first society. Individuals differ in their health, ability, education and/or can be in vulnerable situations, displaced from their homes and/or living under oppressive regimes.

Usable security and privacy [2,1] largely privileges quantitative ordering of preferences of surface features; such *utilitarian* focus of *usability*, however well meaning, has methodological short comings. They cannot capture individual *needs*. Participants of the *first capability approach workshop to protect citizens against online harms* in 2022 [11] proposed a manifesto[1] to expand from *utilitarian usability* to an assessment of individual opportunities to inform the design of inclusive security mechanisms. The workshop proposed Amartya Sen's *capability approach*[2] to systematically assess individual opportunities.

While usability research hasn't considered capabilities and *without capability there is no effective usability*, in this paper we posit that protection mechanisms

* The phrase is borrowed from disability movement, we refer to it to include more disadvantaged groups.

** The author is grateful to Awais Rashid for reading and commenting on an earlier draft of the paper. Awais has actively mentored and positively influenced the author's work in this space for the last three years.

[1] Ross Anderson was one of the key signatories of the manifesto and contributed in formulating the key elements of the manifesto. This paper is provoked by Ross' example of *capabilities*.

[2] Articulated by Sen first in Tanner lectures on Human Values, delivered at Stanford University in 1979. Available on Tanner Lectures website, reprinted in John Rawls et al., Liberty, Equality and Law (Cambridge: Cambridge University Press, 1987)

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

designed using *capability approach* can end up being exclusory unless the list of *basic capabilities* is adequately granular. This is critical to systematically minimise exclusion. The position is elaborated with a set of example capabilities. This work has two purposes: 1) argues the need for a granular list of *basic capabilities* and 2) proposes a method to formulate one.

2 Capability Approach

Amartya Sen outlined the foundations of *capability approach* while critiquing utilitarian and Rawlsian approaches to welfare [23]. This was presented as framework of thought, thereby consciously avoiding giving it an epistemological status of 'The' *capability approach*. Individual freedom and human diversity are at the core of any operationalization of this framework. *Capability approach* has two principal ingredients:

- **Capability**. This captures the opportunities individuals have, for example their physical abilities, as well as the influence of the environment on their opportunities.
- **Functioning**. The life individuals want to live, for example, living a private life.

The framework recognises that mere possession of resources cannot empower individuals to achieve a *functioning*. For example, provisioning a bicycle cannot enable all individuals to achieve the *functioning* of mobility, rather individuals with resources such as able physique, good and safe roads, can be mobile, while individuals without these will need different support to be mobile with dignity.

Basic Capabilities. A critical subset of *capabilities* is formulated as *basic capabilities*:

> *"Basic capability means the freedom to do certain basic things, for example the ability to read and write is a* ***basic capability*** *in certain jurisdictions. They can help 'in deciding on a cut-off point for the purpose of assessing poverty and deprivation' "* [22, p.109].

Delineating a set of *capabilities* as *basic capabilities* makes them focal variables for provisioning. We borrow an example from mobility to explain the notion of *basic capability*. A *basic capability* for individuals with appropriate eyesight is to be able use their eyes to safely cross busy roads. A recognition of this led to the provisioning of zebra crossings with or without push buttons to stop traffic. However, *basic capability* for individuals with partial or no vision would be to avail zebra crossing (without seeing) if they are to be mobile with dignity. A recognition of this need led to the provisioning of tactile pavings and audible push buttons. Martha Nussbaum advocated for a universal list of *basic capabilities* while Sen argued for a more contextual list [17,18]. Welfare literature has considerably deliberated on the method to draw up a list of *basic capabilities* as its granularity has a direct effect on inclusions and exclusions. Diverse and granular capabilities means wider inclusion. In absence of granularity, women's welfare for example, can be subsumed under household and community welfare.

Basic Capabilities in cybersecurity. We refer to *basic capabilities in cybersecurity* as the basic minimum provisioning required by individuals to carry out various cybersecurity tasks. The importance of delineating *basic capabilities* can be established from prior studies; a recent systematization effort highlights the role of age, gender and training influence individual ability to detect phishing emails [5]. A recent study with diverse age groups confirms the influence of age in responding to anti-phishing mechanisms [16]. Security mechanisms and the manner of their provisioning are privileged by a developers' view of what their users need. However, developers' understanding are found to be disconnected from the needs of their users particularly in high-risk, marginalized or vulnerable situations such as whistle blowers, victims of domestic violence, protesters or refugees [15,8].

A systematic capture of barriers to influence *basic capabilities* can help provision inclusive and accessible mechanisms [19]. Similar to general welfare provisioning, cybersecurity *capabilities* too need to deliberate on matters of granularity to minimise exclusion as far as possible. For example, one or more age related impairments can act as barriers in applying tasks as multi-factor authentication, setting up backups or configuring updates [12]. Considering one and not the others might exclude those affected with them or even exclude individuals affected with multiple impairments.

3 Granularity of *basic capabilities*

Capability approach allows a informationally rich comparison of interpersonal welfare. This means gathering appropriate information on individual barriers and situations which in turn leads a fine grained list of *basic capabilities* for a basic minimum standard of living. We engage with an example list of *basic capabilities* that emerged in the workshop[3] against criteria for drawing up such a list from feminist scholarship [21]. The suggested list is as

- Capability to escape destitution: don't build systems that force people to use broadband to claim state benefits, expose frail seniors to fraud.
- Capability to escape commercial predators: don't build systems that exploit dark patterns.
- Capability to find friends and partners: don't build systems that stigmatise.
- Capability to escape personal violence: don't build systems that make it hard to escape abusers.

3.1 Constructive refinement of the capabilities

While the above capabilities appeal to our moral intuition but needs a reasoned qualification to be informationally rich with barriers pertaining to particular demographic groups. We discuss the above capabilities against established criteria for operationalization using *capability approach.* For each of the criteria we suggest example ingredients which can be used to expand them.

[3] This example list was suggested by Ross Anderson as part of his presentation.

Criterion of Explicit Formulation — urges us to go beyond what is reflected through democratic choice. The stated capabilities would require further expansion to satisfy this criterion. While there can be many individuals without the financial ability or vulnerable to fraud, yet there can be subgroups with specific circumstances. For example, individuals fleeing conflict zones might not have devices or have access to shared devices [13]. Moreover, individuals with diverse abilities would require diverse support to be able to use mechanisms to protect themselves against fraud. A systematic capture of barriers would unravel diverse individual opportunities to protect against personal violence, dark patterns or the ability to find friends. A example barrier can be language [25,7] and thus the needs of linguistic minorities should not be lost in a majoritarian articulation of linguistic preferences. In the context of social media privacy controls, a Judge in England observed that disabled children should be able to apply them with or without help [4]. A majoritarian view of controls can overlook needs of disabled minorities and thus the need for going beyond quantitative ordering of majority preferences. On the other hand multiple marginalized identities find it difficult to find support in online spaces compared to privileged groups such as white and married as has been reported in the case of LGBTQ communities [3]. The element of explicit formulation would ensure that the needs of colour and non partnered sexual minorities are not subsumed within the needs of white and married sexual minorities.

Criterion of Sensitivity to Context — means that the list should speak the language of the very demographic group it intends to protect. While going beyond majoritarian voice is important, yet a reasonable *basic capabilities* for individuals considered as part of *explicit formulation* should be at an appropriate level of abstraction to represent their interests, circumstances and needs. For example, sexual minority women in China experience stigmatisation online differently than in other parts of the world [10], thus they might have diverse needs for a basic minimum online participation to find partners. On the other hand, minimum provisions to protect from frauds and commercial predators need nuanced understanding of the needs of the very individuals they intend to protect. For example, there is a gap in studying the password usage ability of dyslexic individuals [20]. Sim et al. [24] report that older adults with disabilities are often neglected in security design deliberations. Elderly users can find it difficult to apply multi-factor authentication mechanisms due to age related conditions such as vision, memory along with family situations [12]. A *capability approach* based assessment of individual opportunities also factors environmental factors. For example, Tor can protect various minority groups against majoritarian violence, however individuals living under oppressive regimes will find it difficult to use such communication mechanisms [14].

Criterion of Different Levels of Generality — specifies an unconstrained list of *basic capabilities* which can be refined to a subset that can be implemented at different points in the future with evolving political, social and technical realities. Consequently some of the capabilities can be implemented in the immediate

future and some in the medium term, while for others there would be a continuous push for conducive individual and environmental conditions. This criterion draws from the previous criterion and we will discuss the examples from the previous criterion to draw the relationship. For example, multi-factor authentication for elderly users with partial disabilities such as vision might be a consideration for future technology research. On the other hand, extant political situations might not be conducive to provision Tor for protecting minority groups, however situating it in a ideal unconstrained list makes it a candidate for continuous political push at appropriate forums [6]. The key however is having the agreed list of *basic minimum* to continually influence the technical and policy agenda [9].

Criterion of Exhaustion & Non-Reduction — means that we include every barrier identified by individuals in a particular context to be considered as a focal variable. Consequently, the *basic capabilities* that evolve are distinct with negligible overlaps. Taking the some of the above examples, multiple marginalised identities means multiple barriers and thus each one of them should be taken into account. The broad umbrella of LGBTQ should not subsume multiple marginalization like colour, gender so on and so forth. The same can be argued for provisioning capabilities to protect against fraud. Elderly citizens might have multiple barriers and a combination of them like failing vision along with arthritic hands. Highlighting each barrier individually can lead to a comprehensive list for provisioning efforts. For example, granular recognition means provisioning safe space for both white and sexual minority as well as black and sexual minority. Similar affordances can be extended to elderly citizens with one or multiple barriers for safe online participation.

4 Conclusion – How granular capabilities help

Cybersecurity capability egalitarianism advocates explicit focus on individual opportunities. In the domain of welfare absence of opportunities are used to measure poverty; similarly absence of individual opportunities to apply cybersecurity tasks can help measure security & privacy poverty [9]. We argue that a comprehensive measure of poverty requires that a systematic capture of individual opportunities should be at a sufficiently intimate level. For example, in digital re-settlement of refugees a focus on the refugees alone is half the picture of precarity; a study of community organisations reveals their challenges to support refugees. Smaller and grassroot organizations do not have adequate security literacy and infrastructure yet they are responsibilized to protect refugees [13]. Such misplaced responsibilization in turn left refugees security & privacy poor. A possible way in this context can be policy deliberations among United Nations High Commissioner for Refugees (UNHCR) and local governments. Similarly, the argument for informationally rich granular capabilities can extend to other areas such as access for social media privacy controls among disabled users. The understanding of care givers' opportunities, in this context to help their wards are also important to provision appropriate controls.

References

1. Yasemin Acar, Sascha Fahl and Michelle L. Mazurek. "You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users". In *2016 IEEE Cybersecurity Development (SecDev)*, pages 3–8. 2016. https://doi.org/10.1109/SecDev.2016.013.
2. Anne Adams and Martina Angela Sasse. "Users are not the enemy". *Communications of the ACM*, **42**(12):40–46, 1999.
3. Nazanin Andalibi, Ashley Lacombe-Duncan, Lee Roosevelt, Kylie Wojciechowski and Cameron Giniel. "LGBTQ persons' use of online spaces to navigate conception, pregnancy, and pregnancy loss: An intersectional approach". *ACM Transactions on Computer-Human Interaction (TOCHI)*, **29**(1):1–46, 2022.
4. BAILLII. "England and Wales Court of Protection Decisions", 2019. https://www.bailii.org/ew/cases/EWCOP/2019/3.html.
5. Shahryar Baki and Rakesh M Verma. "Sixteen Years of Phishing User Studies: What Have We Learned?" *IEEE Transactions on Dependable and Secure Computing*, **20**(2):1200–1212, 2022. 10.1109/TDSC.2022.3151103.
6. Mehrab Bin Morshed, Michaelanne Dye, Syed Ishtiaque Ahmed and Neha Kumar. "When the internet goes down in Bangladesh". In *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*, pages 1591–1604. 2017.
7. Pierre Bourdieu. *Language and symbolic power*. Harvard University Press, 1991.
8. Ian Brown. "Social media surveillance". *The international encyclopedia of digital communication and society*, pages 1–7, 2015.
9. Partha Das Chowdhury and Karen Renaud. "Advocating a Policy Push Toward Inclusive and Secure "Digital-First" Societies". *IEEE Security & Privacy*, 2024.
10. Yichao Cui, Naomi Yamashita, Mingjie Liu and Yi-Chieh Lee. "'"So close, yet so far": exploring sexual-minority women's relationship-building via online dating in china". In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–15. 2022.
11. Partha Das Chowdhury, Lizzie Coles-Kemp, Karolina Follis, Sanja Milivojevic, Awais Rashid, Genevieve Liveley, Gina Netto, Andres Dominguez, Ross Anderson and Kopo Marvin Ramokapane. "From Utility to Capability: A Manifesto for Equitable Security and Privacy for All", 2023. https://bpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/1/670/files/2023/02/Capability-Approach-Manifesto.pdf.
12. Partha Das Chowdhury and Karen Renaud. "'Ought' should not assume 'Can'. Basic Capabilities in Cybersecurity to Ground Sen's Capability Approach". In *Proceedings of the 2023 New Security Paradigms Workshop*, pages 76–91. ACM, Spain, 2023. https://doi.org/10.1145/3633500.3633506.
13. Evan Easton-Calabria. "Responsibility and trust: Using digital technologies in forced migration". In *Handbook on Forced Migration*, pages 446–463. Edward Elgar Publishing, 2023.
14. Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama and Florian Schaub. *Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants*, page 1–15. Association for Computing Machinery, New York, NY, USA, 2018. ISBN 9781450356206. URL https://doi.org/10.1145/3173574.3173688.
15. Josephine Lau, Benjamin Zimmerman and Florian Schaub. "Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers". *Proc. ACM Hum.-Comput. Interact.*, 2018.

16. Tian Lin, Daniel E Capecci, Donovan M Ellis, Harold A Rocha, Sandeep Dommaraju, Daniela S Oliveira and Natalie C Ebner. "Susceptibility to spear-phishing emails: Effects of internet user demographics and email content". *ACM Transactions on Computer-Human Interaction (TOCHI)*, **26**(5):1–28, 2019. https://doi.org/10.1145/3336141.
17. Nussbaum Martha. "Nature, Function, and Capability: Aristotle on Political Distribution". *Oxford Studies in Ancient Philosophy*, pages 145–184, 1988.
18. Martha C. Nussbaum. *Women and Human Development: The Capabilities Approach*. The Seeley Lectures. Cambridge University Press, 2000. https://doi.org/10.1017/CBO9780511841286.
19. Karen Renaud and Lizzie Coles-Kemp. "Accessible and inclusive cyber security: a nuanced and complex challenge". *SN Computer Science*, **3**(5):1–14, 2022.
20. Karen Renaud, Graham Johnson and Jacques Ophoff. "Dyslexia and password usage: accessibility in authentication design". In *Human Aspects of Information Security and Assurance: 14th IFIP WG 11.12 International Symposium, HAISA*, pages 259–268. Springer, Mytilene, Lesbos, Greece, July 8–10, 2020. https://doi.org/10.1007/978-3-030-57404-8_20.
21. Ingrid Robeyns. "SEN'S CAPABILITY APPROACH AND GENDER INEQUALITY: SELECTING RELEVANT CAPABILITIES". *Feminist Economics*, **9**(2-3):61–92, 2003.
22. Amartya K Sen. *The Standard of Living*. Tanner Lectures in Human Values. Cambridge: Cambridge University Press, 1976.
23. Amartya K. Sen. "Equality of What?" In *McMurrin S Tanner Lectures on Human Values*, volume 1. Cambridge: Cambridge University Press, 1987, Cambridge, UK, 1979. Reprinted in John Rawls and Charles Fried and Amartya Sen and Thomas C Schelling. Sterling M. McMurrin (Ed), Liberty, Equality and Law.
24. Mattea Sim, Kurt Hugenberg, Tadayoshi Kohno and Franziska Roesner. "A Scalable Inclusive Security Intervention to Center Marginalized & Vulnerable Populations in Security & Privacy Design". In *New Security Paradigms Workshop*. 2023.
25. Sarah Myers West. "Data capitalism: Redefining the logics of surveillance and privacy". *Business & society*, **58**(1):20–41, 2019.

Security Economics Meets Force Majeure Clauses: Are Security Breaches Unforeseeable and Unavoidable Events?

Marilyne Ordekian, Marie Vasek, and Ingolf Becker

University College London, London, UK
marilyne.ordekian.21@ucl.ac.uk

Abstract. In this study, we integrate security economics with legal analysis, presenting a new paradigm for assessing cybersecurity breaches as potential force majeure – unforeseeable and unavoidable events. Considering centralised cryptocurrency exchanges, we explore how liability disclaimers impact risk allocation and accountability in the industry. Shockingly, the majority of centralised cryptocurrency exchanges currently discharge themselves from liability in case of cybercrime events, despite their common occurrence. This leads to misaligned incentives for exchanges. Our evaluation of the newest EU MiCA Regulation demonstrates the potential to foster a more accountable and resilient regulatory environment for the cryptocurrency industry.

1 Introduction

In his 1994 paper "Liability and Computer Security: Nine Principles," Anderson critiqued the presumption of infallibility in certain emerging technologies, which often resulted in shifting liability onto consumers and leading to unjust prosecutions [1]. After thirty years, this dynamic persists in various forms, particularly with self-regulating emerging financial technologies (FinTech) like centralised cryptocurrency exchanges. More specifically, many entities, as we will demonstrate, exploit regulatory uncertainty to shift or disclaim liability during cybersecurity breaches, perpetuating the same issues Anderson had identified.

Centralised cryptocurrency exchanges are the dominating intermediaries in the digital assets field, facilitating millions of transactions internationally each day [2]. Despite their increased popularity, exchanges have historically been left to self-regulate, with meaningful and comprehensive interventions only now emerging, particularly within the EU. During this regulatory oversight era, even giants such as Mt. Gox and FTX collapsed under the weight of operational mismanagement, fraud, and/or cyberattacks [14,6]. Over the years, exchanges gained a reputation for poor security, costing users millions in losses [9]. Often, many of these breached exchanges ended up eventually failing [10].

Yet, not a lot seems to have changed. In a forthcoming study investigating all centralised exchanges operating in Europe, we found significant weaknesses in

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

their security policies [11]. Not only are those policies porous, but exchanges often disclaim liability for security incidents; alarmingly, categorising them as force majeure events. This concerning practice frames security breaches as unforeseeable and unavoidable events, consequently absolving exchanges of accountability and performing their duty, while ignoring their role in mitigating such threats. Meanwhile, users bear the consequences of such incidents. Based on our findings, these clauses often coexist with liability disclaimers on service performance, suggesting a deliberate effort to shield exchanges from liability for failing to offer a reliable and secure service.

In this short piece, we apply the principles of security economics into a new legal paradigm and argue the following: Are cybersecurity breaches in emerging FinTech industries truly unforeseeable and unavoidable events? To explore this, we present a case study on centralised cryptocurrency exchanges.

2 Force Majeure Clauses: An Overview

Force majeure, meaning "superior force", constitutes an event(s) that excuses one or more contracting parties from the performance of a contractual obligation(s) whilst disclaiming all liability for the resulting non-performance [7]. The concept originates from Roman law in efforts to excuse debtors from performing their duty due to events rendering it impossible or difficult [13]. The primary rationale is that contracting parties should not be liable for events beyond their prevention or foresight. Without such a clause, a party facing such a circumstance could deal with a breach of contract, risking damages and litigation. As this concept plays a vital role in bringing fairness to the execution of contracts, it was later adopted in civil and common law jurisdictions (with minor differences in adaptation in common law systems) [13].

Therefore, a force majeure clause is triggered by an **unforeseeable** and **unavoidable** event that renders one or both parties from executing their obligation(s). Hence, the affected party is excused from performance without incurring liability. Examples of force majeure events include Acts of God (i.e. natural disasters), terrorism, political events, civil unrest, wars, pandemics, etc. Below, we present an example:

"We will not be responsible for damages caused by delay or failure to perform undertakings when the delay or failure is caused by fires, strikes, power outages, acts of God [. . .] computer, server, or internet malfunctions or, any delays, defaults, failures or interruptions that cannot reasonably be foreseen ("Force Majeure"). In the event of Force Majeure, we will be excused from any and all performance obligations [. . .]."

The primary purpose of a force majeure clause is to maximise the protection of parties by mitigating the risks of unintended consequences [7]. These clauses are generally tailored to the specific content and the subject of the contract [4]. For instance, a tenancy contract would include fires, floods, or earthquakes, whilst online service providers often categorise in their terms and conditions events like critical service or infrastructure disruptions as force majeure. This

tailoring is also seen with FinTech entities such as cryptocurrency exchanges, which we overview in the following section.

3 Case Study: Centralised Cryptocurrency Exchanges

To better understand the current self-regulatory practices of FinTech service providers, we studied 75 centralised cryptocurrency exchanges operating in Europe [11]. To this end, we conducted legal analysis on 143 documents and web pages, comprising terms and conditions, security policies, and other legal documents from exchange websites. In this article, we focus specifically on liability disclaimers, considering the impact of force majeure clauses within a security economics framework.

Clauses disclaiming liability for service performance can be found in almost all exchanges (71/75), this includes issues like service reliability and availability, operational failure, and other performance-related problems. A common assertion made by exchanges to disclaim such liability is that they take "all reasonable" precautions to ensure the service's safety, security, and reliability. Yet, the true definition and scope of *reasonable* measures remain one of the enduring ambiguities in current practices.

Over half of the exchanges (40/75) explicitly disclaim liability in cases of user data breaches. This is an issue considering the heightened scrutiny exchanges have been facing to collect more user data (e.g. passports, physical addresses, selfies) to comply with anti-money laundering and countering the financing of terrorism policies (AML/CFT). For instance, in 2023, Binance – the world's largest exchange – pleaded guilty to AML/CFT violations; it was penalised with the largest financial penalty in U.S. history with its CEO, Changpeng Zhao, later serving a brief jail sentence [15]. It has been previously argued that obligating exchanges to comply with these policies without simultaneously mandating robust security measures, poses immense risks to user privacy as exchanges have porous security practices [12]. Withal, the prevalence of data breach disclaimers considering the frequency of exchanges being targets of attacks, suggests that liability disclaimers here may act as a discouraging factor for stronger security investments, which further exacerbates these risks.

This contrasts to liability disclaimers related to cybercrime, encompassing broader incidents like DDoS attacks as well as specific breaches resulting in stolen funds or compromised means of access (e.g., private keys or access credentials) where 59 of 75 exchanges explicitly disclaim liability for such events, while the remainder remains silent on the matter. Given the custodial nature of examined exchanges and their duty as safekeepers of user funds, coupled with the frequent security breaches resulting in substantial financial losses, the presence of these disclaimers raises significant concerns. In fact, such clauses can be seen as a tacit admission of insufficient trust in their security measures and a lack of commitment to the prudential duties inherent in offering custodial services. Moreover, such disclaimers can only further reflect the industry's continued operation in a regulatory Wild West.

Force majeure clauses were present in nearly all the contracts reviewed. Notably, 13 exchanges categorised cyberattacks or security breaches as force majeure events, effectively absolving themselves of all liability by deeming such events as unforeseeable and unavoidable. Whilst the number of exchanges here is comparably low, yet, this sets a concerning precedent within the industry. In the next section, we examine why this practice is problematic and assess whether such events should legitimately qualify as force majeure.

4 Cybersecurity Breaches as Force Majeure Events (?)

One of the key elements required to trigger a force majeure clause is unforeseeability. However, in the modern threat landscape – particularly within the cryptocurrency industry – cybersecurity risks are well-documented and arguably constitute the biggest threats to exchanges, given the nature of their services. In fact, $88.6 billion were lost to hacks until October 2021, which underscores the extent of exchanges' susceptibility to attacks [3].

Custodial exchanges have a prudential responsibility to anticipate such risks and implement robust preventative/reactive measures. Categorising cyberattacks and breaches as force majeure may risk conflating truly unforeseeable occurrences, such as natural disasters, with risks that are inherent and foreseeable in the ordinary operational course of business. This distinction is vital to maintaining accountability and ensuring exchanges uphold their operational responsibilities.

Building on this, the second primary element of a force majeure event is unavoidability, i.e. the event must be irresistible and outside the reasonable control of the affected party. In layman's terms, the event causing an exchange's non-performance could not have been prevented through reasonable actions. This requirement is challenging to meet for exchanges, as they inherently operate in a high-risk environment where attacks are not just possible, but anticipated.

To consider an event as unavoidable, an exchange must demonstrate that it implemented all necessary precautionary measures in line with industry standards. For example, failure to adequately train employees to identify phishing attempts, neglect to timely patch known software vulnerabilities, or – more specifically to cryptocurrencies – storing the majority of customer funds in non-secure hot wallets (as FTX did), all undermine such a claim [14]. Without standardised and industry-tailored security practices, there will inevitably be heightened scepticism about whether an exchange is genuinely secure or merely posturing. To this end, the absence of robust safeguards and accountability mechanisms only leaves these claims open to significant scrutiny.

Furthermore, characterising security breaches as force majeure events raises concerns about legal implications and negligence. Such practice further impacts the arguably inexistent balance of risk between consumers and service providers in general. While service providers like exchanges may exploit these clauses as legal shields against liability, this also raises critical questions about accountability, fairness, and consumer protection. By categorising security breaches as

force majeure, service providers shift the burden of risk and consequences onto users, effectively eroding their own accountability and responsibility. As discussed in Section 3, this practice may disincentivise investments in robust security measures, as the financial fallout of breaches can be mitigated through these contractual disclaimers [8]. Finally, beyond threatening the safety of the service and consumer protection, such practices undermine the corporate and operational diligence expected of service providers in general, leaving users to bear the brunt of possible avoidable risks.

5 Future Changes Under the MiCA Regulation

After a prolonged period of regulatory uncertainty, the EU adopted the world's first cryptocurrency-specific and comprehensive regulation, the Markets in Crypto-Assets Regulation (MiCA) [5]. MiCA aims to harmonise the regulation of the industry across the EU, providing greater standardisation and enhanced consumer protection. The provisions of MiCA concerning centralised exchanges (Crypto-Asset Service Providers, CASPs), entered into force at the end of 2024.

MiCA addresses circumstances under which exchanges may be held liable, though the language leaves room for interpretation. For instance, per art. 75, custodian exchanges are deemed liable for losses of user funds or means of access if the incident is attributable to the CASP (i.e., within their control). Consequently, exchanges will be required to make "all reasonable" efforts to ensure service continuity, including employing resilient and secure ICT systems as mandated by the EU's upcoming Digital Operational Resilience Act (DORA). These practices must also include measures to safeguard the confidentiality, integrity, and availability of data and the service.

While these provisions raise several legal questions, we briefly highlight three key issues. First, the ambiguity surrounding "reasonable" efforts leaves significant uncertainty, as no clear guidance exists on what this standard entails in practice. Second, the scope of application of an "incident" remains undefined. Third, and most importantly, it is unclear what can be considered within an exchange's "control" or "attributed" to it. The latter point is particularly concerning in light of the empirical findings we presented in Section 3. In short, exchanges may exploit this ambiguity to evade liability by arguing that incidents were outside their "control", potentially even categorising breaches as force majeure events beyond their control or prediction.

This gap requires urgent attention from regulators, as it risks undermining accountability in the industry. But, until clearer definitions emerge and enforcement begins, the pursuit for clarity on what is "reasonable", "unavoidable", and "unforeseeable" leaves users at a disadvantage. While the EU has taken an important first step with MiCA, only time and (hopefully) rigorous enforcement will determine whether Anderson's prescient "Nine Principles" will continue to apply in the coming decades.

References

1. Ross J Anderson. "Liability and computer security: Nine principles". In *Third European Symposium on Research in Computer Security (ESORICS '94)*, pages 231–245. Springer, 1994.
2. Chainalysis. "Cryptocurrency Exchanges in 2021: A Competitive Landscape Analysis", 2021. https://go.chainalysis.com/2021-crypto-exchange-landscape-report.html.
3. Ben Charoenwong and Mario Bernardi. "Lessons from a decade of cryptocurrency hacks, 2011–2021". In *The Elgar Companion to Decentralized Finance, Digital Assets, and Blockchain Technologies*, pages 147–166. Edward Elgar Publishing, 2024.
4. Larry A DiMatteo and Lucien J Dhooge. *International business law*. Thomson, 2005.
5. European Union. "Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. OJ L 150/40", 2023.
6. Amir Feder, Neil Gandal, JT Hamrick and Tyler Moore. "The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox". *Journal of Cybersecurity*, **3**(2):137–144, 2017. https://doi.org/10.1093/cybsec/tyx012.
7. Marel Katsivela. "Contracts: force majeure concept or force majeure clauses". *Uniform Law Review – Revue de droit uniforme*, **12**:101, 2007.
8. Jonathan Levin. "Information and the Market for Lemons". *RAND Journal of Economics*, pages 657–666, 2001.
9. Patrick McCorry, Malte Möser and Syed Taha Ali. "Why preventing a cryptocurrency exchange heist isn't good enough". In *Security Protocols Workshop*, pages 225–233. Springer, 2018. https://doi.org/10.1007/978-3-030-03251-7_27.
10. Tyler Moore, Nicolas Christin and Janos Szurdi. "Revisiting the Risks of Bitcoin Currency Exchange Closure". *ACM Transactions on Internet Technology*, **18**(4):50:1–50:18, September 2018.
11. Marilyne Ordekian, Ingolf Becker, Tyler Moore and Marie Vasek. "Evaluating compliance with cryptocurrency exchange regulations using new rules and current practices". *Under Review*, 2025. https://ibecker.eu/l/ordekian2025evaluating.
12. Marilyne Ordekian, Ingolf Becker and Marie Vasek. "Shaping Cryptocurrency Gatekeepers with a Regulatory 'Trial and Error"'. In *Financial Cryptography and Data Security: FC 2023 Workshops, The 4th Workshop on Coordination of Decentralized Finance, CoDecFin, Croatia*. 2023. https://doi.org/10.2139/ssrn.4398362.
13. Caslav Pejovic. "Civil law and common law: Two different paths leading to the same goal". *Poredbeno Pomorsko Pravo*, **155**:7, 2001.
14. United States Bankruptcy Court, D. Delaware. "First Interim Report of John J. Ray III to the Independent Directors on Control Failures at the FTX Exchanges", 2023. https://www.courtlistener.com/docket/65748821/1242/1/ftx-trading-ltd/.
15. United States Department of Justice. "Binance and CEO Plead Guilty to Federal Charges in $4*B* Resolution", 2023. https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

What we talk about when we talk about extortion: The evolution from romanticism to ransomware (2005–2009)

Helen Oliver[1][0000-0003-1467-8165] and Alice Hutchings[2][0000-0003-3037-2684]

[1] Birkbeck, University of London WC1E 7XH h.oliver@bbk.ac.uk
[2] University of Cambridge CB3 0FD alice.hutchings@cl.cam.ac.uk

Abstract. In this paper, we analyse discussion of the concept of extortion in Russian-language underground forums from 2005–2009, during what we term the "Post-Romantic" era. In this period, the press began to publicise cybercriminals' perceived shift away from "hobby hacking" and towards profit-driven crime. While the cybercriminals' dream of automating extortion would be realised years later, the term "ransomware" (программы-вымогатели, literally "extortion programs") first appeared in the CrimeBB dataset in 2006. These early years set the initial conditions for ransomware to grow to its present-day scale, with multimillion-dollar demands and threats to critical infrastructure.

Keywords: Cybercrime · Underground Communities · Extortion.

1 Introduction

"Hackers as romantics are becoming a thing of the past," lamented a July 2005 article shared on the Russian underground forum, anti-chat.ru (AC) about the increased profitability of cybercrime. Forum members reacted with a volley of quotes from the film "Gentlemen of Fortune" [20], in which criminals steal the golden helmet of Alexander the Great from an archaeological dig. In May 2021, Colonial Pipeline, the largest fuel pipeline in the United States, reportedly paid $4.4 million [14] to release the critical infrastructure from a ransomware attack attributed to the DarkSide group [1]. Though most of the payment would later be recovered, the incident highlighted how the profit motive had changed the scale of the threat of extortion by cybercriminals [16]. This change has been reflected in the way members of Russian underground forums talk about these activities.

2 Background

This paper is condensed from the first part of a working paper analyzing the Cambridge Cybercrime Centre's Russian hack forum archive from 2002 to 2021.

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

We explore discussions between 2005 and 2009, before what Fuentes et al. [12] term the development of "local and regional capabilities" in ransomware. We refer to this period as the **Post-Romantic Era**, in recognition of the shift from "hobby hacking" to for-profit cybercrime. From 2005 to 2009 we find this shift is evident in forum discussions. This paper was inspired by Bada and Pete's [3] analysis using Shodan as a focus, as well as Collier et al.'s [6] analysis of infrastructure and alienation in hacker subculture. Lusthaus [17] works towards a comparable goal using interviews. Johnson et al. [15] provide a glimpse of the expanded cultural life of forum members during the COVID-19 pandemic. The threat posed by ransomware is well documented, but as Connolly and Wall [8] explained in their 2019 study of the views of victims and law enforcement, most of the literature is from a technical perspective. The evolution of ransomware itself has been outlined [12,8,10,19,11] including the change from hobby hacking [10] into today's large-scale international cyberattacks with seven-figure pricetags. There have also been multiple analyses of the criminal underground [3,7,2,18,4,13]. What is lacking is an analysis of the evolution of cybercriminal extortion from the point of view of the Russian online hacker community.

3 Methods

The central question of this paper is: how was the change from hobby hacking to for-profit cybercrime [12] reflected in Russian underground forum discussions from 2005 to 2009? To answer this question we carried out a qualitative thematic analysis [9] of threads in two Russian-language underground forums. The Russian word for "ransomware" is "программа-вымогатель". "Вымогател-" is the stem for "вымогательство" ("extortion") and "вымогатель" ("extortionist"), and we used it as an inspirational sampling filter over the entire archive. We also searched on the English "ransom-" and its Cyrillic version, "рансом-", but the latter term produced no results from 2005—2009. We limited the search to those three keywords in order to return fewer results and maintain capacity for a close narrative reading. Because extortion is a fundamental goal of cybercrime, the keyword appears in threads discussing a wide range of topics, not only ransomware. By incorporating the forum members' discussions of topics that were not task-oriented, we had access to a richer picture of their concerns.

Data. We searched the entire archive of Russian-language forums in the CrimeBB dataset [18]. This dataset is available to academic researchers through data sharing agreements with the Cambridge Cybercrime Centre (CCC). Specifically, we analysed Antichat (AC) from 2002 to 2009 (97,454 threads), and XSS from 2004 to 2009 (7,837 threads). In 2005 our keywords began to appear. The majority (85%) of threads from the post-Romantic era that contain the keywords are from AC (81), with 15% (14) from XSS. This era has the smallest proportion of relevant threads in the CCC's archive. The threads were read by a non-native Russian speaker from a flat file with a parallel English translation using Google Translate for convenience, not as a substitute for Russian reading comprehension, as the English translation was unintelligible without the Russian

original. Threads were broadly categorised, then assigned to narrower topics one post at a time. The close narrative reading of every post provided an important foundation for understanding a time period that set the conditions for what followed.

Exclusion criteria and "off-topic" threads. Seemingly "off-topic" threads, unrelated to cybercrime, were among the most informative about the forum members' experiences from 2005 to 2009. However, the words "вымогательство" and "вымогатель" were often used offhandedly to mean simply "rip-off" or to accuse someone of dishonesty; these usages of the keyword were excluded.

Ethical considerations. We obtained approval from the departmental ethics committee. CrimeBB is scraped from publicly available posts on open forums [21]. Details which could identify individuals are excluded, and quotes from members' posts have been rephrased, paraphrased or summarised.

Scope and limitations. As explained in **Data**, our search terms were limited, so the results returned may not be representative of the coverage of relevant topics within the archive. We do not describe specific techniques of extortion or ransomware.

4 Findings

A complete listing of topics in descending order of text volume with keyword counts is shown in Table 1. We will discuss the most informative examples here.

4.1 Themes

Romance Is Dead. Following the July 2005 article declaring the decline of the romantic hacker, a January 2006 article quotes the founder of the anti-virus company Kaspersky Labs on the change from "purely hooligan" hacking 10 years previously; whereas a June 2006 article claims that ideology had been the main motivation. A 2007 discussion post on AC, in which a member was torn between their conscience and the prospect of earning USD 400 from ***Social Engineering***, elicited a response that "hacking is not a source of income, but a lifestyle".

Usage of the Keywords to Denote Malware. The first appearance of one of the keywords to denote ***Viruses*** was in January 2006, when a press article used "троян-вымогатель" ("extortion trojan") to describe the Krotten worm. The term appears again in 2008, describing Trojan.Encoder.19. The term "программа-вымогатель" appears several times in a number of 2009 press articles. One, about the growth of the ***RuNet***, calls the Blackmailer trojan a "вирус-вымогатель" ("extortion virus"). Another warns of ***Fake Antivirus*** software. The keyword appears in 2009 in the multi-year XSS thread swapping ***Virus Source Codes***, describing CMedia, which created porn banners requiring an SMS payment to suppress. An "CMC-вымогатель" ("SMS-extortionist") was offered ***For Sale*** for 30 WMZ (USD in WebMoney). The first instance of ***Calling A Ransomware A Ransomware*** was in 2006, with the appearance of

the word "ransom" in an article mentioning Ransom.A. "Ransom" next appeared in December 2009, in a brace of articles about Win32/RansomSMS.AH, which targeted Russian users.

Informative Mentions of Extortion. The second biggest topic by text volume was ***Getting Caught***. The first appearance of the stem "вымогател-" in this topic was in the relevant statutes of the Criminal Code of the Russian Federation, which are quoted in three threads in both forums over the years. The first was on XSS in 2005, continuing with discussion in January 2006, including members' experiences of brushes with the law, which resulted in some "small" fines. Sentencing guidelines give an idea of what there was to lose. Russia's national average wage was RUB 8,854.90 (USD 310.92)[3] per month; and the subsistence minimum, RUB 3,255.00 (USD 114.29) [5]. Besides imprisonment or corrective labour, fines ranged from RUB 20,000 (USD 702.25), or 2.26 times the average wage; to RUB 1,000,000 (USD 35,112.36), or 112.94 times the average wage; or more, proportionate to the offender's income. Most of the material on ***Getting Caught*** consisted of press articles about international and domestic arrests. The Russian press covered a 2006 case of extortion from a Kaliningrad software company of USD 10,000 (RUB 284,800), paid in instalments of USD 1,000 (RUB 28,480), an amount that forum members judged to be not worth the risk. However, there were reports of Russian hackers getting caught for much smaller amounts. 2008 and 2009 saw reports of blackmail through breached Odnoklassniki accounts, such as an administrator who demanded RUB 5,000 (USD 175.56) after hacking a girl's photos. The last thread of 2009 described a student in Omsk who demanded USD 130 (RUB 3,702.40) to release a blocked mailbox. A domestic case that came up repeatedly was described by a blog post entitled "Crime and Punishment", shared on both forums in October 2006. Three young Russians were sentenced to eight years for hacking a British bookmaker, and the blogger argued passionately that the accused had been made an example of on scant evidence. The "Crime and Punishment" case comes up repeatedly during this time period, including in a press article in the same year, reporting that the Ministry of Internal Affairs (MIA) had declared a hard line on ***Cybercrime***. In 2007, a long read by the same blogger, on ***Cybersecurity*** for hackers, elicited over two hundred responses, ending with a pointed question about whose interests are served by having so many hack forums on the open RuNet.

Recovery. In 2006, a teenager appealed to XSS for help after (apparently) hacking a forum and facing demands for RUB 2,000 and threats to report their unpaid Internet license. Forum members dismissed this as a small sum and told the teenager to get a job such as leafletting in the metro for RUB 150—200 per day. A member from the provinces sympathised that they earned RUB 4,000 per month – not much more than minimum subsistence.

Earning Money Legally. The earliest posts in the archive are from May 2005, discussing the viability of forming a cybersecurity startup. Someone expresses skepticism that anyone in the former USSR would pay for cybersecurity

[3] `https://freecurrencyrates.com/en/exchange-rate-history/USD-RUB/2005/cbr`

when hiring thugs would be cheaper. Another muses that customers are more willing to pay to breach a site than to secure their own; though they name some successful companies, including Positive Technologies. Finally, someone suggests breaching potential customers' sites as a marketing tactic. A 2006 press article mentions in passing that there is no market in Russia for the skills of exceptional coders like the Russian winner of that year's Global Code Jam, who captured the first prize of USD 10,000. The article quotes one of the founders of the RuNet as saying that Russians did *not* get good at coding through illegal hacking, because Russians were rarely convicted of serious crimes (with exceptions, like the "Crime and Punishment" case). One comment stands out amid the outpouring of national pride: "So happy for the guy to be able to earn USD 10,000 honestly. I hope this makes Putin think."

Russian Cybercrime. A 2008 article reports a trial in Sweden of over 150 Russian and ex-USSR immigrants for large-scale Internet fraud. In response to European experts' claims that Russian authorities are uncooperative, the MIA points to the "Crime and Punishment" case. Comments observe that that case is three years old, and the MIA can provide no examples since then. A 2009 article quotes Kaspersky describing this lack of international cooperation as the reason why Russia is a "paradise" for cybercriminals. A member retorts that they would rather live in a paradise for citizens.

Off-Topic but Informative Discussions. A thread on ***Holiday Planning*** gives some clues about the kind of money the forum members considered reasonable for this kind of nonessential spending. The OP has a total budget of RUB 1,000 per person (USD 39.28) per day, on the Black Sea coast in Abkhazia or Crimea. This seems proportionate to the 2007 average wage of RUB 13,527.40 per month [5].

Computer Science Education in Russia. A CS student at a university in a major Russian city invited questions. One member wanted to know if they could study there despite having no money. The student replied that they had never encountered any instances of extortion, that there were no bribes to pay, and that there was no point bribing staff because they would take the money and provide the same service anyway.

5 Conclusion

The years 2005—2009 set Russian cybercrime on its path to becoming the global-scale threat it is today. The path is traceable through forum discussions, but the most revealing posts were about seemingly unrelated topics. Whatever the sources of income of members of these hack forums, discussions of ***Holiday Planning*** give clues about how those incomes compared to the national average by the midpoint of 2007. Discussions also point to corruption and poverty as barriers to access to formal ***Russian CS Education***, to a perception of poor prospects for ***Earning Money Legally***, and to a perception of relative impunity

that might have made ***Russian Cybercrime*** look like the career path of least resistance.

Acknowledgments. Thanks are due to the Cambridge Cybercrime Centre for allowing the use of the CrimeBB dataset. This work was supported by Engineering and Physical Sciences Research Council [grant number EP/V026178/1] from 2020-2021. This work has not been peer reviewed. For the purpose of open access, the authors have applied a Creative Commons Attribution (BY-NC-ND) licence to any Author Accepted Manuscript version arising. Most of all, we thank Ross.

Disclosure of Interests. The authors have no competing interests.

References

1. Lawrence Abrams. "US Recovers Most of Colonial Pipeline's $4.4M Ransomware Payment", June 2021. URL `https://www.bleepingcomputer.com/news/security/us-recovers-most-of-colonial-pipelines-44m-ransomware-payment/`. Bleeping Computer.
2. Sadia Afroz, Vaibhav Garg, Damon McCoy and Rachel Greenstadt. "Honor Among Thieves: a Common's Analysis of Cybercrime Economies". In *Proceedings of the 2013 APWG eCrime Researchers Summit*, eCRS 2013, pages 1–11. IEEE, New York, NY, 17–18 September 2013 2013. `https://doi.org/10.1109/eCRS.2013.6805778`.
3. Maria Bada and Ildiko Pete. "An Exploration of the Cybercrime Ecosystem Around Shodan". In *Proceedings of the 2020 7th International Conference on Internet of Things: Systems, Management and Security*, IOTSMS 2020, pages 1–8. IEEE, New York, NY, 14 December 2020 2020. `https://doi.org/10.1109/IOTSMS52051.2020.9340224`.
4. Rasika Bhalerao, Maxwell Aliapoulios, Ilia Shumailov, Sadia Afroz and Damon McCoy. "Mapping the Underground: Supervised Discovery of Cybercrime Supply Chains". In *Proceedings of the 2019 APWG Symposium on Electronic Crime Research (eCrime)*, eCrime 2019, pages 1–16. IEEE, New York, NY, 13–15 November 2018 2019. `https://doi.org/10.1109/eCrime47957.2019.9037582`.
5. Anna Bolsheva. "Minimum Wage Development in the Russian Federation". Technical Report Global Labour University Working Paper 15, International Labour Organization (ILO), Geneva, 12.
6. Ben Collier, Richard Clayton, Alice Hutchings and Daniel R. Thomas. "Cybercrime Is (Often) Boring: Infrastructure and Alienation in a Deviant Subculture". *The British Journal of Criminology*, **61**(5):1407–1423, 2021.
7. Lena Y. Connolly, Michael Lang, Paul Taylor and Phillip J. Corner. "The Evolving Threat of Ransomware: From Extortion To Blackmail". Unpublished, 2021.
8. Lena Y. Connolly and David S. Wall. "The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures". *Computers & Security*, **87**:1–18, 2019.
9. Juliet Corbin and Anselm Strauss. "Grounded Theory Research: Procedures, Canons, and Evaluative Criteria". *Qualitative Sociology*, **13**(1):3–21, 1990.
10. Srinivasan CR. "Hobby Hackers to Billion-Dollar Industry: the Evolution of Ransomware". *Computer Fraud & Security*, **11**, 2017. `https://doi.org/10.1016/S1361-3723(17)30081-7`.

11. Andrada Fiscutean. "A History of Ransomware: the Motives and Methods Behind These Evolving Attacks", July 2020. URL https://www.csoonline.com/article/3566886/a-history-of-ransomware-the-motives-and-methods-behind-these-evolving-attacks.html/. CSO Spotlight.
12. Mayra Fuentes, Feike Hacquebord, Stephen Hilt, Ian Kenefick, Vladimir Kropotov, Robert McArdle, Fernando Mercês and David Sancho. "Modern Ransomware's Double Extortion Tactics and How To Protect Enterprises Against Them". Technical report, Trend Micro, 2021.
13. Alice Hutchings and Sergio Pastrana. "Understanding eWhoring". In *Proceedings of the 2019 IEEE European Symposium on Security and Privacy*, EuroS&P, pages 201–214. IEEE, 17–19 June 2019 2019. https://doi.org/10.1109/EuroSP.2019.00024.
14. Ionut Ilascu. "Colonial Pipeline Restores Operations, $5 Million Ransom Demanded", May 2021. URL https://www.bleepingcomputer.com/news/security/colonial-pipeline-restores-operations-5-million-ransom-demanded/. Bleeping Computer.
15. Erin Johnson, Vladimir Kropotov and Fyodor Yarochkin. "Cybercriminals Gamble With Victims' Livelihoods to Pass the Covid-19 Blues", 2020. URL https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminals-gamble-with-victims-livelihoods-to-pass-the-covid-19-blues/. Trend Micro Security News.
16. Brian Krebs. "A Closer Look at the DarkSide Ransomware Gang", May 2021. URL https://web.archive.org/web/20210511164739/https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/. Krebs on Security.
17. Jonathan Lusthaus. *Industry of Anonymity: Inside the Business of Cybercrime*. Harvard University Press, Cambridge, MA, USA, 2018.
18. Sergio Pastrana, Daniel R. Thomas, Alice Hutchings and Richard Clayton. "CrimeBB: Enabling Cybercrime Research on Underground Rorums at Scale". In *Proceedings of the 2018 World Wide Web Conference on World Wide Web*, WWW '18, TheWebConf, pages 1845–1854. ACM Press, New York, NY, 23–27 April 2018 2018. https://doi.org/10.1145/3178876.3186178.
19. Ronny Richardson and Max M. North. "Ransomware: Evolution, Mitigation and Prevention". *International Management Review*, **13**(1):10–21, 2017.
20. Aleksandr Sery. "Gentlemen of Fortune". Film, 1971. Mosfilm: Moscow (1971).
21. Kieron Ivy Turk, Sergio Pastrana and Ben Collier. "A Tight Scrape: Methodological Approaches to Cybercrime Research Data Collection in Adversarial Environments". In *Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops*, EuroS&PW, pages 428–437. IEEE, 7–11 September 2020 2020. https://doi.org/10.1109/EuroSPW51379.2020.00064.

Table 1. Topics in descending order of total text volume

Topic	Years	Forums	Threads	Posts	"вымогател-"	"ransom-"
1. New Releases	2009	AC	1	222*	2*	0
2. Getting Caught	2005, 2006, 2008, 2009	AC, XSS	9	317*	51*	0
3. Reputation	2008, 2009	AC	2	732	2	0
4. Cybercrime	2005, 2006, 2009	AC	8	18*	9*	0
5. Recovery	2006, 2009	AC, XSS	5	185	9	0
6. Consumer Rights	2006, 2009	AC, XSS	2	139	3	0
7. DDoS	2006, 2008, 2009	AC, XSS	5	83	8	0
8. Cyberattacks	2006, 2009	AC, XSS	3	37	5	0
9. Viruses	2006, 2008, 2009	AC	8	62	12	0
10. Murder	2008	AC	1	131	1	0
11. Electronic Wallets	2008	AC	1	127	1	0
=12. Corruption	2006	AC	2	2	2	0
=12. RuNet	2009	AC	1	5	1	0
13. Earning Money "Legally"	2007	AC	1	22	1	0
14. Romance Is Dead	2005, 2006, 2007	AC, XSS	4	15	7	0
15. Earning Money Legally	2005, 2006, 2008	AC	4	39	3	0
16. Social Engineering	2009	AC	1	61	1	0
17. Cybersecurity	2006, 2007, 2008	AC, XSS	3	9	3	0
18. Russian Cybercrime	2008, 2009	AC	2	51	3	0
19. Cyberterrorism	2008	AC	1	36	2	0
20. Romance Scams	2007	AC	2	20	3	0
=21. Fake Antivirus	2008, 2009	AC	2	34	4	0
=21. Self-Defence	2006	XSS	1	37	1	0
22. Holiday Planning	2007	AC	1	34	1	0
23. Virus Source Codes	2006, 2008, 2009	XSS	1	76	1	0
24. Scams	2008	AC	1	33	1	0
25. Calling A Ransomware A Ransomware	2006, 2009	AC	2	21	1	17
=26. Social Networking	2008	AC	1	36	1	0
=26. Security Tutorial	2006	XSS	1	13	1	0
=27. Hacker Economy	2007	AC	1	11	2	0
=27. Internet Fraud	2009	AC	1	2	1	0
28. Hacker Culture	2006	XSS	1	32	1	0
29. For Sale	2009	AC	2	25	4	0
=30. Russian CS Education	2009	AC	1	12	1	0
=30. Birthdays	2009	AC	1	56	1	0
31. Critique of Russian Society	2009	AC	1	9	2	0
=32. Offering Nonexpert Advice for Legal Issues	2008	AC	1	13	2	0
=32. Group Project Ideas	2009	AC	1	14	1	0
33. Software Costs	2006	AC	1	8	1	0
34. ICQ Hacking	2006	AC	1	4	1	0
=35. Viruses Written By Forum Members	2009	AC	1	6	1	0
=35. Want Ads	2008	AC	1	5	1	0

Transparent Truths: Critical Friends and Coordinated Disclosure

Alice Hutchings[0000-0003-3037-2684]
and Alastair R. Beresford[0000-0003-0818-6535]

University of Cambridge, UK
{ah793, arb33}@cam.ac.uk

Abstract. This paper compares the process of coordinated disclosure, through which technical vulnerabilities in software are disclosed, to the role of a *critical friend* who provides a constructive critique of a system or service. Both contribute by identifying flaws, fostering trust and improving resilience. Both systems also have many challenges, from incentivising action, balancing transparency and security, and managing relationships. We find many similarities between these two approaches and aim to improve our understanding of both.

Keywords: Critical friends · Coordinated vulnerability disclosure · Transparency · Security.

1 Introduction

In computer security, a third-party perspective is important when it comes to testing system security. Alternative viewpoints are also important more generally in civil society and business. Those who adopt this role might be considered critical friends, who identify real or potential concerns about policies or practices.

Those who find security vulnerabilities in software systems face a choice of what to do. They may keep a vulnerability secret, perhaps for their own amusement or exploitation; report it to the company or person responsible for the software; disclose it publicly [1]; or sell it on the underground market [6]. A high-profile example is the EternalBlue exploit used in the WannaCry ransomware that devastated the NHS in 2017 [11]. This exploit was kept secret by the NSA rather than disclosed; the exploit was then stolen from the NSA and leaked by The Shadow Brokers, an online hacking group whose identity remains unknown.

Coordinated disclosure refers to the process of first making a disclosure on a confidential basis to those that are able to remedy or mitigate the impact of the vulnerability, followed by public disclosure after a period of time has elapsed. The motivation for coordinated disclosure is to incentivise quick mitigation, and 90 days has emerged as the typical confidential period. An example of coordinated disclosure is the 2014 Heartbleed bug, which was communicated to the OpenSSL team and other key insiders to prepare fixes before the problem was announced publicly [5]. The Meltdown [9] and Spectre [8] vulnerabilities are also

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

high profile examples, discovered in mid-2017 and disclosed in January 2018. Notably, the embargo period was almost double the standard 90 days typically provided by Google's Project Zero [2] vulnerability discovery team. In other instances Project Zero have resolutely stood by the 90-day frame, famously disclosing vulnerabilities despite Microsoft not having released a patch in time [3].

There are various ways the power of industry, government, and the elite are kept in check to prevent abuses and promote accountability in democratic societies. These mechanisms include regulatory frameworks, legal systems, oversight institutions, whistleblowing, and media scrutiny. These mechanisms often require civil society to actively challenge actions. Tenured academics are often perceived to be relatively neutral and independent and therefore often play a key part in this process. We may think of such people as *critical friends*, a term that has its origins in education. By providing both critical and supportive responses, it allows the recipients to evaluate their work, leading to higher order thinking [4].

The aim of a critical friend is to question those in authority, often raising concerns that may negatively affect the less powerful. The main raw material of a critical friend is evidence so good access to evidence is important. Evidence can be used to provide engagement with key stakeholders, and a critical friend can use evidence to provide motivation and capability for change. Evidence is enhanced by a critical friend through analytic capacity, theoretical insight, and the ability to critique.

2 Incentivising action

Computer security researchers have traditionally found it difficult to persuade companies to fix vulnerabilities in their systems. This has led to coordinated disclosure, where information is provided in confidence for a limited period, after which it is disclosed publicly. This approach incentivises all participants: the owner of the affected software system has a period to prepare an update to fix the issue; the user receives an software update before the flaw has been exploited by an adversary; and the researcher receives public credit once the embargo period has ended.

Similar challenges may arise for critical friends who may be ignored when raising concerns directly. However, without access to an agreed disclosure process, they need to look to other ways to initiate action. The most overt actions of a critical friend are publishing rigorous evaluations and engaging with the media. Depending on the issue at hand, there may be concerns that going public may cause further harm, through public backlash or reactionary knee-jerk responses. For those who enjoy it, academic freedom can be critical in this process.

3 Rewards and recognition

While researchers receive public credit for taking part in coordinated disclosure, there are alternatives: researchers may choose to exploit vulnerabilities directly or sell them on. To encourage engagement with the disclosure process, many

software vendors run bug bounty programmes which offer a financial reward for reporting issues. For example, Google and Apple both offer up to $1m for the most serious vulnerabilities in Android and iOS respectively. These prices remain significantly below those available from grey market vendors who buy zero-day exploits and distribute them to selected adversaries (see §6). For example, Zerodium offer up to $2m for vulnerabilities in iOS; $2.5m for Android. In a competitive market, prices provide insight into software (in)security. A high price suggests vulnerabilities for a system or application are rare or hard to discover, indicating good security. Conversely, low prices, or no bug bounty programme may signal widespread vulnerabilities and poor security hygiene.

The market price attached to a vulnerability depends on the value which may be extracted by an adversary, which in turn is limited by the number of targets which may be successfully infiltrated. Whenever a vulnerability is used to exploit a software system, there is the possibility that its use is discovered due to crashes, logs or other unusual behaviour which are noticed by the user directly or software and systems they use to monitor the secure operation of their devices. Once discovered, the vulnerability may be reported to a vendor who then fixes the flaw, rendering the vulnerability useless. Consequently there's a natural equilibrium: compromising more systems may generate more value for the adversary, but may shorten the period of time the vulnerability functions.

Despite this, there remains a differential in the fees payable under a bug bounty programme and the grey market or underground market (see $1m vs $2m-$2.5m above as an example). Part of this may be a moral choice: researchers may feel it is their duty to take part in a disclosure process. Other benefits arise from disclosure: academic researchers may publish papers describing new types of vulnerability; and industry professionals may enhance their public reputation through blog posts or talks on their work at major conferences.

Critical friends often work without explicit reward. Their contributions are driven by powerful intrinsic motivations. They are able to use their experience to learn about policy contexts, develop new collaborations, increase motivation and capability to engage, and develop an awareness of tensions and trade-offs.

4 Balancing transparency and security

Coordinated disclosure is a delicate balance between transparency and security, in which time plays a major role. Timely fixes are encouraged by reporting the vulnerability with a set amount of time before publication. Public disclosure not only ensures that a fix is produced, but it also encourages remediation because awareness ensures patches are installed promptly. Public disclosure also provides recognition and builds a body of work which informs the security and practitioner community: ideally past mistakes are avoided in future and industry undertakes proactive steps to look for similar errors in other software systems.

There are still a number of open debates about how to handle vulnerability disclosures responsibly. For example, what is the appropriate length of time between private and public disclosures? Should disclosures be published if the

vulnerability is yet to be fixed, or no effort is made to fix it? In some cases, the courts have been consulted. In 2013, Volkswagen started legal proceedings against academic researchers and their universities to block the publication of vulnerabilities affecting their vehicle locking systems. The researchers had given Volkswagen six months to fix the issues they identified. It took two years for the courts to rule against Volkswagen [13]. In effect, the court case process extended the embargo period for Volkswagen from six months to two years. It remains to be seen if injunctions like this will be misused more broadly to delay reports.

Bug bounty programmes are not without their challenges. In 2022 the former Chief Security Officer for Uber was convicted of obstructing justice for failing to report a data breach to the US Federal Trade Commission. The charges related to a data breach in 2016 where attackers stole data and then threatened to publish it unless a ransom was paid. The CSO misused the bug bounty programme to authorise payments to the attackers [7].

Effective critical friends can increase awareness of and reframe issues to influence ways of thinking. Often, critical friends will directly initiate the engagement with policy makers and companies. Perhaps less frequently, a critical friend may be invited to the table, sitting on boards and committees. This level of transparency and openness is sometimes difficult for organisations to grapple with. In a notable example, Google shut down its Advanced Technology External Advisory Council after just two weeks, after employees petitioned against one of the appointees, and another board member resigned [14]. Likewise, the UK Government's Centre for Data Ethics and Innovation's Advisory Board was quietly shut down while the Sunak government was simultaneously pushing to become a world leader in AI governance [10].

5 Relationships

The relationship of actors in the coordinated disclosure process can be seen as transactional. Bug bounty teams may collaborate closely, and some may even take on the role of a trade union [12]. The interactions between researchers and companies is mostly cooperative and involves payment in exchange for reports as well as other forms of reward and recognition. Occasionally the relationship is more confrontational, where those reporting vulnerabilities are not recognised as contributors. In the example of Volkswagen earlier, researchers were treated as enemies to be fought in a court of law, so reporting vulnerabilities sometimes come with legal risks.

Critical friends are typically independent, free to speak their minds without concern for their status. However, core tensions arise when it comes to navigating politics. In many cases, decisions are not just a matter of evidence. Roles, interests, problem framings, cultures, priorities and values, timelines, capacities, and processes also affect how decisions are made. Governments and companies may be less willing to engage with those who do not understand these, and who are critical of their approaches, leading to perceptions of rubber stamping and cronyism. When the emphasis is on the *friend*, it requires a relational approach,

building trusted relations and shared ownership. There are inherent tensions between the idea of being a friend and being critical that are difficult to reconcile.

6 Adversaries

A key difference between coordinated disclosure and critical friends relates to the presence of third party adversaries. Critical friends provide constructive feedback, support, and scrutiny to help improve internal policies and practices. On the other hand, coordinated disclosure involves defenders preventing external adversaries from successfully carrying out malicious acts.

Sometimes vulnerabilities are not fixed, as they are not disclosed to the company or individual that can fix them. Undisclosed vulnerabilities are sometimes discovered or acquired by nation states, security agencies and police forces. These vulnerabilities are then used to obtain access to computer devices, often remotely, and without the user's knowledge. This is done either by developing in-house expertise, or purchasing *spyware* from commercial suppliers such as Pegasus from NSO Group or FinFisher from Gamma Group. Since finding vulnerabilities used to carry out such operations are difficult (and therefore expensive as well as time-consuming), they are carefully guarded and used sparingly.

There are good reasons for both governments as well as commercial suppliers to limit access to spyware which weaponise vulnerabilities as a tool to manipulate computer systems without users' consent or knowledge. The most obvious reason is to prevent the harm which would otherwise occur: spyware and indeed the cyber-arms trade more generally must be regulated and controlled.

There is also a less obvious reason: if the rate at which vulnerabilities are discovered and patched exceeds the rate at which such vulnerabilities can be found, then no usable vulnerabilities will remain; the spyware no longer works. As a result, the use of spyware by government or commercial supplier has a natural limit—if it is deployed on too many devices, its usage is detected too frequently, and the vulnerabilities the spyware relies on are fixed faster than new vulnerabilities are discovered. This natural limit on the usage of spyware is good news for society: the number of members under surveillance is limited. Nevertheless, as a society we may worry if this technology is used for the right purpose. Is it used to thwart terrorism and investigate serious organised crime, or is it used to threaten free speech or intimidate journalists?

7 Conclusion

Coordinated disclosure is a response to technical vulnerabilities affecting computer systems, while critical friends find intellectual vulnerabilities, such as flaws in methodology, biases, or ethical oversights, that affect society. There are key differences between the two. Coordinated vulnerability disclosure leads to more transactional relationships between bug bounty hunters and developers, while critical friends often (but not always) have a more collaborative approach. Despite their differences, we argue both are essential for fostering transparency

and accountability, and their relevance is more pertinent than ever. Societal and technical systems are increasingly necessary for daily life, but as their complexity increases, they also become more fragile, leading to frequently arising challenges.

Acknowledgments. This paper is part of a project that has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 949127) (for AH). This paper is inspired by the late Professor Ross Anderson, our colleague and ally, who taught us much about critical friendship and security vulnerabilities.

Disclosure of Interests. The authors have recently received donations to support their research from Google (AH, ARB), Meta (AH) and Nokia Bell Labs (ARB).

References

1. Nicholas Boucher and Ross Anderson. "Talking trojan: analyzing an industry-wide disclosure". In *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses*, pages 83–92. 2022.
2. Russell Brandom. "Keeping Spectre secret: How an industry-breaking bug stayed secret for seven months — and then leaked out", 2018. URL `https://www.theverge.com/2018/1/11/16878670/meltdown-spectre-disclosure-embargo-google-microsoft-linux`.
3. Catalin Cimpanu. "After Microsoft delayed Patch Tuesday, Google discloses Windows bug", 2017. URL `https://www.bleepingcomputer.com/news/microsoft/after-microsoft-delayed-patch-tuesday-google-discloses-windows-bug/`.
4. Arthur L Costa and Bena Kallick. "Through the lens of a critical friend". *Educational Leadership*, **51**:49–49, 1993.
5. Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey *et al.* "The matter of heartbleed". In *Proceedings of the Internet Measurement Conference*, pages 475–488. 2014.
6. Serge Egelman, Cormac Herley and Paul C Van Oorschot. "Markets for zero-day exploits: Ethics and implications". In *Proceedings of the 2013 New Security Paradigms Workshop*, pages 41–46. 2013.
7. Tom Gerken. "Ex-Uber security chief sentenced over covering up hack", 2022. URL `https://www.bbc.co.uk/news/technology-65497186`.
8. Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher *et al.* "Spectre attacks: Exploiting speculative execution". *Communications of the ACM*, **63**(7):93–101, 2020.
9. Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom *et al.* "Meltdown: Reading kernel memory from user space". *Communications of the ACM*, **63**(6):46–56, 2020.
10. Alexander Martin. "British government quietly sacks entire board of independent AI advisers", 2023. URL `https://therecord.media/uk-disbands-ai-advisory-board-cdei-rishi-sunak`.
11. National Audit Office. "Investigation: WannaCry cyber attack and the NHS", 2018. URL `https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/`.

12. Yangheran Piao, Temima Hrle, Daniel Woods and Ross Anderson. "Study Club, Labor Union or Start-Up? Characterizing Teams and Collaboration in the Bug Bounty Ecosystem". In *IEEE Symposium on Security and Privacy (SP)*, pages 20–20. 2024.
13. Roel Verdult, Flavio D Garcia and Baris Ege. "Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer". In *Supplement to the Proceedings of 22nd USENIX Security Symposium*, pages 703–718. 2015.
14. Jane Wakefield. "Google's ethics board shut down", 2019. URL `https://www.bbc.co.uk/news/technology-47825833`.

Rational Astrologies and Security

John Kelsey[1,2] and Bruce Schneier[3]

[1] National Institute of Standards and Technology
[2] COSIC/KU Leuven
[3] Harvard Kennedy School

1 How do we spend our security budget?

For any product or system, a certain set of resources is dedicated to security. We can think of this as the system's *security budget*. This includes things easily translated into money (good locks, an alarm system with a monitoring contract, a security guard's salary), but also more abstract things like extra hassle for users of the system, or time to market.

One lesson we have learned, in our many years working in security, is that designers spend a lot of the security budget on things *other* than security. Of course, they spend most of the security budget on making attacks harder. But they spend more of the security budget than we like to admit on other things that *look* like security, but actually aren't.

In 2003, Schneier coined the term *security theater* [10] to describe security measures that provide the feeling of improved security while doing little or nothing to actually achieve it. A classic example of security theater was the stationing of unarmed National Guard troops in US airports in the months after the 9/11 terrorist attacks. It is difficult to see how this made air travel safer or terrorism less likely, but people may have found the guardsmen a reassuring presence in an uncertain time. In general, security theater involves spending some of the security budget on user interface or marketing. Users feel more secure, even though they aren't.

There is another non-security way that designers can spend their security budget: on making their own lives easier. Many of these fall into the category of what has been called *rational astrology*. First identified by Randy Steve Waldman [13], the term refers to something people treat as though it works, generally for social or institutional reasons, even when there's little evidence that it works—and sometimes despite substantial evidence that it does not.

Waldman writes:

> *A rational astrology is a set of beliefs which one rationally behaves as if were true, regardless of whether they are in fact. Rational astrologies need not be entirely fake or false... Some rational astrologies may turn out to be largely true, and that happy coincidence can be a great blessing. But they are still a rational astrologies to the degree the factors that persuade us to behave as though the beliefs are true are not closely related to the fact of their truth.*

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

Waldman's examples include the penchant for buying the same tech that everyone else is buying, hiring people with degrees from elite colleges, and undergoing the same marginally effective medical treatments as everyone else. These are all rational choices because going against conventional wisdom is both more costly and brings with it more risks.

In security, rational astrologies take many forms. They can involve design decisions that are easily defended to management (example: using the market-dominant security product even if it doesn't improve security much), protecting designers from bad consequences in case the system is attacked (example: finding some external standard to follow), or simply applying common security mechanisms in places where they do little good (example: requiring complex password rules when passwords are stored in the clear on the server). Sometimes, a rational astrology involves a measure that purports to address some unsolvable problem (example: lie detectors). In economic terms, security theater is often a result of information asymmetry, whereas rational astrology in security is often the result of a principal–agent problem.

There are many examples of rational astrologies in modern-day internet security, and recognizing these can make us better at understanding both security and the organizational dynamics that lead to a lot of wasted effort in trying to secure important systems.

2 A Taxonomy of Rational Astrologies

Some examples of rational astrologies that lead designers of secure systems to spend some of their security budget on non-security things appear below. This is certainly not a complete list!

Justifiability (*"Nobody ever got fired for buying IBM."*)

Some security decisions are easy to justify to management, auditors, or the public. Choosing an easy-to-justify measure over a better one that is harder to justify is one way to spend some of the security budget on designer convenience.

Many organizations require FIPS validation for products they use to do cryptography. It is not entirely clear how much the FIPS validation process actually results in more secure devices, though it likely has some benefits. But much of the value of FIPS validation is not about these benefits, but rather about the *institutional* benefit of being able to demonstrate that the expected level of precautions are being taken.

Many organizations have password complexity rules derived from old NIST guidance: eight or twelve characters, upper/lower/symbol/digit. These are often enforced even when they don't apply: when the underlying system stores passwords in the clear, or when access is only online (and so making password-cracking attacks harder is pointless) [6]. Even where off-line attacks are possible, allowing longer passphrases would almost certainly be more secure. But it is easier to follow the commonly used requirements, even when they make no sense, than to argue for more sensible ones.

There are good reasons for developers to use cryptographic standards rather than roll their own cryptography. However, there are also a great many sketchy or poorly studied algorithms that have become standardized. In classic rational astrology fashion, it's better for almost anyone to choose one of these standard algorithms—even tricky-to-use ones like CBC-mode encryption—than to invent their own. The developer can justify this decision to his management, and may hope to escape blame if something goes wrong—after all, he followed the standard, what else was he supposed to do?

Least Bad Option (*"Something must be done. This is something. Therefore, this must be done."* [3])

Sometimes the available security solutions to a particular problem are not much use. However, the designer or his employer feels the need to address the problem *somehow*. In this case, part of the security budget may be spent on futile measures meant to solve an unsolvable problem. (This is probably the closest to Waldman's original meaning of rational astrologies.)

An example of this is the widespread use of lie detector tests. Lie detector tests are probably not all that accurate or effective in screening for problem employees [4,5] (either before or during employment), but they meet an institutional need for security agencies. So they continue to be widely used, spending a chunk of those agencies' security budget on something that probably does little good.

Another example of this is security training for users to avoid online scams. It is often difficult to tell how much benefit this training has [7], but the persistence of successful phishing attacks, sometimes on very high-profile targets, suggests that these mandatory training sessions may not be bearing much fruit. But again, these meet an institutional need, allowing the institution to claim that they've done all they could to prevent such attacks.

Bureaucratic Inertia (*"It's always been done this way."*)

Sometimes a regulation or organizational policy requires some security measure that once made sense, but no longer does. In this case, part of the security budget is being spent by an organization or standards body not bothering to update requirements or procedures to keep up with the times.

For example, antivirus software is often required by standards or company policy, but may not really do much good at this point. But since it has been required for so long, no one wants to risk their credibility or career by arguing that it is no longer useful.

Financial and business records used to be stored on paper, which created a difficult-to-modify record. Most financial and business records are now stored electronically , but procedures assuming the "paper" record represents ground truth persist. A similar issue arose in the past when some countries tried to move from paper to electronic ballots—there was no permanent difficult-to-change record of the voter's intention.

3 Discussion

Both security theater and rational astrologies may seem irrational, but they are rational *from the perspective of the people making the decisions about security.*

Security theater is often driven by information asymmetry: people who don't understand security can be reassured with cosmetic or psychological measures, and sometimes that reassurance is important. It can be better understood by considering the many non-security purposes of a security system. A monitoring bracelet system that pairs new mothers and their babies may be security theater, considering the incredibly rare instances of baby snatching from hospitals. But it makes sense as a security system designed to alleviate fears of new mothers [11].

Rational astrologies in security result from two considerations. The first is the principal–agent problem: The incentives of the individual or organization making the security decision are not always aligned with the incentives of the users of that system. The user's well-being may not weigh as heavily on the developer's mind as the difficulty of convincing his boss to take a chance by ignoring an outdated security rule or trying some new technology.

The second consideration that can lead to a rational astrology is where there is a social or institutional need for a solution to a problem for which there is actually not a particularly good solution. The organization needs to reassure regulators, customers, or perhaps even a judge and jury that "they did all that could be done" to avoid some problem—even if "all that could be done" wasn't very much.

Waldman states that "Some rational astrologies may turn out to be largely true, and that happy coincidence can be a great blessing." In the security domain, rational astrologies are often true. The reason is that if they weren't, their failure would result in pressure to change them. But the efficacy of a rational astrology is not why it was chosen. Like security theater, if a rational astrology turns out to be a good security choice, it's due to the fact that the system implementers didn't have a correct threat model in the first place.

In his seminal paper, "How Cryptosystems Fail" [1], Ross Anderson wrote:

> *Most interesting of all, however, is the lesson that the bulk of computer security research and development activity is expended on activities which are of marginal relevance to real needs. A paradigm shift is underway, and a number of recent threads point towards a fusion of security with software engineering, or at the very least to an influx of software engineering ideas.*

Three decades later, the prevalence of rational astrologies illustrate the many places where this paradigm shift has not yet taken place.

4 Acknowledgments

In 1998, we dedicated "The Street Performer Protocol" [8,9] to Ross Anderson, commemorating the years he spent busking in Europe with his bagpipes. Over

the decades, Ross's ideas and work have profoundly influenced both of our thinking, both related to security [2] and to life in general. We mourn his loss and celebrate his legacy [12].

References

1. Ross J. Anderson. "Why Cryptosystems Fail". In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu and Victoria Ashby (Editors), *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, November 3-5, 1993*, pages 215–227. ACM, 1993. https://doi.org/10.1145/168588.168615. URL https://doi.org/10.1145/168588.168615.
2. Ross J. Anderson. *Security engineering — a guide to building dependable distributed systems (2. ed.)*. Wiley, 2008. ISBN 978-0-470-06852-6.
3. Anonymous. "Politician's syllogism". In *Wikipedia*, November 2024. URL https://en.wikipedia.org/wiki/Politician's_syllogism.
4. American Psychological Association. "The Truth About Lie Detectors (aka Polygraph Tests)", 2004. https://www.apa.org/topics/cognitive-neuroscience/polygraph.
5. National Research Council. "The Polygraph and Lie Detection", 2003. https://doi.org/10.17226/10420.
6. Dinei Florêncio, Cormac Herley and Paul C. van Oorschot. "Pushing on string: the 'don't care' region of password strength". *Commun. ACM*, **59**(11):66–74, 2016. https://doi.org/10.1145/2934663. URL https://doi.org/10.1145/2934663.
7. Jody L. Jacobs, Julie M. Haney and Susanne M. Furman. "Measuring the Effectiveness of U.S. Government Security Awareness Programs: A Mixed-Methods Study". In Fiona Nah and Keng Siau (Editors), *HCI in Business, Government and Organizations — 10th International Conference, HCIBGO 2023, Held as Part of the 25th HCI International Conference, HCII 2023, Copenhagen, Denmark, July 23-28, 2023, Proceedings, Part I*, volume 14038 of *Lecture Notes in Computer Science*, pages 14–33. Springer, 2023. https://doi.org/10.1007/978-3-031-35969-9_2. URL https://doi.org/10.1007/978-3-031-35969-9_2.
8. John Kelsey and Bruce Schneier. "Electronic Commerce and the Street Performer". In Bennet S. Yee (Editor), *Proceedings of the 3rd USENIX Workshop on Electronic Commerce, Boston, Massachusetts, USA, August 31 – September 3, 1998*. USENIX Association, 1998. URL https://www.usenix.org/conference/3rd-usenix-workshop-electronic-commerce/electronic-commerce-and-street-performer.
9. John Kelsey and Bruce Schneier. "The Street Performer Protocol and Digital Copyrights". *First Monday*, **4**(6), 1999. https://doi.org/10.5210/FM.V4I6.673. URL https://doi.org/10.5210/fm.v4i6.673.
10. Bruce Schneier. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. Wiley, 2003.
11. Bruce Schneier. "In Praise of Security Theater", 2007. https://www.schneier.com/blog/archives/2007/01/in_praise_of_se.html.
12. Bruce Schneier. "In Memoriam: Ross Anderson, 1956-2024". *Commun. ACM*, 2024. URL https://cacm.acm.org/news/in-memoriam-ross-anderson-1956-2024/.
13. Randy Steve Waldman. "Rational Astrologies", 2012. https://www.interfluidity.com/v2/3513.html.

Who Are "We"? Power Centers in Threat Modeling

Adam Shostack[0000-0001-6837-5165]

University of Washington and Shostack + Associates
shostack@uw.edu

Abstract. I examine threat modeling techniques and questions of power dynamics in the systems in which they're used. I compare techniques that can be used by system creators to those used by those who are not involved in creating the system. That second set of analysts might be scientists doing research, consumers comparing products, or those trying to analyze a new system being deployed by a government. Their access to information, skills and choices are different. I examine the impact of those difference on threat modeling methods.

1 Introduction

Threat modeling is a collection of techniques for proactive security analysis of systems. The consensus industry methods are based on Shostack's Four Question Framework ("What are we working on, what can go wrong, what are we going to do about it, did we do a good job?" [13]). This paper builds on work by feminist scholars and activists to look at the influence of the intended users of industry methods. In other words, the use of 'we' in the framework was a choice that ignored power dynamics. I suggest a threat modeling approach designed to helping people analyze a system they were not involved in creating. (Terms like 'customer' or 'user' are not broad enough. Systems are often imposed, such as resume scanners, traffic cameras or border security.) For clarity, this paper avoids the convention of single author referring to themselves as 'we.' This draws heavily on themes of power dynamics from Ross Anderson's work.

There are two main senses in which the term *threat model* is used. The earlier is 'What's your threat model?' and 'random oracle', or 'a network attacker,' could be complete answers. The term was adopted into 'a model of threats,' in the sense of an abstraction of possible future harms (spoofing, tampering, etc) as applied to a system under development [6], and was deployed in informal practices such as whiteboard discussions about system security. These were adopted by [6,4,16] and others into increasingly structured methodologies. The first sense is answered by a few words, the second sense is often answered with a set of diagrams, lists of threats and mititagations and tables interlinking them.

I'll refer to these approaches as 'analyst' threat modeling and 'creator' threat modeling, respectively. The first helps us understand the relevance of an attack or analysis, the second helps anticipate and thus prevent them. Interestingly,

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

the question 'what are we working on' can be applied in either, while the techniques for answering it change. Analysts start by identifying components, data flows, and scope from a purely observational perspective. Creators have access to documentation, source code, and decision makers.[1]

2 Critiques

Sets of scholars and practitioners sought to bring creator threat modeling techniques to the analyst perspective. These included those writing under an umbrella of feminist cybersecurity and others focused on the needs of activists. In doing so, they exposed biases and limits of the techniques. Others lacked either access to the developers, or technical knowledge of software creation or operations.

2.1 Survey of Critiques

Freed et al examine 'interface-bound attackers,' who cause harm while using products as intended [3].[2] Spammers, bullies, trolls, phishers and creators of deepfakes operate within system rules, yet Stamos notes these attacks caused most harm while he led security at Facebook [15].

Slupska et al attempted to threat model a smart lock, and in particular analyze it for issues of intimate partner violence (IPV) [10]. The project exposed first, that creator perspective is limited, and second, that the techniques of creator threat modeling don't help an end user understand the problem. I'll use this as an example, because it illustrates many challenges with creator threat modeling.

Creator techniques assume a trustworthy administrator. IPV perpetrators often take control of a user session, and monitor systems for changes. If Alice manages the lock, Bob (an abuser) may have her password or demand administrative access. Bob may be notified if Alice limits his access. If Bob is the admin and Alice uses physical access to the lock to reset it, Bob may be notified or asked to approve the change. So how should the lock company design an access control matrix? They might focus on an admin who can create accounts or change permissions, and users who lock or unlock the door. But the use case of two users with the administrative password is unusual for computer security, and our normal response of 'set an acceptable policy' may lead to a literal slap in the face. The complexity and effort of enumerating attacks may inhibit creators from investigating or recording them. If they are analyzed, the complexity of addressing them may be declared to be an 'edge case' or otherwise de-prioritized.

Additionally, creator threat modeling methods like STRIDE or kill chains don't help Alice (as an analyst) discover or reason about these problems.

[1] A distinction that I failed to note in a recent corporate whitepaper [11].

[2] The author's unpublished exploration of how to threat model such systems is at `https://github.com/adamshostack/conflictmodeling/`

Space limits our ability to discuss a growing body of work including that by EFF [1], Levy [7], Loadenthal [8], Kazansky [5], and Sterling [14].

2.2 Analysis

We can consider possible threat modelers in a space defined by technical knowledge and system knowledgem as shown in Figure 1.

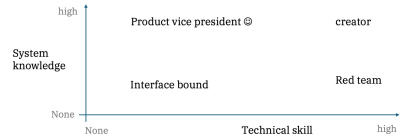

Fig. 1: A threat modeling space

Social Mileu Microsoft recognized that design choices were being made unknowingly by developers and wanted them to be able to perform analysis. To scale, we aimed at simpler processes. (There were several downsides to this, including perhaps insufficient recognition of the quality tradeoffs between experts, and a focus on reviews and documents over skills and engagement.) These circumstances informed the creation of threat modeling methodologies appropriate for use by technical experts to analyze systems with which they were highly familiar, or where they had access to the developers or code.[3] Early versions of the Four Question Framework used 'you,' as in "What are you working on?", and that was intentionally changed to 'we' to be more collaborative.[4]

This approach can be (and was!) contrasted with Anderson's educational approach. Colleagues argued "We can't require people to get a PhD in security," or "read a 500 page book."[5] Anderson expected people to think critically and well, Microsoft needed to provide a process or methodological set of steps they could follow. The focus on process was seen as a requirement for scaling, supported auditability, and was a response to a frequently expressed "just tell me what you want me to do."

The approach can also be contrasted to the sorts of threat modeling done by spies, attackers, bug bounty participants, or even academics who start with limited knowledge of a system, but a great deal of technical knowledge, possibly including security knowledge. They may be willing to dedicate more time, or they may see a single bug as a sufficient result. (The 'single bug' goal can be contrasted with the need for creators to build a secure system.) Their technique choices and investment of energy will be shaped by those circumstances.

[3] It is tempting to say 'easy access,' but that ignores the sometimes contentious inter-team relationships.

[4] Other important work included that of Kohnfelder and Garg [6] and Swiderski and Snyder [16]. A slightly fuller history is available at [11].

[5] Noting that the first edition of *Writing Secure Code* was 501 pages including introduction, and had a quote from Bill Gates, "Required reading at Microsoft" on the front cover.

Microsoft's approach was an implicit decision of which participants matter. The company put technical participants (and technical threats) first. The concerns of the people impacted was not a 'use case' that we discussed often. This move made perfect sense *to the company*, who refered to their products as 'secure by design.' This can be contrasted with the approaches required by the Food and Drug Administration, whose design-time requirements for medical device makers include a 'multi-patient harm view.' Here, the FDA is acting as a counter-balancing power center relative to device makers. Deeper consideration of power relationships could improve the benefits brought by threat modeling.

Technical Knowledge. Microsoft's software engineering roles (even program management) require deep technical knowledge. Their threat modeling methodologies thus assumed technically skilled participants.

Knowledge of system. Threat modeling methodologies were developed for internal use by Microsoft product teams who were asked to engage with product security experts. Cost and effort of knowledge transfer less important because these experts would often embed for periods between weeks and years. Even so, those experts might not be briefed on features for many reasons. Those could include people doing feature work didn't see security implications, or a desire to avoid security so an insecure feature could ship. Reviews were also conducted by highly skilled experts, and likely closer to what's called product red teaming.

3 Threat Modeling 'for the rest of us'

This section presents a simpler approach to threat modeling, designed for use by those with lower technical skill and less knowledge of a system. (The term is used for clarity, not as a judgement.) I've selected pronouns to be personal, even though foundational work to be done by advocates. The Framework is:

1. What have they delivered?
2. How will it hurt me?
3. Can I protect myself?
4. Should I even use it?

These questions are designed to be answerable, even if finding answers may require specialized skills. They aligned with the Four Question Framework to help experts remember them. Next, I explain each question and structured approaches.

3.1 What have they delivered?

Understanding what a software package is has become more complex with the prevalence of 'web apps' and associated back ends, compared to earlier models of software on floppy disks.

We might be able to use a simple model of 'local' and 'cloud.' People believe that data on their device is private and more secure, a belief created or reinforced by both intuition, and marketing like "Your fingerprint never leaves your device." Questions that can be asked by those with low technical skill might include:[6]

- Does it work without internet access?
- Can I use it without creating an account or providing a working email address?
- What does the privacy policy tell me?

Analyzing privacy policies requires determination, and maybe skill, but can expose accessible lessons, like "We share data with our 1400 partners."

Those with more technical skill use browser plugins like Noscript or tools like Wireshark, and going deeper, analyst methods start to resemble those used by security researchers, rising to enumerating libraries, using a debugger or even logic probes or electron microscopy to analyze a chip or device. Firmware and mobile apps can be downloaded and prised open, and freely available code even provides the permissions the library uses [17].

3.2 How will it hurt me?

Creator-oriented threat modeling may draw on frameworks like STRIDE to structure an analysis, but that requires technical skills [12]. A simpler set of threats, such as what does it learn and where does it send it may be helpful, but even local processing may be against the interests of a user. For example, does it show ads? Will it change function on update?

3.3 Can I protect myself, and Should I even use it?

The history of general-purpose computing is a history of modifying software to serve local needs, including security. Adblockers [18]. The trend towards restricted platforms (e.g., phones, IoT) limits user control while increasing protection against malware [19]. These restrictions complicate decisions about whether to use such systems.

More broadly, defending against trusted but untrustworthy software is challenging, even for experts. For less skilled users, it can become a Kafka-esque experience, with valid advice hard to separate from superstition.

4 Conclusion

The author regrets implying that threat modeling techniques are universal. Both people's depth of technical skills and their involvement in the creation of a system influence how they may threat model.

[6] These questions should obviously be tested for usability.

Acknowledgements

Julia Slupska and Leonie Tanczer helped me understand the problem they were grappling with. Josiah Dykstra, Jay Healey, Loren Kohnfelder and Kim Wuyts provided helpful feedback on drafts. Over decades, Ross Anderson's writings have profoundly influenced my own. I mourn his loss and hope to contribute this small bit to the celebration of his legacy.

References

1. Electronic Frontier Foundation, *Risk Assessment (Threat Modeling)*, June 24, 2019, `https://www.eff.org/files/2020/01/06/threatmodeling-onepager.pdf`
2. Farmer, W. R. and Venema, A., *Improving the Security of Your Site by Breaking Into It*, message to comp.security.unix, December 1993, `https://cyberwar.nl/d/1993-FarmerVenema-comp.security.unix-Improving-the-Security-of-Your-Site-by-Breaking-Into-It.pdf`
3. Freed, D., J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell, *A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology*, in Proceedings of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing, 2018, pp. 163-177.
4. Howard, M., and D. LeBlanc, *Writing Secure Code*, 1st ed. Redmond, WA: Microsoft Press, 1999.
5. Kazansky, B. *'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance*, Big Data and Society, January 29, 2021, DOI: 10.1177/2053951720985557
6. Kohnfelder, L., and P. Garg, *The threats to our products*, Microsoft Interface, Microsoft Corporation, vol. 33, Apr. 1999.
7. Levy, K. and Schneier, B., *Privacy Threats in Intimate Relationships*, Journal of Cybersecurity, Vol 6, Issue 1, 2020, available at: `https://academic.oup.com/cybersecurity/article/6/1/tyaa006/5849222`.
8. Loadenthal, M., *Risks, Dangers, and Threat Models: Evaluating Security Analysis for Conflict Practitioners*, August 2021, DOI:10.13140/RG.2.2.35515.95526
9. Schneier, B., *Attack Trees: Modeling Security Threats*, Dr. Dobb's Journal, December 1999.
10. Slupska, J. and L. M. Tanczer, *Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things*, in The Emerald International Handbook of Technology Facilitated Violence and Abuse, 2021, pp. 663–688.
11. Shostack, A. *Understanding the Four-Question Framework for Threat Modeling*, corporate whitepaper, November, 2024, `https://shostack.org/whitepapers`
12. Shostack, A., *Threats: What Every Engineer Should Learn From Star Wars* (Wiley, 2023).
13. Shostack, A., *Threat Modeling: Designing for Security* (Wiley, 2014).
14. Sterling, L., *Practitioners of Civil Resistance: Assess Your Cybersecurity through Threat Modeling* March 22, 2018, International Center for Non-violent Conflict, `https://www.nonviolent-conflict.org/blog_post/practitioners-civil-resistance-assess-cybersecurity-threat-modeling/`

15. Stamos, A., *Stepping Up Our Game: Re-focusing the Security Community on Defense and Making Security Work for Everyone*, YouTube, 2017. Available: `https://www.youtube.com/watch?v=YJOMTAREFtY`
16. Swiderski, F., and W. Snyder, *Threat Modeling*, Microsoft Press, 1st ed., 2004.
17. Xin, J. *app-third-party-library*, GitHub, 2024. Available: `https://github.com/xinjin95/app-third-party-library` [Accessed: 22 Nov 2024].
18. Zeunert, M. *Chrome Extension Statistics: Data From 2024*, blog post August 29, 2024, `https://www.debugbear.com/blog/chrome-extension-statistics`
19. Zittrain, J. L. *The Future of the Internet: And How to Stop It*. New Haven: Yale University Press, 2008.

Towards abusability research in HCI: Five questions for digital-safety in troubled times

Christian Eichenmüller and Zinaida Benenson

Friedrich-Alexander-Universität Erlangen-Nürnberg
christian.eichenmueller@fau.de
zinaida.benenson@fau.de

Abstract. Taking Ross Anderson's invitation to think about the abusability of technology as a point of departure, this contribution argues for a consolidation and expansion of research on how technology is used against its users. Connecting abusability with existing research on the digital-safety of at-risk users, we spell out five initial questions that researchers and developers might think about when trying to make technology less abusable. Such research is pertinent, as the rise of authoritarian and autocratic tendencies within democratic societies swells the ranks of at-risk user populations.

Keywords: Abusability · digital-safety · at-risk users · secure systems

1 Introduction

"It's not enough to think about usability; you need to think about abusability too."
— Ross Anderson [3, p.59]

This piece of wisdom, stowed in Ross Anderson's magnum opus, is our starting point for five probing questions regarding digital-safety in authoritarian times. The re-election of Donald Trump is just the latest sign of an authoritarian turn and fears over the democratic constitution of Western societies are growing – developments which also impact the distribution of digital-safety risks within these societies. For instance, even a cursory glance at the situation within the US suggests that new groups of people – undocumented migrants, abortion advocates, journalists, lawyers, political opponents of the President – have entered the ranks of so-called "at-risk populations".

In the sprawling HCI debate about digital-safety, at-risk users are typically described as those who are more likely to be digitally attacked or targeted by surveillance and/or who could be disproportionately harmed by such attacks [44]. Widely discussed examples of at-risk user populations include activists [1,7,12], dissidents [19,31], journalists [8,14,28,29], refugees [37], sex workers [27], or victims of intimate partner violence [6,9,17]. Yet, the contours of at-risk populations and their digital-safety requirements are continuously changing. With the rise of authoritarianism, research on these shifts is even more urgent.

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

This contribution is a call for researchers and developers to not just think about how to make technology usable, but also how to avoid its abuse. Abusability research addresses socio-technical consequences and potential social, physical, political or psychological harms. Below, we spell out five initial questions that researchers and developers might think about to make technology less abusable.

2 Five questions for abusability research

2.1 New realities: Which conditions enable abuse?

Abusability describes the potential of turning technology against its users. Two developments underscore a growing importance of abusability research:

(1) The proliferation of digital devices means that questions of abusability penetrate a user's most intimate spaces. This fact has been recognized in the intimate partner and interpersonal abuse literature [22,40,41]. Given the increasingly networked nature of social life, it becomes hard for users to withdraw from digital-safety risks.

(2) The proliferation of digital devices has not been accompanied by a comparable extension of user control over their information. The conditions of datafication are characterised by a power imbalance between users, who often lack the technological literacy to become digitally sovereign or more resilient, and corporate providers, who are themselves part of a competitive ecosystem in which data is a commodity [34,45].

Just as usability research inquires how to make technology more usable, abusability research asks the question how to make technology less abusable. Such research might rest on individual level, even single-case, inquiries whereby abusers/opponents and attack paths are identified through threat modeling [21,38]. Yet, equally relevant are ecosystem approaches addressing for instance the introduction of hardening settings for device types, such as Apple's Lockdown Mode [23]. Though there is a robust debate on privacy enhancing technologies, the question of abuse with/through technology cannot be a purely user-centered inquiry. Instead, abusability research addresses the embeddedness of users in relations of technology, power, and abuse.

2.2 Mapping abuser networks: Who threatens digital-safety?

The classic "opponents" in security engineering [3, pp.17—61] are also those who threaten users' digital-safety: nation-state adversaries [25], cybercriminals [10,32], as well as all those motivated by financial, political or personal interests and ready to turn technology against others. Recently, the rise of authoritarian and autocratic tendencies within Western societies [5] has begun to significantly shift the coordinates of digital-safety risks in those societies. For example, revelations regarding the use of Pegasus spyware against journalists [2] and domestic democratic opposition in countries around the world hint at patterns of widespread abuse [13,24,33]. As technical capabilities expand, we are likely to see renegotiations [36] over what is legal and over what is legitimate (not the same).

In light of these shifting coordinates, researchers trying to map digital-safety risks are not just confronted with unprecedented levels of technical details, such as when trying to reverse engineer chains of exploited vulnerabilities, but also with social and political struggles over institutionalised surveillance, spyware trade networks, and backroom deals by political and corporate power brokers.

2.3 Mapping abusability: Who is at risk of abuse?

A short answer to this question could be: everyone. Just as usability concerns every potential user, abusability is relevant across user populations. However, from a research perspective, this response is unsatisfactory. As digital-safety researchers have shown, some groups are more at risk than others [16,30,35]. Mapping absuability across technologies and user populations can help mitigate the extent to which technologies are turned against users [20].

Hours after Donald Trump's re-election in November 2024, Black people across the United States had received racist text messages telling them they had been "selected" to pick cotton and had to report to "the nearest plantation" [15,43]. Sometimes referring to the recipients by name, the implication was clear enough: communities of colour are once again being targeted. The psychological consequences of such abuse are immense.

As this example shows, the extent to which technology is used against its users' is tied up with social and political dynamics. Hence, a question for developers is: Who could be targeted by the system or mechanism I am building? Just as usability is best addressed at the design stage, thinking about abusability from the start offers the best chance for avoiding the worst abuses. So long as the question of abusability is not addressed systemically, users themselves will have to fend for their digital-safety.

2.4 Understanding abuse pathways: How does abuse scale?

Abuse through the repurposing of information systems is not a new phenomenon. Viktor Mayer-Schönberger writes:

> *"In the 1930s, the Dutch government had put in place a comprehensive population registry containing name, birth date, address, religion, and other personal information for each citizen. The registry was hailed as facilitating government administration and improving welfare planning. Then the Nazis invaded the Netherlands and took possession of the registry, ruthlessly repurposing the personal information of millions of Dutch citizens to identify, persecute, and murder Jews and gypsies. Because of the information contained in the comprehensive registry, the Nazis were able to identify, deport, and murder a much higher percentage (73%) of the Dutch Jewish population than in Belgium (40%), France (25%), or any other European nation."* [26, p.141]

This example from the last century illustrates the damage that large-scale information systems can do in the wrong hands. Fast forward to the contemporary information society and it is apparent that there is no shortage of exploitable systems. If anything, when resources allow, "collect it all" has become a tried and tested strategy in state [11,18] and corporate arenas [4,42], and the possibility of "attack scaling" [3, p.29/30] has multiplied. Adding to this novel AI capabilities in accelerating information processing and repurposing, we recognize how abuse becomes possible on unprecedented scales.

Yet, the digital age has not just provided for collecting and exploiting information at scale. It now also allows for the production, fabrication and distribution of information in unprecedented volumes. Fake news, disinformation and misinformation have become scalable political strategies, amply employed by autocrats against their domestic and geopolitical adversaries. Describing how contradictory statements and blatant lies are constantly repeated, Anne Applebaum writes:

> *"This tactic, the so-called 'fire hose of falsehoods' produces not outrage but nihilism. Given so many explanations, how can you know what actually happened? What if you can never know? If you can't understand what is going on around you, then you are not going to join a great movement for democracy, or follow a truth-telling leader, or listen when anyone speaks about positive political change. Instead, you will avoid politics altogether. Autocrats have an enormous incentive to spread that hopelessness and cynicism, not only in their own countries, but around the world."* [5, p.79]

The aim of this tactic is to disorient. In such an information environment, anything can be undermined, from scientific assessments of climate change, to public health policies in times of a pandemic, or the integrity of an opposition figure. These examples show how abuse scales. The digital-safety literature provides plenitudes of more pointed and focused abuses and attacks on at-risk users, from phishing and targeted surveillance to doxxing and smear campaigns. Under these circumstances, users need allies, and they need reliable and secure systems.

2.5 Protecting users: How to build secure, non-abusive systems?

This brings us back to the question that drives Ross Anderson's magnum opus. In his words, there is neither a "magic formula" nor a "silver bullet" for the development of secure systems. Instead, Ross reminds us, a "security engineering manager has to know thousands of little things; that's why this book is so fat!" (one can really hear him now) [3, p.965/6].

For security engineers, Ross Anderson broke down the challenge of secure systems into two queries: "Are we building the right system?" and "Are we building it right?" [3, p.966]. The power of these inquiries does not just stem from a systematic approach, it also bespeaks a deeper intrinsic motivation: Ross wanted his students to do the right thing.

It is within these queries where academic communities meet (and why he was such a good convener of these). Whether informed by psychology, economics or sociology, Ross Anderson embedded secure systems development in interdisciplinary investigations. The method is not to assert, but to invite.

To understand how technology is turned against users, it is worthwhile to ask: Which conditions enable abuse? Who threatens digital-safety? Who is at risk of abuse? How does abuse scale? And how do we achieve secure, non-abusive systems? These questions provide a socio-technical research framework, whose insights might inform the "abusability testing" of technology [39].

Two pioneering contributions regarding abusability testing are the toolkit by Strohmayer et al. [41] and the work by Stephenson et al. suggesting an abuse vector framework for interpersonal abuse situations [40]. Absent from the existing literature are studies that broaden the scope of abusability inquiry to the many old and new at-risk populations, whose digital-safety is threatened by authoritarian and autocratic tendencies. Here we see a great need for research to make technology less abusable in the years ahead.

3 Conclusion

Following Ross Anderson's invitation to think about the abusability of technology, we call on HCI researchers to supplement work on how to make technology usable with investigations on *how to make it less abusable*. Existing research on digital-safety needs of at-risk user populations can serve as first benchmarks in this endeavor. Animated by concerns over how technology is turned against its users, we have formulated five initial socio-technical questions that researchers and developers might think about when trying to make technology less abusable. This research is pertinent, as the rise of authoritarian and autocratic tendencies within democratic societies swells the ranks of at-risk user populations.

References

1. Martin R Albrecht, Jorge Blasco, Rikke Bjerg Jensen and Lenka Mareková. "Collective information security in large-scale urban protests: the case of Hong Kong". In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3363–3380. 2021.
2. Amnesty International. "India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists", 23 Dec 2023. Available at: `https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/`.
3. Ross J Anderson. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.
4. Mark Andrejevic. *Infoglut: How too much information is changing the way we think and know*. Routledge, 2013.
5. Anne Applebaum. *Autocracy, Inc.: The dictators who want to run the world*. Random House, 2024.

6. Rosanna Bellini, Kevin Lee, Megan A Brown, Jeremy Shaffer, Rasika Bhalerao and Thomas Ristenpart. "The digital-safety risks of financial technologies for survivors of intimate partner violence". In *Proceedings of the 32nd USENIX Conference on Security Symposium*, pages 87–104. 2023.
7. Maia J Boyd, Jamar L Sullivan Jr, Marshini Chetty and Blase Ur. "Understanding the security and privacy advice given to Black Lives Matter protesters". In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–18. 2021.
8. Behlül Çalışkan. "Digital security awareness and practices of journalists in Turkey: A descriptive study". *Conflict & Communication*, **18**(1), 2019.
9. Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy and Thomas Ristenpart. "The spyware used in intimate partner violence". In *IEEE Symposium on Security and Privacy (SP)*, pages 441–458. IEEE, 2018.
10. Ben Collier, Richard Clayton, Alice Hutchings and Daniel Thomas. "Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture". *The British Journal of Criminology*, **61**(5):1407–1423, 2021.
11. Jeremy W Crampton. "Collect it all: National security, big data and governance". *GeoJournal*, **80**:519–531, 2015.
12. Alaa Daffalla, Lucy Simko, Tadayoshi Kohno and Alexandru G Bardas. "Defensive technology use by political activists during the Sudanese revolution". In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 372–390. IEEE, 2021.
13. Ronald J Deibert. "The autocrat in your iPhone: How mercenary spyware threatens democracy". *Foreign Affairs*, **102**:72–88, 2023.
14. Philip Di Salvo. ""We have to act like our devices are already infected": Investigative journalists and internet surveillance". *Journalism Practice*, pages 1–18, 2021.
15. Dalia Faheid, Ashley Williams, Jack Forrest, Jillian Sykes and Sean Lyngaas. "Authorities work to find the source of racist texts sent to Black people nationwide after the election. Here's what we know". *CNN*, 10 Nov 2024. Available at: `https://edition.cnn.com/2024/11/09/us/racist-texts-black-people-investigation-what-we-know/index.html`.
16. Diana Freed, Natalie N Bazarova, Sunny Consolvo, Eunice J Han, Patrick Gage Kelley, Kurt Thomas and Dan Cosley. "Understanding digital-safety experiences of youth in the US". In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–15. 2023.
17. Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart and Nicola Dell. "Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders". *Proceedings of the ACM on human-computer interaction*, **1**(CSCW):1–22, 2017.
18. Glenn Greenwald. *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan, 2014.
19. Laura Gianna Guntrum. "Keyboard Fighters: The Use of ICTs by Activists in Times of Military Coup in Myanmar". In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–19. 2024.
20. Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou and M Angela Sasse. "Digital Security—A Question of Perspective. A Large-Scale Telephone Survey with Four At-Risk User Groups". In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 27–27. IEEE Computer Society, 2023.

21. Becky Kazansky. "'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance". *Big Data & Society*, **8**(1):2053951720985557, 2021.
22. Karen Levy and Bruce Schneier. "Privacy threats in intimate relationships". *Journal of Cybersecurity*, **6**(1), 2020.
23. Benedikt Mader, Christian Eichenmüller, Gaston Pugliese, Dennis Eckhardt and Zinaida Benenson. "I Blame Apple in Part for My False Expectations: An Autoethnographic Study of Apple's Lockdown Mode in iOS", 2024.
24. Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak and Ron Deibert. "Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries". Technical report, Citizen Lab, 2018.
25. William R Marczak, John Scott-Railton, Morgan Marquis-Boire and Vern Paxson. "When governments hack opponents: A look at actors and technology". In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 511–525. 2014.
26. Viktor Mayer-Schönberger. *Delete: The virtue of forgetting in the digital age*. Princeton University Press, 2009.
27. Allison McDonald, Catherine Barwulor, Michelle L Mazurek, Florian Schaub and Elissa M Redmiles. "'It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online". In *30th USENIX Security Symposium (USENIX Security 21)*, pages 375–392. 2021.
28. Susan E McGregor, Polina Charters, Tobin Holliday and Franziska Roesner. "Investigating the computer security practices and needs of journalists". In *24th USENIX Security Symposium (USENIX Security 15)*, pages 399–414. 2015.
29. Susan E McGregor, Elizabeth Anne Watkins, Mahdi Nasrullah Al-Ameen, Kelly Caine and Franziska Roesner. "When the weakest link is strong: Secure collaboration in the case of the Panama Papers". In *26th USENIX Security Symposium (USENIX Security 17)*, pages 505–522. 2017.
30. Savanthi Murthy, Karthik S Bhat, Sauvik Das and Neha Kumar. "Individually vulnerable, collectively safe: The security and privacy practices of households with older adults". *Proceedings of the ACM on Human-Computer Interaction*, **5**(CSCW1):1–24, 2021.
31. Shishir Nagaraja and Ross Anderson. "The snooping dragon: social-malware surveillance of the Tibetan movement". Technical Report UCAM-CL-TR-746, University of Cambridge, Computer Laboratory, 2009.
32. Sergio Pastrana, Daniel R Thomas, Alice Hutchings and Richard Clayton. "Crimebb: Enabling cybercrime research on underground forums at scale". In *Proceedings of the 2018 World Wide Web Conference*, pages 1845–1854. 2018.
33. Laurent Richard and Sandrine Rigaud. *Pegasus: The Story of the World's Most Dangerous Spyware*. Pan Macmillan, 2023.
34. Bruce Schneier. *Data and goliath: The hidden battles to collect your data and control your world*. WW Norton & Company, 2015.
35. John Scott-Railton. "Security for the high-risk user: separate and unequal". *IEEE Security & Privacy*, **14**(2):79–87, 2016.
36. Michael Silberman. "Policing Pegasus: The Promise of US Litigation for Commercial Spyware Accountability". *Georgetown Law Technology Review*, **8**:245–286, 2024.
37. Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner and Tadayoshi Kohno. "Computer security and privacy for refugees in the United States". In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 409–423. IEEE, 2018.

38. Julia Slupska, Scarlet Dawson Duckworth, Linda Ma and Gina Neff. "Participatory threat modelling: Exploring paths to reconfigure cybersecurity". In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–6. 2021.
39. Ashkan Soltani. "Abusability testing: Considering the ways your technology might be used for harm". In *Enigma*. 2019. Available at: `https://www.usenix.org/node/226468`.
40. Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang and Rahul Chatterjee. "Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse". In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 69–86. 2023.
41. Angelika Strohmayer, Julia Slupska, Rosanna Bellini, Lynne Coventry, Tara Hairston and Adam Dodge. "Trust and abusability toolkit: Centering safety in human-data interactions". Technical report, Northumbria University, 2021.
42. Stuart A Thompson and Charlie Warzel. "Twelve million phones, one dataset, zero privacy". In *Ethics of data and analytics*, pages 161–169. Auerbach Publications, 2022.
43. Adria R Walker. "Black people across US receive racist text messages after Trump's win". *The Guardian*, 8 Nov 2024. Available at: `https://www.theguardian.com/us-news/2024/nov/08/racist-text-messages-trump-win`.
44. Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L Mazurek, Manya Sleeper and Kurt Thomas. "SoK: A framework for unifying at-risk user research". In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 2344–2360. IEEE, 2022.
45. Shoshana Zuboff. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs, 2019.

Usable Security in Organizations – Solutions looking for a Problem Owner

Simon Parkin

Delft University of Technology

Abstract. Great strides have been made in the study of the human factor in security, in particular in finding ways for security in organizations to be more usable for employees alongside their productive work. However, a user-centred approach to security, that acts naturally to limit the burden on employees, remains aspirational. Where the usable security community has assembled a large body of techniques to reduce the burden on employees, seeing this move into common practice – for the impact on users to be a primary concern for those responsible for IT-security provisioning – still relies heavily on a change of mindset amongst practitioners. While that has not happened, the techniques of user-centred security have been selectively applied in practice, to the disadvantage of employees. We must learn to promote our approaches relative to the growing market of solutions which purports to support the user, and position more usable solutions in terms that accommodate the pressures, resource constraints, and expectations placed upon IT-security infrastructure managers themselves.

Keywords: human-centred security · security economics · organization security.

1 Introduction

The fundamental work of Ross Anderson in security economics (e.g., [4,5]) opened up two great possibilities which have inspired the work described here. Firstly, applying economics principles to understand how decision-making, resourcing issues, and incentive problems often limit the success of security solutions, beyond any technical shortcomings. Secondly, Anderson's security economics work also deftly demonstrated that security challenges may be best approached with a mix of disciplines. Here, we consider security usability challenges in organizations alongside practitioner decision-making, and wider organizational pressures, in a manner inspired by Anderson's security economics work.

Much research has been conducted over the last twenty years and more, to understand the human factor of security in organizations. This includes both generation of evidence, and development of engagement methods. The research community has been able to characterise the rifts between employees and security managers [2,7], how training and awareness initiatives can fail [8], and where employee effort to work securely is confounded by security controls and policies that work against their productive goals [11,22].

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

A number of barriers work against these advancements – and the spirit of user-centred security – entering organizations as routine practice. An ongoing pursuit of more usable forms of security in organizations, that identifies and accommodates the employee, is still positioned as *aspirational*. This rests on a security manager having a mindset to pursue more usable security in their organization, that in turn motivates the commitment of resources toward that goal. This further relies on the *reference narrative* [20] of the manager being one where they pride themselves on their security provisions being usable, in essence a practitioner who is already onboard, to overcome any uncertainty in how to proceed. This is in contrast to a mindset which imposes restrictions on users to meet security needs first.

For most security managers not already interested in listening to requests from their userbase, the usable security community has yet to find a path for a security manager to get to where we want them to be [17,27]. We have not defined a path to adoption of more usable security solutions for employees, that can become 'everyday' practice for the kind of security manager who believes that employees should align with the manager's interpretation of how to serve the organization's needs [17]. Put another way, we have not made sufficient progress in getting usable security into organizations in a natural way, 'by stealth' [26].

User-centred security has tried to disrupt current security management practices by imposing mindsets, and calling for them to change. Approaches include protesting that managers do not care about user time (and usability) as much as they should [17], or that security is being pitched as more important than productive work (for instance through security culture initiatives [8], etc.). Our protests rely on forcing a shift of mindset, through arguments about what the narrative should be in practice, which has not happened. This holds back the application of usable security advancements.

This raises questions as to how the growing body of usable security research is expected to enter practice. While usable security techniques rely on a usable security mindset, it has risked advances in the field being applied in selective ways in practice, to satisfy a narrative of an environment being controlled and made predictable, wherein employees conform to security policy foremost. Usable security has not taken purchase in the majority of organizations [13], instead being a 'nice to have'. Unchecked, user-facing security interventions start from a position of favouring the preferences of the manager, which have a tendency to lean on the employee to do more [17], with the view that management and policy compliance come first. This has meant that growing challenges, such as the complexities of organization IT, wherein multiple solutions are deployed together (alongside productive work [9,10]) are not being met head-on [18].

There is a need to directly consider who to address usable security advancements to, who is in a position of power and resource, to involve the user more in finding less burdensome workplace security solutions. This effort would combine usable security and security economics [5], to appreciate that we have not defined whose decision we are informing, or sufficiently defined and differentiated the costs and benefits of user-centred security proposals, relative to other choices

which favour the technically-minded narrative of infrastructure control and the security manager knowing best.

2 Giving shape to expectations of usable security in organizations

Much work has aimed to understand the security manager perspective on the actions of the user, the employee [6,17,26,27]. The arguments made in usable security rely mostly on effort, 'hassle' [10], and policy conflicts, and that how much of this is left to the employee to resolve – and overcome – is excessive. Yet, there is an acceptance that *some* effort is expected of users to work securely and avoid workplace security threats. A user-centred approach would minimize this effort and ensure that the residual effort is commensurate to the tasks users perform. However, how usable security improvements are pursued within an organization appears to be bounded by how much an organization is willing to spend on the activity rather than a discernible end-goal, since there is no limit to the opportunities to reduce burden amidst the complexities of organization IT. That is, usable security does not have the same appealing end-goals as one-time training packages, for instance [17].

Part of the issue here is also that seeing the benefit in a user-centred approach relies on instrumenting, measuring, and appreciating the disurptions and accumulation of effort by employees, collectively, in their various interactions with security-related technologies. This requires resource to be invested by the organization or manager, and a sociotechnical assessment to characterise the existing costs, to see the proposed benefits. This would already require a manager who is not inclined to favour the user to concede that they had it all wrong, to *then* collect the evidence to prove it to themselves.

Given existing measurement of security usability in organizations (or lack thereof), we have not defined an alternative way of managing user-facing security in organizations that is sufficiently distinct (in the view of current security managers) from current practice (in activities and affordances), to motivate the outlay of the (mostly speculative) costs. The distinction is made on different terms, and in turn different evidence (such as training completion and phishing click-rates [17,18]). Where user-centred security proposes alternative approaches, they do not have the same benefits of steadfast control, and they incur their own distinct, additional costs to monitor and maintain. The opportunity cost for those managers not already enthusiastic about usability – to explore what may be efficiency benefits with possible security benefits – is too high.

Compounding this is that good security fits the context of use. Practitioners may appreciate the implied benefits of listening to the challenges and needs of employees, but at the same time may not want a thought exercise, and prefer instead to immediately find a workable solution [19]. A manager gravitates toward the most certain and bounded solution within their means. In organization security, control looks like management – this is why shadow security behaviours (where employees fashion security measures to match their productive needs),

where they persist [1,3,23], are often seen as something to eliminate, rather than learn from. Where there are high costs to enforcing soft controls such as training and security culture [25], a security manager who believes employees should be aligned with their vision of control may simply be unequipped to engage and incur the (additional) costs of enforcing secure working through softer controls.

User-centred improvements must also be bounded; this is perhaps why we see evidence of 'inverse usability' in organizations [18], where resources – if they are even available – are invested in engaging with employees only in those instances where they have a problem with the security solutions provided to them.

3 Relating user security to a manager perspective

We have not defined a user-centred way to manage security for the 'dispassionate' manager, who foremost wants to show that they are managing the infrastructure well, and within their given means. Being open to employee input may come across as giving up control, or of not being able to demonstrate being a assertive manager (delivering one-way guidance to employees, as the expert who has to 'protect them' [14]).

Complicating matters further, current user-facing solutions in the market can appear to be achieving user-centred security, such as training and awareness packages that are deployed without consultation with employees [12]. The approach of the usable security research community has been to critique such solutions on our own terms; instead, we should consider how user-centred security can also account for what the market and managers want, and be competitive and distinct on market terms.

Where proactive user-centred security is succeeding, it is arguably with those managers who are already convinced and see user involvement as part of their narrative. For the most part, especially more technical managers may already believe that they are practicing user-centred security by deploying 'a' training package, and are unable to make a distinction between that and what employees might otherwise benefit from to make secure working more doable (which perhaps is why awareness managers are not routinely involved in procurement decisions [18] – it is not signaled that there would be a need to). The signal for what more a manager should do to consider the needs of the employee is indistinct. It would be necessary to articulate the distance between where practice currently is, and a more user-centred approach, rather than relying on a change of mindset and narrative to unlock the resource and drive to make this happen.

We are not at a point where security managers can practice the kind of 'negative capability' that Keats describes [21] and which has been explored to a limited degree in the study of management practices [16], wherein a security manager may be comfortable with not being able to control the environment around them, and to some extent invite the unexpected. We are missing a narrative that allows a security manager to project that they are managing, while also being accommodating of employees as experts of their own domain in the organization, to uplift productivity, security, and other expectations [15].

4 Looking ahead

Accepting that we must meet the security practitioner where they are, this shifts the direction the user-centred security community should be heading. The following are first possible directions:

More usable security in regulations, as goals and protections. Awareness and training for employees are already entering regulations (e.g., GDPR, PCI [18]), where these signpost what should be included. Beyond this, it would be difficult to set a baseline as, arguably, the most user-friendly security solutions are crafted to the context of use – this forces more thought exercises for unprepared managers. More mention of user-facing solutions in regulation, however, risks more templates and generic solutions. Another approach would be to define 'red lines' that employees should not be forced to cross, e.g., only committing a certain amount of time to security every day. An argument of needing to 'follow the company policies' already risks being used as permission to ask employees to expend a great amount of energy for security, beyond their job description, and needs to be kept in check.

Define first steps – let the manager demonstrate value to themselves. Provide a roadmap for solutions for user-centred security provisioning in organizations. These should articulate benefits for users that remove blockers to secure working, but are also within the manager's existing means. This would be instead of relying on a change of mindset to putting the user first, to 'release' the resources to improve security usability (where although ideal, this has not happened, yet). This would also force the usable security research community to identify *who* we expect to make a particular change, and how they can achieve the change within their available resources. This will also help us to track which usable security improvements fail, and why. A manager may be hesitant to accommodate employee needs if they do not have the resources to honour those needs (where feedback on phishing reporting is already lacking in implementation, in part for this reason). One implicit narrative up to now is, employees have to follow policies, and that a good manager makes policies which are correct – we would need to provide prescriptive approaches (as well as narratives) for such a manager to engage with users, in a way where inviting input is not to also invite questions about the capability of the manager to define a good policy.

Find effective stories about usable security in organizations. While user-centred security approaches do not immediately point to what one or other organization should do, we can do more to identify good examples in reality, and explain what is good about them. This could support a *recognitional approach* [19], to support testing possible solutions and sticking with a *workable solution*, rather than searching tirelessly for an optimal solution. We would find relatable case studies [24] which demonstrate value in usable security. Currently, not-so-user-centred solutions – which burden and responsibilize the employee – are the first solution to be tried and to appear workable.

References

1. Jan-Philip van Acken, Floris Jansen, Slinger Jansen and Katsiaryna Labunets. "Who is the IT Department Anyway: An Evaluative Case Study of Shadow IT Mindsets Among Corporate Employees". In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 527–545. 2024.
2. Anne Adams and Martina Angela Sasse. "Users are not the enemy". *Communications of the ACM*, **42**(12):40–46, 1999.
3. Sarah Alromaih, Ivan Flechais and George Chalhoub. "Beyond the Office Walls: Understanding Security and Shadow Security Behaviours in a Remote Work Context". In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, pages 507–525. 2024.
4. Ross Anderson. "Why information security is hard – an economic perspective". In *Seventeenth Annual Computer Security Applications Conference*, pages 358–365. IEEE, IEEE, New York, 2001.
5. Ross Anderson and Tyler Moore. "The economics of information security". *Science*, 2006.
6. Debi Ashenden and Darren Lawrence. "Can we sell security like soap? A new approach to behaviour change". In *Proceedings of the 2013 New Security Paradigms Workshop (NSPW)*, pages 87–94. 2013.
7. Debi Ashenden and Darren Lawrence. "Security dialogues: Building better relationships between security and business". *IEEE Security & Privacy*, **14**(3):82–87, 2016.
8. Maria Bada, Angela M Sasse and Jason RC Nurse. "Cyber security awareness campaigns: Why do they fail to change behaviour?" *International Conference on Cyber Security for Sustainable Society*, 2015.
9. Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol and Angela Sasse. "Productive security: A scalable methodology for analysing employee security behaviours". In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 253–270. 2016.
10. Adam Beautement, M Angela Sasse and Mike Wonham. "The compliance budget: managing security behaviour in organisations". In *Proceedings of the 2008 new security paradigms workshop*, pages 47–58. 2008.
11. John M Blythe, Lynne Coventry and Linda Little. "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors". In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pages 103–122. 2015.
12. Lina Brunken, Annalina Buckmann, Jonas Hielscher and M Angela Sasse. "'To Do This Properly, You Need More Resources": The Hidden Costs of Introducing Simulated Phishing Campaigns". In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 4105–4122. 2023.
13. Deanna D Caputo, Shari Lawrence Pfleeger, M Angela Sasse, Paul Ammann, Jeff Offutt and Lin Deng. "Barriers to usable security? Three organizational case studies". *IEEE Security & Privacy*, **14**(5):22–32, 2016.
14. Joseph Da Silva. "Protection, expertise and domination: Cyber masculinity in practice". *Computers & Security*, **133**:103408, 2023.
15. Albesë Demjaha, Simon Parkin and David Pym. "The boundedly rational employee: Security economics for behaviour intervention support in organizations". *Journal of Computer Security*, **30**(3):435–464, 2022.

16. Robert French. "“Negative capability”: Managing the confusing uncertainties of change". *Journal of organizational change management*, **14**(5):480–492, 2001.
17. Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge and M. Angela Sasse. "“Employees Who Don't Accept the Time Security Takes Are Not Aware Enough”: The CISO View of Human-Centred Security". In *Proceedings of the 32nd USENIX Security Symposium (USENIX '23)*. 2023.
18. Jonas Hielscher and Simon Parkin. "“What Keeps People Secure is That They Met The Security Team”: Deconstructing Drivers And Goals of Organizational Security Awareness". In *33rd USENIX Security Symposium (USENIX Security 24)*. 2024.
19. Robert JB Hutton and Gary Klein. "Expert decision making". *Systems Engineering: The Journal of The International Council on Systems Engineering*, **2**(1):32–45, 1999.
20. John Anderson Kay and Mervyn A King. *Radical uncertainty*. Bridge Street Press Decision-making beyond the numbers, 2020.
21. John Keats. *The Letters of John Keats*. Reeves & Turner, 1895.
22. Iacovos Kirlappos, Adam Beautement and M Angela Sasse. "“Comply or Die”' Is Dead: Long live security-aware principal agents". In *Financial Cryptography and Data Security: FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers 17*, pages 70–82. Springer, 2013.
23. Iacovos Kirlappos, Simon Parkin and M Angela Sasse. "Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security". In *Workshop on Usable Security (USEC) 2014*. 2014.
24. Mary S Morgan. "Resituating knowledge: Generic strategies and case studies". *Philosophy of Science*, **81**(5):1012–1024, 2014.
25. Frank Pallas. "Information security inside organizations — a positive model and some normative arguments based on new institutional economics". *Available at SSRN 1471801*, 2009.
26. Simon Parkin, Aad Van Moorsel, Philip Inglesant and M Angela Sasse. "A stealth approach to usable security: helping IT security managers to identify workable security solutions". In *Proceedings of the 2010 New Security Paradigms Workshop*, pages 33–50. 2010.
27. Lena Reinfelder, Robert Landwirth and Zinaida Benenson. "Security managers are not the enemy either". In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–7. 2019.

Difficult Truths for our Harsh Times

Have security & privacy research, and the students we have trained, actually made the world a better place?

Stuart Schechter[1]

Harvard University School of Engineering and Applied Sciences
papers@stuartschechter.org
https://stuartschechter.org

Not everyone will miss Ross Anderson.

Ross was not afraid to speak truths that made people uncomfortable. His ideas and arguments threatened the beliefs, status, power, ego, and bank balances of others — often those with power. His writings and talks undermined proponents of hardware attestation, chip-and-pin authentication, and surveillance, to name just a few. Many of those threatened by what Ross had to say professed to be faithfully working to serve the public. Many likely believed they were.

Most of those of us celebrating Ross's life are members of the scientific and academic community that researches security within the context of computing, technology, and public policy. While we may not be policymakers or titans of industry, almost all of us are privileged to have knowledge and skills that give us far more power over our use of technology than the average citizen, and to train others to use that power. Most of us believe that we use the skills and knowledge we are privileged to possess to faithfully serve the public.

We can honor Ross by embracing discomfort and questioning our own beliefs that we, individually and as a community, are using the powers we possess to make the world a better place.

Examining this question *should* indeed make us uncomfortable. I first met Ross in 2002, while I was a graduate student, at a time when the study of security was just starting to receive the attention it deserved. It was an exciting time, and many of us had high aspirations and ambitious goals. Yet, it is hard to imagine a metric of success for serving the public – real living people – for which our field can claim anything but defeat.

Imagine the questions we would have to answer if our prior selves could hold a post-mortem of the goals and aspirations we started with in the early 2000s.

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

Have we protected people's identifiers or other key information?

No. It's nearly impossible to participate in modern society without taking actions that will eventually lead to the leak of your government identifiers, financial data, phone number, and physical address. What have we achieved?

1. Nearly every member of the public now has enough free credit reporting to last until the heat death of the universe, and
2. we have numbed the public to seemingly-endless disclosures that their data has been compromised.

Have we protected against scams, extortion, and other cybercrime?

Nope. Any successes we can claim in harm-reduction have been counteracted many times over by our contributions to harm-amplifying technologies.

We helped create the cryptocurrency technologies that have enabled rug pulls, ransomware, pump and dump schemes, romance scams, and human enslavement. We helped breathe new life into organized crime and authoritarian governments that harbor criminals. We helped fund a $197 million dollars of spending in the 2024 US election to support candidates willing to commit to ensure the spread of this cancerous *'industry'*,[1] eclipsing the lobbying of all other industries. We succeeded in making the lobbying of the fossil fuel industry seem like noise – a mere $60 million! – by comparison.

Cryptocurrencies alone may have produced the *magnitude* of impact that, back in 2002, Ross and I might have hoped the field would achieve. Alas, that impact was in the wrong direction.

Have we built a robust cybersecurity industry to at least attempt to protect the public?

Still No! What we have built is an industry to protect business from the public. Walk the floors of our biggest industry conference, RSA, and you will see the extravagant display of the wealth of the cybersecurity industry that purports to bring in nearly $200 billion dollars a year. Yet, you'll be hard-pressed to find one of the roughly 600 vendors that is making products to protect actual people ('consumers', in industry-speak).[2] Economic theorists might tell us that the public should reap the benefits of a cybersecurity industry that protects businesses from losses that might otherwise be passed onto consumers but, in practice, much of what the industry sells are compliance products to protect businesses from negligence lawsuits. The net effect is that these expenditures protect business from members of the public who might seek recompense for the prices we pay for business's *endless* stream of security failures.

What's worse, this industry produces security products that require highly-privileged access to customers networks and data and that, if compromised, can

[1] Using the word 'industry' generously to describe enterprises that produce no actual goods.

[2] The notable exceptions that proves the rule are password managers. Some were founded with the mission of serving consumers, but shifted focus to enterprises after being purchased by private equity (LastPass) or receiving investments from venture capitalists (1Password).

have devastating security consequences. Yet, these companies almost all start out as start-ups that prioritize shipping product over safety. Even as companies mature, the code is rarely as robust as it should be given its criticality. Over and over, the products of our cybersecurity industry have themselves introduced new vectors through which attackers can compromise even the organizations that are in greatest need of protection and that invest the most in it. Or, as in the case of CrowdStrike, security products have introduced entirely new failure modes that require no adversarial behavior to disrupt lives and incur billions of dollars of losses.

Have we secured citizens from authoritarian technology?

Mostly we have done the opposite. We have given authoritarians greater control over their citizens' access to technology.

In 2002 most citizens had *technological autonomy*: their primary computing device was a personal computer onto which they could install or compile any software they wanted. Their government might ban certain software and make it hard to find, but if a government wanted its citizens to have access to modern technology, it had to give them access to general-purpose computing devices that were at least capable of running *any* software.[3]

Then, Apple and Google discovered they could make more money if they monopolized the means through which software was distributed on their platforms. When they introduced iOS and Android, they took away users' autonomy to install the software of their choosing. It's not like we could ignore the consequences: at roughly the same time (2009) Amazon removed books that they hold sold to consumers from the devices they had sold to consumers.

Security technologists at Apple and Google told users that their loss of autonomy was in their best interest. Many of us in the security research community agreed that the only way to prevent malware was to prevent users from having the choice to do so. Our culture of blaming users for failures of software architecture[4] helped industry justify robbing users of their autonomy. And, once industry could restrict users' access to software, governments could force industry to impose their own restrictions. Today, governments can decide whether we are allowed to use applications that can perform encryption, and they have turned our computing devices are used to surveil us, reducing our privacy.

[3] Back in 2002, trusted platform modules appeared to be the biggest threat to technological autonomy.

[4] Malware was so prevalent on personal computers because their security model gave all software the power to corrupt other software by default. Mobile operating systems sandboxed applications from each other by default, and evolved fined-grained permissions systems so that users would not need to give the games they downloaded access to their camera, contact information, and stored passwords.

Do we still even aspire to build trustworthy systems to keep people safe?

Depressingly, No. In an Orwellian twist, we have allowed industry to pervert the very meanings of such basic concepts as safety and trust. Back in January 2002, the year I met Ross, Bill Gates laid out a corporate vision for what 'Trust' meant to tech's de-facto leader of the time:

> Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It should be easy for users to specify appropriate use of their information including controlling the use of email they send.
> ...
> There are many changes Microsoft needs to make as a company to ensure and keep our customers' *trust* at every level – from the way *we* develop software, to *our* support efforts, to *our* operational and business practices.[5]

Regardless of what you think of Gates, Microsoft's history,[6] or the extent to which Gates and Microsoft were able to deliver on those principles, Gates was willing to state without ambiguity that 'trust' meant being accountable to customers about the quality and safety of its products.

Contrast that with today's doublespeak, where today's tech companies use '*trust and safety*' to mean protecting users from others, so that their company can control how their users' data is exploited, where their users' attention goes, and to obscure how this all happens so that users remain as oblivious as possible. The industry littered with companies we helped birth and students we helped train has redefined *trust and safety* to mean moderating others' content and access. These companies intentionally elide even the slightest consideration that their platforms, such as social networks and dating apps, might not adequately protect the public's data or might sell that data to advertisers, governments, political parties, and anyone else willing to pay.

This capture of our lexicon has been enabled by the students our academic institutions have produced and by our academic research institutions themselves, which hold conferences dominated by industry members and that embrace this language.

Industry thrives on the talent that our research institutions train and we thrive by consuming the funding they provide. Our research institutions welcome with open arms those who advanced their careers by enabling the industry's most abusive oligarchs. In addition to cozying up to companies and institutions that we know to be actively trying to subvert the public good, many of us not only

[5] Emphasis in quote added to highlight that when *Microsoft's* founder and then-CEO used the word 'trust', he used it to hold *Microsoft* accountable to its users. The original January 15, 2002 memo is reproduced available via a 10-year retrospective from Microsoft and a Wired article from January 17, 2002

[6] Disclosure: I worked at Microsoft Research from 2007 until 2016.

accept research funding from them, but brag about that research funding when brandishing our credentials. And we don't question when our institutions do it.

Many of our most prestigious scientific research institutions have helped to promote technologies that harm the public. Cornell Tech advertises its placement on CoinDesk's Best Universities for BlockChain. Stanford and Berkeley (the latter funded by cryptocurrency company Ripple) are also actively promoting their links to the '*industry*'. Our institutions show no shame for doing so because too few of dare question the propriety of our colleague's research funding,[7] and too many would ostracize those courageous enough to do so.

Have we improved the study of the science of security?

Not significantly. Our scientific culture perpetuates systems that subvert the truth. Scientists' success and prestige is not judged by the meticulousness of our methods or our caution against overstating the implications of our findings, but on how significant we can make our findings appear, how many papers we can publish, and whether these appear in venues of the highest prestige. We gather for exclusive meetings amongst our research-area elites, to decide how we will distribute prestige, and pat ourselves on the back for performing this 'community service'. Our time and effort is directed at explaining to a super-majority of researchers submitting results that their work does not meet 'the bar' for the arbitrarily-chosen acceptance rate that we believe maintains our desired aura of prestige. We put service to our employers, and industry organizations, and program committees over service to science and budding scientists.

We know these institutions pervert how we conduct and evaluate science to serve their interests, but we choose complicity rather than risk our degrees, jobs, promotions, and social status. Perpetuating system that we know to pervert science may be the default choice, *but it is a choice.* It is a choice we make unconsciously every time we dedicate a service hour to peer reviewing a work to determine if it's worthy of prestige, when we could instead be helping others conduct more meticulous research and communicate it to the public more clearly.

I do not believe that most of us don't want to make pro-social choices and better the world. And some members of our community have had huge positive social impact. Two worthy examples are efforts to democratize public key infrastructure (Let's Encrypt) and secure messaging (Signal), both through not-for-profits. These wins came from principled people who believed that it should be safer for *everyone* who wants to publish information on the web, and safer for *everyone* to communicate with others over telecommunications networks. There's a lot to learn from these *exceptional* wins, and I do not mean to diminish them, but we can't get the most out of them if we fail to understand that they are, indeed, *exceptions.* If we don't own up to our field's failures, examine our roles in those, and learn from these failures, we can't expect to fail less in the future.

[7] Until recently major universities accepted research funding from known pedophiles.

What can *we* do?

One of the underlying problems for those of us who work in security, privacy, trust, and safety is the ambiguity over *who* we are most obligated to protect. Many of us in public-facing security roles purport that protecting the public (*users*) is our paramount goal when, in fact, our first obligation is to protect our employers.

Ambiguity and deception about our motives and obligations underlie many of the failures we need to own up to: the cybersecurity industry that protects companies from the public's negligence lawsuits instead of making us safer, the cryptocurrency industry that protects organized crime's payment infrastructure at the cost of public safety, and big tech platforms that use security to justify reducing our technological autonomy and handing it over to authoritarian governments. These failures were made possible by security technologists who contributed to the illusion that they were part of an endeavor that served the public, or who stood silent while their peers engaged in such deceptions.

Whereas doctors are bound by the ethical code of nonmaleficence, there is no code that obligates those of us working in security protect and inform the public when the public interest is in conflict with that of our employer.[8] Whereas doctors can assert that they must do no harm lest they violate their oath and put their future employability at risk, we have no code to fall back on if our employers explain that killing our metaphorical patients will maximize shareholder value and that we are thus contractually obligated to do so.

We should have our own codes of nonmaleficence. We'll inevitably need more than one. That's fine. They can be like open-source licenses. A few will become popular and most people will find one of the popular ones works for them.

Not everyone needs to adopt a code of nonmaleficence for them to have impact on our field. Even a small number of us would have impact. The public would soon learn which companies and organizations were willing to employ those of us who had adopted a code of nonmaleficence and which were not. Those who know of peers who have adopted a code of nonmaleficence, but choose not to do so, will have only themselves to blame when they are asked put their shareholders over the public after being asked to present their work as that of protecting the public.

In addition to codes of behavior, we need to build a culture where we expect more from each other and help each other anticipate and make hard choices. We need to ask hard questions of each other, and we need to expect our peers to ask hard questions of us.

- "Are you confident that you are making the choice that makes people's lives better?"
- "Are you actively looking for ways you may be causing harm or are you actively trying not to look?"

[8] Breach-disclosure laws attempt to remedy a symptom of this problem, but not the underlying cause.

– "Is your ability to gauge whether this choice furthers the public interest compromised by it furthering your own interest or that of your employer?"
– "Are you confident you are the protagonist in this story?"

We need to all be a little more willing to ask ourselves, colleagues, friends, and those with power over us questions that are certain to make us all uncomfortable and some of us even angry.

Those most likely to be angered will be people in authority who fear having their power undermined. We have to be prepared for them to brush us off with indignant responses, such as "Who died and made you the asshole who thinks it's okay to ask that kind of question?"

Funny you should ask. It was *Ross Anderson.*

Acknowledgments

I am grateful to Frank Stajano and the Rossfest organizing committee for including a work that greatly deviated from their submission guidelines in trying to honor Ross. This work benefited greatly from the ideas, incisive comments, encouragement, and proofreading of/by Ben Edelman, Cormac Herley, Maritza Johnson, Andy Ozment, and Bruce Schneier.

Open problems about the forthcoming financial infrastructure of the digital society

Frank Stajano[0000-0001-9186-6798]

University of Cambridge
frank.stajano@cl.cam.ac.uk

Abstract. The migration towards digital currency appears inevitable. Technical designs for digital cash have been put forward since the 1980s. For every technical problem, from prevention of double spending to divisibility of coins to privacy protection, creative cryptographers have offered some technical solution. But no design solved all problems simultaneously, because some of the requirements are inherently contradictory.
Society is at a crossroads. A new version of the financial infrastructure of the digital society is being built under our feet, from cryptocurrencies and CBDCs to DeFi, but without a clear architectural design and without any explicit agreement about the necessary trade-offs. We must be creative in envisaging new solutions but also vigilant in anticipating the long-term consequences, for all parties, of any proposed approach: it will be hard to displace any technology that is widely deployed.
In this position paper we offer a bird's eye overview of important unresolved problems for digital currencies and decentralised finance, highlighting the societal, financial and political problems where a trade-off between conflicting requirements must be struck.
We believe it is imperative that we carry out this analysis ahead of deployment and that we make explicit choices about the properties that the financial infrastructure of the digital society must guarantee. Failure to do so risks locking us into an architecture that will unfairly benefit a few early movers with vested interests, to everyone else's detriment.

1 Introduction

Perhaps the best way for me to honour my brilliant PhD supervisor Ross Anderson is to attempt to follow his lead and venture beyond the narrow technical boundaries of security, so as to address a forthcoming societal problem that requires a long-term vision and an interdisciplinary approach. In this position paper I won't offer any solutions. We need to start with the questions.

The days of cash are numbered. It seems inevitable that cash will eventually become digital. We are not talking merely of payment methods becoming digital (tap watch to pay for coffee) but actually of currency itself becoming digital and, crucially, programmable, with banknotes and coins eventually disappearing, despite assurances to the contrary to avoid a public backlash.

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

The core technical problem of using a string of bits as cash[1] has been extensively studied by cryptographers since the early 1980s, starting with Chaum's pioneering inventions [8,6,7]; but only with the emergence of Bitcoin [15] has digital cash reached public awareness. Although today's highly volatile cryptocurrencies are unsuitable as either a medium of exchange or a store of value, they have still become a three-trillion-dollar asset class. Meanwhile, the world's major economies have been planning for Central Bank Digital Currencies (CBDCs)—despite considerable scepticism from both within [21,10] and outside [13,18].

Triggered by the Bitcoin revolution [3,16], various innovations have flourished around "blockchain" (a distributed tamper-proof ledger that no single party could manipulate), made programmable by the Smart Contracts originally proposed by Szabo [19] and then first implemented by Ethereum [5]. Under the paradigm of Decentralised Finance (DeFi) [22], financial actors may interact with each other through programmed contracts that are automatically enforced and executed without having to trust an intermediary such as a bank or a broker.

On this technology, platforms have emerged that enable peer-to-peer lending, trading, currency exchange, arbitrage, speculation, options, futures and so forth, importing the ideas and mechanisms of traditional finance into a disintermediated (and, so far, largely unregulated) parallel universe [17].

Many more original ideas are being explored in this financial Wild West, which still moves more quickly than the regulators.

2 The problem

The shift to digital currency and DeFi will cause radical transformations in the digital society. We are living this process moment by moment and we have difficulty seeing the big picture of what is happening; but it is imperative that we do. We might list various desirable properties for digital currency (unforgeability, privacy, divisibility, offline operation, trustworthiness, usability, robustness, recoverability, traceability and so forth)—and indeed clever techies have invented cryptographic methods to implement each of them—but it is impossible to build a version of digital currency with all of these good properties simultaneously, because some of them are inherently in conflict with each other.[2]

We need a long-term, big-picture vision. I believe we must first understand where we are, understand what the technology plausibly allows us to do, understand the constraints of the design space and understand the benefits and pitfalls of a hypothetical global deployment of each of the plausible variants and innovations. Then, systematise these future scenarios to inform the general public and the key decision makers before committing to any particular implementation that will exclude the alternatives and will be hard to change, once entrenched, because of backwards compatibility shackles.

[1] A seeming impossibility: bits are inherently copiable, which opens the door to multiple spending [7].

[2] Cfr. questions 2, 3 and 4 in the next section.

3 Open questions

Research questions that need exploring include the following. Although some of them may have already attracted substantial attention, we are still far from a holistic perspective.

1. What desirable properties should digital currencies and DeFi possess, for the greater good of the citizens of the digital society?
2. Where is the correct trade-off between ensuring that digital money retains its purchasing power[3] versus allowing governments and central banks to respond promptly with cash injections to potentially catastrophic emergencies such as COVID-19, the invasion of Ukraine or the inevitable recessions caused by economic cycles? On the macroeconomic front, central banks will obviously want to retain control of the levers that allow them to steer their country's economy, including the ability to print more money. Are cryptocurrencies so destabilizing to traditional monetary policies that they will be banned, as argued by Dalio [14]?
3. Where is the correct trade-off between the privacy afforded by cryptocurrency transactions [1] and the traceability required to prevent large-scale criminal abuse such as ransomware and tax evasion? While it is clearly undesirable to allow the bad guys to operate undetected, it would be just as bad to deploy a financial infrastructure that allowed pervasive surveillance by the State: evil governments would readily use such powers to crush their opposition. This trade-off has been discussed extensively but perhaps a new taxonomy might help, and it would be interesting to study how much anonymity and unlinkability the regulators of a non-evil government would still tolerate.
4. What other pairs of desirable properties of digital currencies and DeFi result in irreconcilable tensions where we can't have both and a trade-off must be sought? It would be a useful contribution to identify as many of these constraints as possible.
5. At the "meta" level, for such tussles that involve the fabric of the digital economy and thus affect all its citizens, what decision method would ensure the fairest outcome? One-head, one-vote? Centralised decision by elected representatives? Decentralised democratic decision making? Across national boundaries (cfr. question 6)? One-country, one-vote? GDP-weighted? Strong vested interests as to what "fairness" even means... Quite political!
6. Digital currencies and DeFi, as a common good, must be trans-national. Clearly each central bank will want to impose its own constraints and retain control of the money supply, yet international interoperability remains key. Is it possible to build a technological foundation that, like the Internet, works interoperably despite the local pieces being built and managed by mutually mistrustful principals? On a related note, is it possible to build a

[3] As Bitcoin originally set out to do in the wake of the 2008 financial crisis and subsequent quantitative easing.

trans-national technological foundation (the "laws of physics" of the digital universe) that a rogue evil government would not be able to subvert just by defining new national laws?

7. How to guarantee the redeemability of our digital assets against actual buying power when the digital trading platform is not under our own jurisdiction?
8. Though fintech startups have shorter time horizons, from a perspective that spans centuries (such as Dalio's [12]) we must envisage major disruptions such as the demise of the US dollar as the world's reserve currency—or even World War 3. The first two World Wars caused major resets of the world's monetary systems.[4] How should such big-picture awareness inform the design of the world's digital money infrastructure from a macroeconomic viewpoint? Will anything, besides gold, remain a reliable store of value and retain international trust? Will CBDCs only ever be fiat money?[5] What will make the CBDC of another country trustworthy? Technologically and economically, these are ultimately architectural questions about the limits of what is feasible. But the political power issues around control of the world's reserve currency are even more significant; in imagining the future we cannot pretend to ignore that such dramatic power shifts will be accompanied by large-scale military conflicts.
9. Boiling things down to the essentials, what are the substantial points of agreement and disagreement between the properties of the CBDCs (e-dollar, e-yuan, e-euro and so forth) that have been put forward in the white papers of the world's major central banks? Which of the disagreements would make these currencies incompatible, to what extent and with what consequences? Which of the incompatible alternatives is most "fair" to the various classes of citizens of the digital society? What can we learn from the small-scale trials that have already been carried out, for example in China with expiring digital yuan [4]?
10. Similarly, what are the key common points and key distinguishers of the major decentralised cryptocurrencies? Can we articulate their original visions and how they compare to what those cryptocurrencies have morphed into today?[6] Are there any invariants? What can we learn from *these* experiments? What happened that had not been expected at design time?

[4] Cfr. hyperinflation and ultimately the demise of German Mark after WW1; and Bretton Woods after WW2.

[5] Note how being tethered to the US dollar, or even to a basket of fiat currencies, as some stablecoins [9] do, is still rather different from being redeemable for gold. And what would "redeemable for gold" even mean in a decentralised transnational context? Which principal would be making the underlying promise to pay out in gold, and why should anyone trust them to uphold it? Recall how Russia never returned the 90+ tonnes of gold that Romania sent there for safeguarding in 1916.

[6] Bitcoin, for one, is now radically different in many important dimensions from what its 2008 white paper envisaged—it is only used for speculation rather than as a medium of exchange and mining is now concentrated in the hands of a few large consortia rather than distributed among all participants, to cite but two.

11. What are the incentives and interests of the incumbent players that DeFi and digital cash might displace, such as retail banks, credit card companies, stock brokers and so forth? How might such incentives influence and possibly distort the transition? What new roles could these actors take on, if any, that might leverage and exploit their existing infrastructure?
12. How to prevent digital exclusion? How will the elderly and the digitally illiterate deal with digital currency? (We see the teething problems already with digital payments, even if still based on traditional currency.) How to cater for those who, mistrusting computers, will never agree to give up physical cash? How to make the new digital systems reliable and recoverable in the face of both accidental errors and fraud? How to ensure that ordinary people won't lose their life savings just because a digital wallet or a crypto key or some other geeky gobbledygook was not backed up [20]?
13. DeFi substantially increased the attack surface for both technical attacks [23] and (given its novelty, opacity and lack of regulation) for traditional frauds at scale. While Mt. Gox's 2014 collapse started with hacking incidents (but then also involved accounting fraud from CEO Mark Karpelès), the FTX collapse of 2022, in which CEO Sam Bankman-Fried was convicted of fraud, conspiracy and money laundering in excess of 10 billion USD, was substantially a "traditional fraud" as opposed to a technical attack on the cryptocurrency protocols. Unregulated business practices have been exploited (cfr. the 2023 Peraire-Bueno brothers' MEV attack [11] on Ethereum). Could any architectural safeguards, such as formal verification, prevent such attacks, or will attacker ingenuity always find something new [2]?

4 Conclusions

I strongly believe it would be unwise to leave it to a few enterprising technical innovators (or incumbent trillion-dollar internet giants), each with their own vested interests, to define the specific subset of properties of the financial infrastructure of our future digital society, and for everyone else to have to accept them as a *fait accompli*. We have a duty to foresee where the various alternatives could lead us and anticipate the potential upsides and downsides rather than being surprised and upset by them after the fact, once it is too late to move away from the already-deployed technology.

We are at the stage where a new universe is being created and its laws of physics are being written. This new universe, the financial infrastructure of the digital society, will become a digital commons of fundamental importance and we must carefully ensure we end up with desirable properties for it. Desirable and fair, that is, for *all* the citizens who will have to live in it, including the digitally illiterate and those struggling in the bottom portion of the wealth curve.

References

1. Ghada Almashaqbeh and Ravital Solomon. "SoK: Privacy-Preserving Computing in the Blockchain Era". 2021. URL https://eprint.iacr.org/2021/727.
2. Ross Anderson and Nicholas Boucher. "If It's Provably Secure, It Probably Isn't: Why Learning from Proof Failure Is Hard". In *Proc. Security Protocols Workshop*, pages 199–204. Springer-Verlag, 2023. ISBN 978-3-031-43032-9. https://doi.org/10.1007/978-3-031-43033-6_19. URL https://arxiv.org/pdf/2305.04755.
3. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll and Edward W. Felten. "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies". In *IEEE Symposium on Security and Privacy*. 2015. URL https://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf.
4. Biagio Bossone and Ahmed Faraghallah. "Expiring money (Part I)", November 2022. URL https://blogs.worldbank.org/allaboutfinance/expiring-money-part-i.
5. Vitalik Buterin. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", 2014. URL https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf.
6. David Chaum. "Blind Signatures for Untraceable Payments". In David Chaum, Ronald L. Rivest and Alan T. Sherman (Editors), *Advances in Cryptology*, pages 199–203. Springer US, Boston, MA, 1983. ISBN 978-1-4757-0602-4. https://doi.org/10.1007/978-1-4757-0602-4_18. URL http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF.
7. David Chaum, Amos Fiat and Moni Naor. "Untraceable Electronic Cash". In Shafi Goldwasser (Editor), *Advances in Cryptology—CRYPTO '88*, volume 403 of *LNCS*, pages 319–327. Springer-Verlag, 1990, 21–25 August 1988. ISBN 978-0-387-34799-8. https://doi.org/10.1007/0-387-34799-2_25. URL https://chaum.com/wp-content/uploads/2021/12/Untraceable_Electronic_Cash.pdf.
8. David L. Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". *Commun. ACM*, **24**(2):84–88, February 1981. ISSN 0001-0782. https://doi.org/http://doi.acm.org/10.1145/358549.358563. URL https://dl.acm.org/doi/pdf/10.1145/358549.358563.
9. Jeremy Clark, Didem Demirag and Seyedehmahsa Moosavi. "Demystifying stablecoins". *Communications of the ACM*, **63**(7), July 2020. URL https://dl.acm.org/doi/pdf/10.1145/3386275.
10. Economic Affairs Committee. "Central bank digital currencies: a solution in search of a problem?" HL Paper 131, House of Lords, January 2022. URL https://publications.parliament.uk/pa/ld5802/ldselect/ldeconaf/131/131.pdf.
11. Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach and Ari Juels. "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability". In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 910–927. 2020. https://doi.org/10.1109/SP40000.2020.00040. URL https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152675.
12. Ray Dalio. *Principles for Dealing with THE CHANGING WORLD ORDER — Why Nations Succeed and Fail*. Simon & Schuster, 2021. ISBN 978-1-4711-9669-0. URL https://www.economicprinciples.org.
13. David T. Llewellyn. "Is Retail Central Bank Digital Currency A Solution Searching For A Problem?", 2024.

14. Taylor Locke. "Ray Dalio: The government 'outlawing bitcoin is a good probability"', 2021. URL https://www.cnbc.com/2021/03/26/bridgewaters-ray-dalio-good-probability-government-outlaws-bitcoin.html.
15. Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system", October 2008. URL https://web.archive.org/web/20140320135003/https://bitcoin.org/bitcoin.pdf.
16. Arvind Narayanan, Joseph Bonneau, Edward W. Felten, Andrew Miller and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016. URL https://bitcoinbook.cs.princeton.edu/.
17. Abrar Rahman, Victor Shi, Matthew Ding and Elliot Choi. "Systematization of Knowledge: Synthetic Assets, Derivatives, and On-Chain Portfolio Management". *arXiv preprint arXiv:2209.09958*, 2022. URL https://arxiv.org/pdf/2209.09958.
18. Frank Stajano. "Sleepwalking into disaster? Requirements engineering for digital cash (Position paper)". In *Proceedings of 28th Security Protocols Workshop (SPW 2023)*, page 3–19. Springer-Verlag, Berlin, Heidelberg, 2023. ISBN 978-3-031-43032-9. https://doi.org/10.1007/978-3-031-43033-6_1. URL https://www.cl.cam.ac.uk/~fms27/papers/2023-stajano-currencies.pdf.
19. Nick Szabo. "Formalizing and Securing Relationships on Public Networks". *First Monday*, **2**(9), Sep. 1997. https://doi.org/10.5210/fm.v2i9.548. URL https://firstmonday.org/ojs/index.php/fm/article/view/548.
20. Huw Thomas. "Man told he can't recover £598m of Bitcoin from tip". BBC News Online, January 2025. URL https://www.bbc.co.uk/news/articles/cj0r0dvgpy0o.
21. Christopher J Waller. "CBDC: A Solution in Search of a Problem?", August 2021. URL https://www.bis.org/review/r210806a.pdf.
22. Sam Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz and William Knottenbelt. "SoK: Decentralized Finance (DeFi)". In *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, pages 30–46. 2022. URL https://dl.acm.org/doi/pdf/10.1145/3558535.3559780.
23. Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song and Arthur Gervais. "SoK: Decentralized finance (DeFi) attacks". In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2444–2461. IEEE, 2023. URL https://csdl-downloads.ieeecomputer.org/proceedings/sp/2023/9336/00/933600c444.pdf.

Part III

Cherished memories

Cherished memories

Collected by Anh V. Vu

University of Cambridge

When Ross passed away, I set up a website at `https://anderson.love` to collect cherished memories shared by his friends, students, colleagues, and those who had not met him but learnt lessons through his book. I went through online places to collect all public tributes, and also included private messages through internal emails and handwritten notes, with consent.

A number of people responded directly to the appeal to write a short one-page note for this Festschrift. I contacted a number of others whose messages I had already collected on the website and asked them if they would condense them down to one page for inclusion here.

I believe future generations, including myself, will learn invaluable lessons from these remembrances, gaining a deeper understanding of Ross's vast contributions and how nicely he treated students and colleagues.

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

I vividly remember the first time I met Ross. He was presenting at Berkeley in 2002 on "Why Information Security Is Hard"—the manuscript that helped establish the field of research on the economics of information security. I was a PhD student there. I sent him an email, on the slim hope that he might find time to meet with me while on campus. Incredibly, he replied, and made time to meet with me—an unknown admirer of his work. He was as gracious as he was intimidating.

That was the first of many wonderful interactions I was blessed to have with him over the subsequent 20 years. And now they seem too few.

Ross was a groundbreaking scholar who fought the good fight. He was relentless in his efforts, seemingly fearless of the powers he challenged. That was inspirational. *Look,* I would tell myself, *here is a serious scholar who is not afraid to take clear positions on critical issues and speak truth to power!*

I still recall how awestruck I was during our first chat at Berkeley. Over the years, I discovered so many other facets of Ross's incredible life, including the warm, gentle, and incredibly funny side of his personality. And yet, my amazement at his intellect never faded. Over the years, Ross was to me a mentor, an inspiration, a model, and a friend. He will be deeply missed.

—Alessandro Acquisti

Ross was not just a colleague, but a beacon of inspiration for all of us who had the privilege of knowing him. His wisdom and guidance left a mark on our lives, enriching us in ways we can never fully express.

Ross had a remarkable ability to touch the lives of those around him, offering invaluable advice and unwavering support. His impact reached far beyond the confines of our workplace, extending into the hearts and minds of everyone he encountered. His legacy of kindness, generosity, and compassion will forever be cherished by all who were fortunate enough to know him.

I feel honoured and blessed to have had the opportunity to call Ross a mentor. He will always hold a special place in my heart. His legacy will continue to inspire us all.

—Maria Bada

When I started my PhD in Germany in 2003, I did not know anything about security, but was determined to learn. So I put the first edition of Ross Anderson's *Security Engineering* on my night table, and systematically read through it for several weeks every night. Some years ago I realized that everything I know about security originates from this book.

I met Ross personally much later, in 2017, on the Security and Human Behavior Workshop, and he was incredibly and unexpectedly kind to me. It was a tough time in my professional life, and I felt protected when he was around. Just so. He was also, to my great surprise, interested in my research and helped with advice and connections.

I liked most his unique humour, and especially his smile. It illuminated his face and surroundings like sunshine. Thank you, Ross.

—Zinaida Benenson

I first met Ross as an undergraduate—he was lecturing computer security. His lectures were a real inspiration: I adored the connections from cryptography to application and the many ways in which devious behaviour could cause untold trouble. As a PhD student, I bought a copy of his (then new, first edition) textbook and took pleasure in sending him a few corrections. I will also not forget him as my internal PhD examiner—a wonderful couple of hours of discussion. I remember how proud I was that someone this important had taken the time to read my dissertation in such detail.

Ross and I have continued to collaborate, in recent times as part of the Cambridge Cybercrime Centre, on a new protocol to protect whistleblowers and journalists, and co-supervising Jenny Blessing. He's been wonderful to work with: insightful, knowledgeable, and fun to chat with. He really cares about students and staff alike. We will all miss him immensely.

—Alastair Beresford

I learned something new every time I talked to Ross. More often than not during research brainstorming sessions he would wander off from the main topic to a different topic only tangentially related, which at times could be exasperating (particularly when we had a deadline) but you couldn't help but admire his ability to make connections between seemingly unrelated ideas. I remember one meeting where we started out talking about encrypted messaging and then at one point he leaned back in his chair, crossed his arms behind his head, and said "Well, when Lord Parkinson privatized the electricity industry in 1990..." I can't remember exactly what came after that or what happened when Lord Parkinson privatized the electricity industry, but he could talk at length for 20 minutes straight about the obscure topics off the top of his head.

He had a particular talent for engaging examples and quippy phrases—once, he wanted to make an analogy to reputation-based content moderation. The example that came to his mind was the way things work at an "elite gentlemen's club in London" where membership requires nomination by another member. That particular example didn't end up making it into the final version of the paper, but it was very characteristic of Ross.

It's in large part because of Ross's advocacy and research that security engineering as a discipline exists. Many in the security community as a whole now take it for granted that systems designers should think about the human outcomes of security. Ross changed the way people thought about security to the point that today it seems almost obvious that any system design should take into account usability, economic factors, and much more, making his encyclopedic textbook freely available online for all to read. He could be gruff on first impression but had a big heart and was unfailingly gracious. He will be greatly missed personally and professionally.

—Jenny Blessing

I used to think cryptography would save us. When I first met Ross, I was fresh off my first research publication and smitten by the mathematical beauty of my undergraduate cryptography classes. I envisioned a future restructured around computers enforcing fairness and safety.

I'd met a handful of other cryptography professors as potential PhD advisors and they all listened to my excitement as I rattled off problems I meant to solve with cryptography and said, "Sounds great, I'd love to work on that with you." I had tea with Ross for the first time in the canteen of the Gates building. He listened to my spiel intently, looked at me and calmly said, "Eh, those problems sound interesting but cryptography doesn't really work that way."

I realised right away that Ross was different. He didn't care about ideas just because they were elegant. He cared if they would work. He wasn't focused on tools from cryptography (or later from economics, psychology or other fields he mastered) for their own sake. He was focused on real-world problems and how technology would change and often fail when used in practice.

When I started as Ross' student, he noticed I was concerned about the early days of social media. Most of the others I spoke with dismissed it as an unserious research topic, thinking "these sites sound terrible for privacy, why would anybody use them?" Ross listened as I talked about how many young people were on Facebook and, despite having never used it himself, he got it. He realised young people felt they had no choice and that the implications of sharing so much personal data would be profound. We wrote a few papers exploring the privacy implications, but Ross also doubted encryption would solve it.

My work on passwords was similar. Passwords were the most mundane topic in all security research—technology that had barely changed since the '80s. Everybody hated them, but thought passwords would soon be replaced. Ross encouraged my interest in understanding them better. That's where the action was, even if they lacked the glamour of cryptographic techniques. I wrote my dissertation on what we could learn about passwords from data breaches. Ross and I predicted passwords would be around for "at least ten more years" and twelve years later we've been proven right.

What made Ross special? He was deeply skeptical while also being boundlessly curious. His curiosity led him to engage with problems others dismissed or overlooked. But his skepticism kept his work grounded. He intuitively grasped how complex the world was, and that almost everyone—researchers, politicians, companies—was overestimating how well they really understood what they were doing. There was nothing Ross didn't want to learn more about. He'd listen to anyone, while not taking anything they said at face value.

If I realised right away that Ross was different, I also knew right away that I wanted to be like him. Before I met him I just wanted to write prose like Ross. When I worked under him I wanted to approach research problems like Ross. Now that he's gone, I want to challenge and change my students like Ross changed me.

—Joseph Bonneau

Ross has long been a source of deep personal inspiration for me. He taught innumerable lessons in research, publishing, and technical skills, but more importantly he taught through example how to set and achieve lofty goals, how to ask the important questions, and how to redefine any system—technical or human—to make it better. Ross was honest; he did not sugarcoat feedback, and for that his students are stronger and better prepared for the "real" world. Underneath this, though, it was always abundantly clear how much Ross cared about his students, their interests, and helping them to achieve their dreams.

Ross was one-of-a-kind. He was able to balance so many different activities with grace and seemed to know something significant about everything. Ross could talk with anyone. Ross made and published significant discoveries, and taught a non-trivial portion of the population either directly or through the knowledge in his books.

Thank you, Ross, for everything.

—Nicholas Boucher

Inviting me to help found WEIS changed my career in such a fundamental way. He created this pathway and ways forward that changed my trajectory. And now I am reading that he did that to so many people, where a single interaction with him was a life inflection point.

I suppose he told you his bagpipe social engineering story: he discovered as a student on the continent that if you were in a given range of people in Germany they would drop some coins in your case. So he would march around playing of his many bagpipes in the train station, walking just close enough to people to engage the social contract—with a bagpipe—and have enough to student the day away. He told this story to me and my younger child, who played brass in band, at FC by the ocean.

I posted this when I heard, "Ross Anderson cared deeply about the human outcomes of security & policy. He did not focus his brilliance on amassing tech wealth but instead on the hardest challenges, using nuanced technical insights in fighting to protect the vulnerable."

He was one of kind. And now I suppose I will never understand the differences between the Scottish and British enlightenments.

—Jean Camp

Ross was for me like a father, after my biological father and my spiritual father confessor. It so happened that all three of them died within 15 months apart, which made the pain greater, but perhaps just bearable at the limit.

My first contact with Ross was during my undergraduate, around 2007, when I was looking for a place in Europe to make my PhD. Then I met James Whittaker, while we were both working at Microsoft (I was just an intern), who made me the link with Ross. Very soon Ross arranged an interview to get industry funding for my PhD. At this point I did not receive it, as my competitor was preferred at that time. But two years later, after completing my undergraduate and working for one year in research, I came to Cambridge with the help of Frank Stajano for a one year MPhil course. During this time, I made a project that was very interesting for Ross, as it was demonstrating in a very practical manner some vulnerabilities of the banking system, something that appealed him very much. As a result, towards the end of my MPhil Ross came in my office and said "I want to propose you for the Google PhD scholarship". This was an amazing opportunity for me, since I was looking for funding for my PhD in many places without too much success until that point; and this funding was indeed a great gift, as it covered all our necessary expenses for the four years of my studies.

But Ross continued to surprise me and gave me further gifts from the beginning of my PhD. In the very first day, he came again in my office and said (words are approximate, but keep the meaning): "We have a deadline for a conference in a few days and we need your help with some experiments". I performed the necessary experiments within the required time and even some minor contributions to the paper, which was immediately accepted at the Financial Cryptography conference 2011. At the conference I made some good friends and I even presented the paper. Many people, in particular students, were rightly surprised that I published a paper at an international venue so early in my PhD. Of course, this was mostly Ross's merit, but is yet perhaps another example of his extraordinary capabilities to publish interesting research ideas in a very efficient manner.

Ross's guidance throughout my PhD was essential in my overall determination. During my first year for example, when I had all sorts of doubts he gave me two very helpful hands (besides many others that I cannot tell now for lack of space): first of all, he encouraged me to participate at a locally organised cryptography workshop that brought many international researchers. There, I met Hugo Krawczyk (designer of HMAC), who gave me the courage to continue my search in my research area as well as some useful advice. The second hand Ross gave me was to expose me to a recent research book he received, that was rightly in the area in which I was looking for ideas. These actions may seem of little significance to some, but they were completely essential for me to clarify the direction of my PhD, which I eventually completed under the great supervision of Markus Kuhn.

—Marios Omar Choudary

Ross Anderson left us far too soon. I grieve for him and send my love to his family.

Ross was an intellectual giant and an absolute legend in computer and information security and, like any true giant, he was incredibly down-to-earth and friendly.

I first met Ross at the very beginning of my career, when I was a very junior faculty. Having been told of his famously low tolerance for idiocy, and being completely star stuck, I remember being very anxious the first time I was introduced to him. As it turns out, he was absolutely lovely and kind. Perhaps that's because the French and the Scots famously get along (by correctly blaming the English for everything that is wrong in this world), but I was impressed by his congeniality.

You can tell a lot about somebody's character just from the way they talk to higher-ups and people in lower positions. Ross' sharp and acerbic wit was solely reserved to people in position of power that, truly, should not have been there. For those of us that were not—junior faculty, students—he was an indefatigable advocate, wonderful and kind mentor, and always had time for us.

I remember in late 2010 seeing a call for a very large grant from DHS. It was a very long shot, but I wanted to apply, and I thought that some of Ross' work was a good fit for what the funding agency was looking for. So, I invited him to team up. He accepted, and I wanted to get him to be front and center on the grant given his notoriety. He said that he wouldn't mind if we thought it'd help, but that I (and Tyler Moore, at the time another junior faculty on the grant) should be running the show, not him. Often with senior faculty, that's code for "put my name on this thing, I'll take the money, but don't ask me to do anything." In Ross' case, that meant tirelessly writing entire sections and editing the whole proposal, giving us a lot of advice, and then, stepping back from the limelight. We wrote a lot of that proposal at Financial Crypto in Saint Lucia, in between cocktails and beach time.

We got the grant. It completely changed my career. Later, I heard through the grapevine that Ross was one of my biggest supporters when asked to write evaluation letters. It was incredibly helpful to have such a legend in my corner.

So, I owe Ross a lot, and I am sad that I never will be able to repay him even a fraction of everything he did for me. But, now that I am becoming slightly more senior, I will try to honor his memory by using him as a model in my interactions with junior colleagues.

Thank you, Ross.

—Nicolas Christin

I first met Ross in another century when I was working in industry and trying to persuade Governments they were doing dumb things to control the Internet, to control encryption and to listen in to everything we said in private. I was always impressed by how he would turn up, apparently unprepared, listen for a while, scribble down a few notes and then stand up and make a short intervention that made more sense than the previous speakers all put together.

Later, I was there to help him, Caspar, Ian and others kick-start FIPR, and there again at a Christmas drinks do in London when a casual conversation changed my life—he'd sounded a bit bored with teaching and I was getting bored working for an ISP. I said we should swap jobs for six months and he said perhaps not, but I could come to Cambridge and do a PhD if I wanted. He then navigated the system for me, because we were taking little notice of rules of when and how you should apply and in the following September I started to become an academic. Twenty-four years later and with much help from him and I am beginning to get the hang of it.

He was much in demand, and rightly so, to speak on panels. If he could not go he'd recommend one of his PhD students or RAs to go instead; when they would never have been asked in their own right. That's why I got a trip to Financial Cryptography in Dominica. I came back and explained the attractiveness of Caribbean islands in February (and how this conference only had talks in the morning because everyone went to the beach in the afternoon) and thereafter he always managed to be able to go to FC himself.

One of the things I have learnt over the past week is how normal these types of stories are for people who knew Ross. I've read dozens of little notes and appreciations, scattered over blog comments, or in emails by many of the people I know well, and a lot that I don't, of how Ross changed the course of their lives too, by advice, by finding some improbable way to give them a job or a speaking chance, by supporting their endeavours elsewhere, or just by being there to chat with them whilst walking the dogs.

Governments (and University hierarchies) are still doing dumb things, but Ross did so much more than most to try and change that—not least by encouraging others and by building communities that will continue the struggle to make things better.

Some people change the world through their inventions or their wise words. Ross did some of that—but he was also that rarest of people, someone who has changed the world by empowering others to do that changing for us all. RIP.

—Richard Clayton

I will always remember the first time we properly worked together (having mostly bonded over being fellow Scots in Cambridge and teasing each other about politics in the lunch queue). I've truly never met anyone like him. I so valued the time I got to spend getting to know him over many lunches at the lab, drinks at conferences, and dinners up in Edinburgh, and will miss him terribly.

—Ben Collier

Ross Anderson began working on healthcare IT in 1995. I first met Ross in July 1997 at a Rutgers DIMACS workshop[1]. I was an MIT student on an internship at Bellcore. Ross walked up to the overhead projector at dinner with his transparencies for "Security in Clinical Information Systems." He effectively created the field of healthcare cybersecurity, which led me to medical device security. Sipping cheap hotel wine with boffins from across the pond, I recall we scammed extra drink tickets. My notes from August 14, 1997 say cryptically, "Ross Anderson continued his talk on medical network security in the UK... Anderson explains that most attacks (in his medical records security experience) come from the inside. During the last dinner, Markus Kuhn and I discussed at length problems/solutions... the reasoning made sense to me after a glass of wine."

I saw Ross again in 2002 when he visited my PhD thesis advisors M. Frans Kaashoek and Ron Rivest at MIT during the Peer-to-Peer and Distributed Hash Table era. An anonymous person informed me, "Ross will be in Shafi's office. I have a key. If you'd rather be even stealthier. My lips are sealed." I don't recall the context, but I probably played a practical joke on Ross. I ended up hosting a couple talks, including one by George Danezis and Richard Clayton.

Around 2006, we reunited again. I had joined UMass Amherst after wrapping up a "predoc" at JHU with Avi Rubin. Graduate students Adam Stubblefield and Matt Green were stealing donuts by cloning my Exxon Mobile Speedpass and 125 kHz Prius keyfob. They did some really cool cryptanalysis of an RFID device. My research shifted to RFID security. I devoured the research by students at Cambridge. My students decided to reverse engineer 13.56 MHz HF contactless RFID credit cards. Worse than the ExxonMobile Speedpass, the credit card companies didn't appear to use any cryptography at all. We could clone many cards and mount replay attacks with relative ease[2]. Our paper led to snorkeling with Ross in Trindad/Tobago during a social outing at Financial Cryptography, but my mask was not fitting properly. Ross ended up staying on the boat with me to chat research. We hit it off. We interacted often on medical device security, especially pacemaker security[3]. He hosted my talk at Cambridge, introducing me to the OG faculty lunch. One of our last interactions was his memorable webinar while I was Acting Director of Medical Device Security at the U.S. Food and Drug Administration (FDA)[4].

Now 28 years and several additional diopters after I first met Ross, we gather here today to remember a man who had such a lasting impact on so many minds and souls. Thank you, Ross, for welcoming me to the field so many decades ago, and thanks for being a supportive friend. I'll miss your wisdom and wit. May you rest in peace.

—Kevin Fu

[1] http://archive.dimacs.rutgers.edu/drei/1997/schedule/Speaker-list.htm
[2] https://www.nytimes.com/2006/10/23/business/23card.html
[3] https://thaw.org/2019/05/29/ieee-award/
[4] "Security Engineering of Machine Learning" by Ross Anderson, 2022 https://www.youtube.com/watch?v=ykMw9ps9a4g

I recall first meeting Ross Anderson at the initial ACM Conference on Communications and Computing Security, in November 1993. Ross presented his landmark paper explaining "Why Cryptosystems Fail," The paper revealed a deep understanding of how cryptosystems are misused in practice, displaying significant insights acquired in banking over many years. It was with good reason that Roger Needham was proud to introduce Ross to the security old-timers as his bright PhD student and up-and-coming researcher. Many of us noticed that a star of our field was born then. The last time I had a chance to speak with Ross was about his future research plans, during Summer 2023 and my sabbatical leave at University of Cambridge.

Over the intervening decades I took note of three of Ross' traits. First, he had a wicked sense of humor that became evident even when he reflected on his own work. Indeed, his *Security Engineering* book, which has become a landmark textbook, was written in an engaging storytelling manner rather than dry academic prose. Once he gleefully noted that an advantage of writing a storytelling book is that one is no longer tempted to change a story when convenient.

Second, Ross had an uncommon intellectual curiosity that led to the establishment of new fields of security, including security economics and security and human behavior; their importance escaped many researchers who believed that engineering and mathematics are all that matter in achieving information security. My own work on the foundations of trust in computer systems and networks, as well as the "axioms" of insecurity and usable security, was based on key ideas of behavioral economics, and was motivated in part by Ross' insight that economics and human behavior will always play an important role in our field.

Third, Ross was generous in expressing his appreciation for others' novel research results. During my sabbatical visits to Cambridge I noticed his dedication to students' research, his encouragement, and the wealth of new ideas which he shared with them.

Ross was a proud Scot. While on a sabbatical leave at Carnegie Mellon University, which was founded on Scottish traditions, he regaled my family with his after-dinner bagpipe performances that rivaled the best of the local pipers. We were amazed that he traveled with his small set of pipes and upon arrival was quick to find a cohort of pipers in Pittsburgh.

More recently, he shared with me and others his profound disappointment with the mandatory retirement policy at Cambridge and his determination not to let this event curb his desire to continue researching, teaching, and mentoring students. More than anything else during this difficult time, he relied on the love of his life, Shireen, his wife of over three decades.

Ross's untimely death left a major void in the life of many. Nevertheless, his star will continue to shine in the heavenly crown of computer science for future generations.

—Virgil Gligor

Ross Anderson had quite a fearsome reputation for cutting through real-world cryptographic systems like a hot knife through butter with simple and cheap practical attacks. As he created the Information Hiding Workshop and supervised much early research in the space, Ross was one of the founders of the field of anonymous communications. After a Security Protocols Workshop presentation on mixnets with Andrei Serjantov, Ross invited myself and Ania Piotrowska to Cambridge for an in-person security seminar on our new Nym mixnet. I was naturally rather terrified given his reputation. After a perfectly cordial seminar and lunch at Robinson College, we were in for a surprise.

"Blockchains are a scam to separate foolish people from their money!" Ross thundered in the narrow hallways of the Security Group. As the idea of an "electronic annuity" was indeed invented in his own Eternity Service paper, in the end Ross agreed that *perhaps* there was a real use of a blockchain for Nym in replacing the Tor directory authority. I ended up walking Ross through our prospectus, telling Ross that we had to – rather awkwardly for an anonymous communication system – do extensive identity checks on our token holders in order to be compliant with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations.

"KYC," Ross retorted, "is a privacy-invasive tool of the US and the banks to crush their opposition." He proceeded to give us an in-depth take-down of the various legal reasons for this invasion of identity, reminding us that it was indeed our own all-too-human identities in our own company paperwork that were the fatal flaw in our own anonymity system. Ross argued vehemently that no cryptography in the world could save us from the authorities showing up at our door and simply forcing us, via either court orders or a rubber-hose, into putting a backdoor into our own system. Ross argued that decentralization made the problem even worse, as then *anyone* could add a backdoor. We spent the rest of the afternoon discussing how to secure software supply chains in excruciating detail.

At the end of the long day, Ross gave us a signed copy of *Security Engineering* which I then put in the office of Nym for all our programmers to read. Ross had an abiding passion for using economics to enable turning his vision of the Eternity Service into reality. Ross was indeed mildly terrifying but he was a genuinely wonderful person dedicated to building secure—and even anonymous—systems.

—Harry Halpin

Ross was the first person (besides my PI) I got in contact with when I arrived to Cambridge. He included me in a discussion group he was organising and we had some great discussions about security and software architecture.

Maybe this sounds like a small thing, but for me it was huge considering the pandemic situation. It helped me to meet new people and provided a platform to interact with the department members, and it truly made a difference. I will always be grateful for his support.

—Jasmin Jahić

I first met Ross online, in September 1994, while I was an undergraduate at FAU Erlangen. I had just developed several ways to circumvent a pay-TV scrambling system used in the UK and Ross approached me by email to say that he had broken a "multiplex shift register keystream generator" (Cryptologia, July 1990), which he believed to be used in that same system. We soon had regular exchanges about hardware security, reverse engineering, cryptography, steganography, censorship resistance, and more. By January 1995, only a month after submitting his own PhD, he asked about my plans for the future and whether I would be interested in joining his security research group at Cambridge to do a PhD. He was keen to publish what we discussed and so we started to collaborate on our first papers on tamper resistance.

We first met in person in June 1996, at the Isaac Newton Institute, where he ran a half-year programme at the time. I was immediately impressed by how many of the most famous and influential names from the world of coding theory, cryptography and computer security he had brought together there, and the wide range of topics he was interested in and collaborating on, with lots of people. He was always exploring new aspects of the wider field, picked up new ideas quickly and enthusiastically, and was able to communicate them in the most engaging ways, whether in discussions, talks or papers. We met again at conferences in the U.S. while I spent 1996/97 at Purdue doing a masters. After his fruitful suggestion that I apply for an EU scholarship to do a PhD in Cambridge, I finally joined him at the Computer Laboratory in October 1997. It was housed in somewhat grim buildings at the time, with comparably limited facilities, but the Security Group that Ross had taken over from Roger Needham turned out to be a very productive place and we soon wrote more papers, on Tempest and steganography. By 2001 the department had moved into a nice new building in West Cambridge and offered me a lectureship.

Ross was not the meticulous theoretician, nor much of a computing practitioner. (For example, he taught software engineering for decades without ever being fluent in a programming language.) But he was always keenly interested in topics that directly affect people in the real world and he inspired many students to do clever and influential work. He spent enormous energy on fighting for consumer protection, such as holding banks to account over flaws in their procedures and computer systems, and their attempts to pass on liability and the burden of proof to customers when things went wrong. His early papers on these topics contained some of the most engaging writing I had ever seen in scholarly communication. He also was keenly aware of the value of the University as a self-governing community of scholars, and uncompromisingly committed to protect it as a place for creativity and freedom against overbearing administrative interference.

Ross was a real force of nature and a great storyteller. He was never boring. I will miss him very much and hope many of his fights will continue.

—Markus Kuhn

Ross transformed my life.

He saw the pressure of the job I was under, the limitless gas of excuses, the heat of the logic that was hidden from me. He taught me to turn heat into light, to articulate, to shine, and to write. Let others react to my work, instead of rolling around in the mud with jobsworths.

I want his family to know this, because I have no doubt his writing and his teaching took him away from them often.

More than anything he taught me that a real hero shouldn't have a nemesis. To really be human one must transcend petty embodiments and target the abstract and reactionary injustices of the world wherever and in whomever they are found.

He showed me that I wasn't alone, and that crucially my new allies were people all over the world of different lived experiences. They might be young or old, of a dizzying array of genders, or skin tones, and that we would change things by what we write: be it code or legal precedents. I will miss his irascible nature, his childish jokes, and his mature discussions. I have his books, and his writing, and a community brought together by him (even now).

To Shireen, I am very sorry you have lost him so suddenly, but I am grateful you lent him to the rest of us from time to time. It didn't just change my life, it changed me as a person. I know I'm not the only one, and this book will help you see what he did when he wasn't with you.

—Eireann Leverett

Ross made a profound impact on me. He was an outstanding mentor who set a positive example of how to be an effective academic and a genuinely good person.

His mentorship style was very effective. He provided plenty of guidance, advice, and feedback. But he also kept a healthy enough distance that helped me grow into an independent scholar. I'll never forget our first meeting in his office. He explained to me that at the end of the first year, I'll have a viva. Until then, he told me I was free "to work on whatever the hell I want", and that we'd figure out if it worked at the viva. Of course, I saw him plenty that first year, and he was always generous with his time when I had questions or needed feedback. But we never had regularly scheduled meetings. Instead, Ross would randomly pop into my office (which was next door to his) any time he had something that he thought might be of interest to me or if he had an idea he wanted to talk through. Those meetings would invariably lead to discussions of what I was working on, and in that way shaped my path.

Ross always sought out opportunities to elevate his PhD students (and really, any junior scholars). I benefited directly. Anytime he was asked to speak, if he had a conflict, he would recommend one of his students instead. That's how I got to travel all over Europe, from Austria to Cyprus, giving keynotes on security economics as a PhD student. It's also how I co-authored a paper with him in Science and a report for the European Commission. And the best part was, I was never just his stand-in. He expected real contributions, treating me as a fellow scholar even before I felt like one. Only later did I realize that by sharing these opportunities he helped make it true.

Ross imparted on me the importance of working on real problems that people care about. He valued collaboration and sought it out at every opportunity. And he was never satisfied with the status quo. He was unafraid to argue for change when warranted. I have done my best to internalize these lessons in my own career, inspired by his example.

On a more personal level, I always enjoyed the times he invited the Security Group to his home in Wrestlingworth. Shireen cooked a delicious meal, and the conversations would go on for hours. During one such visit, Ross broke out his bagpipes. Needless to say, the sound was impressively loud, particularly in a small dining room!

Finally, I really appreciated getting to know Shireen better during Financial Crypto conferences. Shireen, Jillian and "the moms" (my mother and mother-in-law) would hang out at the beach while Ross and I attended sessions. Then at meals and in the evenings and social events we would all come together and enjoy each other's company. I will always cherish those memories.

—Tyler Moore

I want to note how important Ross Anderson was, not just within the UK digital community, but globally. He was the model of a politically and socially involved computer scientist. When I first heard of him in the 90s, he was doggedly trying to point out that the then security protections against ATM (cashpoint) fraud were too weak, and that the banks were blaming customers for leaking their PIN codes when in fact, those codes were eminently crackable.

After that, he was *the* key figure in fighting restrictions on cryptography in the UK, putting together a coalition of CS experts in founding the Foundation for Information Policy Research, and then becoming one of the key advisors to the Labour party. As a gruff, Scottish socialist, Ross was tailormade to act as a counterbalance to the United States' heavy lobbying of the Blair administration to tow the line on making usable crypto illegal outside of the United States.

FIPR and its successes spawned a strong, and experienced digital rights community in the UK early on. It was Ross and Caspar Bowden (who also sadly passed away far too early) who were crucial in encouraging this group to work with others in Europe to form EDRi, which remains the core of digital rights advocacy in Brussels. If you've ever wondered why the EU occasionally comes up with good cyberlegislation, it's because of the influence of EDRi – and that coordination came from Ross and Caspar recognising that the real decisions were being made not in the UK or the US, but in the growing work of the EU.

But at the same time as doing this political work, Ross was also building the foundations of a serious cybersecurity approach. He applied political, economic and social aspects to computer security models: his early writing on /where/ to put the liability for computer security flaws are still influencing approaches to legal liability now. He drew deeply from actual uses of technology: my favourite memory of him is him explaining how the Irish Republican Army passed around secrets under the nose of the British Army to an amazed BBC journalist.

Ross' high reputation allowed Cambridge University to lure Microsoft funding for their infosec department. The results of that collaboration indirectly led to CHERI, a capability-based security system designed by the brightest minds in the UK and beyond, and still the great hope for truly robust digital security.

Ross was still working on the cutting edge: the other week, Cory Doctorow pointed me to a paper he co-authored recently on how ML models might collapse in the face of ingested ML-generated content. When I devoted a chunk of a lightning talk to him at EthDenver, a prominent Filecoin ecosystem participant came up to me afterwards to thank me for highlighting Ross' work, as he had been instrumental in supporting her early career. Ross was grumpy, unforgiving, a blistering writer of flaming emails, and sometimes oblivious of the effect his disapproval could have on others. But he pursued and achieved singularly useful advances in the field of information security, and in the wider, messier world of digital rights and global politics. He was mad at Cambridge for forcing him to retire at 67, and he was right – not just from a political point of view, but from the truth that he still had so much to give. He died too soon.

—Danny O'Brien

This collection of memories of Ross will have many fine descriptions of his achievements and character, and I'll be able to add little in technical terms. Ross was a great help to us at the Royal Society and other institutions, with his scientific and technical excellence, his enthusiasm and energy, and his exceptional integrity. Since so many others here are better able to describe his work I'll just mention one area, not involving computing at all, in which we had a mutual interest—Scottish and Irish traditional music. Ross was both a good player of various bagpipes, and also collected and was very knowledgable about sources and origins of the music. Talking over such things was a pleasant diversion in the breaks between meetings on much more pressing matters of security policy.

The last time Ross and I played together was in a pub session in Cambridge a couple of weeks before his death—he on pipes and I on fiddle and accordion. He was on great form, with much amusement about some technical issues with one of his sets of pipes, and a good cross section of music styles with the other musicians present. There is a huge collection of traditional tunes and dance music to play together. Seeing him in such good form made his sudden death so soon afterwards an even greater shock. However, 'Maireann an ceol' as the Gaels say, as does the memory of Ross.

—John Pethica

The first time I met Ross in person was in his office at the University of Edinburgh, just a few days after I arrived in Scotland. He greeted me warmly, asking about my journey to the UK and how I was adjusting to life here. Ross shared stories about his time living in Scotland and his first job working on small submarines in Edinburgh. We then discussed my PhD plan, ranging from network effects in economics to AI-powered vulnerability discovery and repair. Additionally, he suggested numerous study materials, including classic books and online courses. This meeting gave me a profound sense of his extensive knowledge across diverse fields. Our second meeting was a month later in Cambridge. I stayed at Churchill College. Ross invited me to the college dinner, where I also met his wife, Shireen, and his grandson, Ivan. We shared a wonderful meal together. Afterward, Ross showed me around the computer lab and introduced me to other PhD students. In his old office, Ross gifted me a copy of the third edition of his book *Security Engineering*. Inside the cover, he wrote: "*To Lawrence: Welcome to the front line!*". It was a hefty book, I have always cherished it. At Edinburgh, this book is the main textbook for the course of the same name, which Ross cotaught with Yuvraj, and I served as a teaching assistant. He visited Edinburgh nearly every week during the spring term to teach this course. Ross was one of the most respected professors here, and the interactions with him left a lasting impact to both faculty and students. He was always passionate about engaging students in discussions during class, encouraging them to think more deeply by asking questions. I also learned a lot from sitting in on his lectures. Ross had remarkable energy, and his schedule was always packed. I still remember the small thick notebook he carried everywhere—he often pulled it out to check the schedule. Although Ross spent most of his time in Cambridge, we frequently communicated through emails and online meetings. He regularly sent me news, blogs, and papers that he found interesting and thought would be helpful for me, discussing them with me to spark new ideas. Since several months before I arrived in the UK, Ross has invited me to join the weekly reading groups and group discussions at both Cambridge and Edinburgh, which has helped me smoothly adapt to my PhD studies. Combined with our own supervision meeting, I met him 4–5 times a week. All of this benefited me immensely.

The last time I saw Ross was the Wednesday before his passing; he came to teach the final tutorial. We had dinner with my other supervisor, Daniel, at Café Andaluz. We talked a lot, covering topics ranging from the Chaos Computer Club to his great-uncle's experiences during World War I. Ross was staying at the Marriott Hotel at that time, which was on the way to my apartment, so we could take a walk together. I walked him to the hotel, shook his hand, and we said goodbye. I never imagined it would be our last. So many memories—words fall short. Ross was always patient with me and offered all the help he could, both in my studies and in life. As his only PhD student at Edinburgh, I will never forget his guidance and the time we spent together. Thank you, Ross. I will always miss you, and may you rest in peace.

—Yangheran Piao

A beautiful mind has left us. I lost an esteemed colleague, dear friend, and mentor. Ross's influence stretched far beyond his role as a Professor at the University of Cambridge; he was a world-renowned figure whose brilliance and impact resonated throughout information and computer security research, spanning generations of researchers and scholars.

His intellect was unique, his research groundbreaking, and his dedication unbreakable. Ross was able to fuse profound knowledge with an incredible moral compass. He fearlessly championed privacy and information access rights, raising his voice against the misuse of technology and governmental overreach, always advocating for justice and integrity. And his impact is enormous. Beyond his academic fame, Ross was a living repository of wisdom, his mind a vast library of historical knowledge. His influence reaches beyond our immediate community, shaping the broader technology and policy landscape.

I had the privilege of knowing Ross and calling him a friend, and I was deeply touched by his genuine kindness and willingness to lend a helping hand. He embodied the true essence of compassion and generosity, leaving a legacy that will endure eternally.

To Ross's family, I extend my deepest condolences. May you find comfort in knowing that his legacy will continue to inspire countless individuals.

Ross, though you are no longer with us, your spirit will forever reside in the hearts and minds of all touched by your brilliance and kindness. Lastly, I borrowed a snippet from the known poem "Do Not Stand at My Grave and Weep" that I thought fits you well:

"I do not stand at your grave and weep.
You are a thousand winds that blow,
You are the diamond glints on snow,
You are the sunlight on ripened grain,
You are the gentle autumn rain.
..."

—Ahmad-Reza Sadeghi

I can't remember when I first met Ross. Of course it was before 2008, when we created the Security and Human Behavior workshop. It was well before 2001, when we created the Workshop on Economics and Information Security. (Okay, he created both—I helped.) It was before 1998, when we wrote about the problems with key escrow systems. I was one of the people he brought to the Newton Institute, at Cambridge University, for the six-month cryptography residency program he ran (I mistakenly didn't stay the whole time)—that was in 1996.

I know I was at the first Fast Software Encryption workshop in December 1993, another conference he created. There I presented the Blowfish encryption algorithm. Pulling an old first-edition of Applied Cryptography (the one with the blue cover) down from the shelf, I see his name in the acknowledgments. Which means that sometime in early 1993—probably at Eurocrypt in Lofthus, Norway—I, as an unpublished book author who had only written a couple of crypto articles for Dr. Dobb's Journal, asked him to read and comment on my book manuscript. And he said yes. Which means I mailed him a paper copy. And he read it. And mailed his handwritten comments back to me. In an envelope with stamps. Because that's how we did it back then.

I have known Ross for over thirty years, as both a colleague and a friend. He was enthusiastic, brilliant, opinionated, articulate, curmudgeonly, and kind. Pick up any of his academic papers—there are many—and odds are that you will find a least one unexpected insight. He was a cryptographer and security engineer, but also very much a generalist. He published on block cipher cryptanalysis in the 1990s, and the security of large-language models last year. He started conferences like nobody's business. His masterwork book, Security Engineering—now in its third edition—is as comprehensive a tome on cybersecurity and related topics as you could imagine. (Also note his fifteen-lecture video series on that same page. If you have never heard Ross lecture, you're in for a treat.) He was the first person to understand that security problems are often actually economic problems. He was the first person to make a lot of those sorts of connections. He fought against surveillance and backdoors, and for academic freedom. He didn't suffer fools in either government or the corporate world.

He's listed in the acknowledgments as a reader of every one of my books from Beyond Fear on. Recently, we'd see each other a couple of times a year: at this or that workshop or event. The last time I saw him was last June, at SHB 2023, in Pittsburgh. We were having dinner on Alessandro Acquisti's rooftop patio, celebrating another successful workshop. He was going to attend my Workshop on Reimagining Democracy in December, but he had to cancel at the last minute. (He sent me the talk he was going to give. I will see about posting it.) The day before he died, we were discussing how to accommodate everyone who registered for this year's SHB workshop. I learned something from him every single time we talked. And I am not the only one.

My heart goes out to his wife Shireen and his family. We lost him much too soon.

—Bruce Schneier

I first met Ross Anderson around 1993. I was a crypto nerd all excited about PGP, and I attended a talk he gave at Cambridge, entitled "Why cryptosystems fail". He talked about how banking systems claim to be infallible but in fact make a number of engineering mistakes that enable a variety of frauds. He explained the frauds, not in the abstract but with reference to actual cases; then daringly asserted that the banks made the mistakes but denied the evidence and blamed the victims. Wow, that was hot stuff! I was riveted in my seat. "We need people like this to tell it straight, stick it to the man and defend us poor consumers", I thought. Who was this guy? I didn't know it then, but the speaker was just a lowly PhD student, a mature PhD student of computer security pioneer Roger Needham. He had graduated from Cambridge in maths some 15–20 years before and had since worked around the world in various fields, including banking. And then, having saved enough to pay for graduate studies, he had gone back for a PhD, and he had taken to research like a fish to water. This was to become his first high profile paper. In the meantime, a few years after attending that lecture, I also came to his same decision of returning to university to earn a PhD as a mature student. By then he was a newly minted Assistant Professor with half a dozen PhD students, none of whom had graduated yet. "If I'm going to do a PhD at Cambridge", I told myself, "I can't miss the chance of working with this guy." That was one of the best decisions I ever took. As an academic, I learnt my craft from him. He had an uncommon talent for storytelling, for writing compelling and perfectly formed prose in his first draft, and for never backing down when someone powerful disagreed with him. He explored new fields with enormous intellectual curiosity and he had an uncanny ability to act as the catalyst that would create a new community and bring it to critical mass. He did that many times, founding a long sequence of workshops, conferences and organisations, from the uk-crypto mailing list to the Foundation for Information Policy Research, the Information Hiding workshop, the Fast Sofware Encryption workshop, the Workshop on Economics and Information Security, the one on Security and Human Behaviour, and I'm missing out plenty more. I remember he religiously took notes at every one of our security seminars, whoever the speaker was, building an extensive knowledge base from first-hand sources that he then distilled into his book, *Security Engineering*, which he wrote during the last year of my PhD. Now his encyclopedic 1200 page volume, which he kept updating till his third edition in 2020, is a must-read for anyone doing anything in security, and it's amazing that a single person could have so many insightful things to say on so many facets of our field. I'm rambling a bit by now, sorry; it's very sad to see him go at only 67, but I hope I am conveying a little bit of why I chose him, of why I was excited at the prospect of working with him, and of why I feel that choosing him as my PhD supervisor was one of the most significant decisions in my career. And I had no idea at the time that, after completing my own PhD, I would be appointed to a Cambridge lectureship myself and become his colleague. Thanks Ross, rest in peace and thank you for everything.

—Frank Stajano

In my second year at university David Simner suggested that reading Ross' textbook *Security Engineering* was good preparation, and so over the course of a few weeks that autumn I read it cover to cover. Now I am a Senior Lecturer in cybersecurity, and one of the places that began was there. I still recommend that anyone involved in security read the latest edition of that book, because of the way it so clearly and accessibly explains and systematises such a huge breadth of important topics in cybersecurity.

So many people owe so much to Ross. His broad understanding of cybersecurity that proactively drew in other disciplines and created fields like security economics. His commitment to civil society through the cryptowars, patient privacy, government IT, and civil liberties. His commitment to his family and friends, and his support for disadvantaged people. While much of what he did was public, some of the most important things were only visible if you got close.

He made a huge difference to the careers of many people (including my own), with many of his PhD students and postdocs going on to obtain faculty, or other senior roles where they have in turn had a huge impact. He supported a diversity of thought and brought people into the department from a range of disciplines, helping to redefine what computer science is.

He had a huge impact on the University of Cambridge (once named "most powerful person") through a range of campaigns and several terms on the University Council. He was ever a *critical* friend of the Vice Chancellor and played an important role in uncovering various kinds of corruption, mismanagement and discrimination. I learnt a lot from him through that. For a while he chaired the Cycling and Walking Sub Group of the Transport Working Group of which I was secretary. I think our first formal joint work was our proposed policy on cycling and walking, which was completely ignored by the University. He fought with me for the rights of postdocs to continue to be allowed to vote in University democracy (we lost). He was always someone you wanted by your side in a fight.

Ever one to have a memorable turn of phrase, in his battles with the central administrators he'd plant a little ghost of himself in their heads so that every time they thought of doing something silly (e.g. on IP) the ghost would remind them of what response that would get and so put them off—saving much time.

Another memorable description was of the zombie government policies on cryptography, or ID cards, or NHS IT. Ross and others would keep killing these policies off, carrying them away and burying them deep under the ground. Only for the policies to claw their way back out again after the next election.

One of our many great losses is that we will no longer have Ross in our ranks as we fight these good fights. However, many of us carry the memory of Ross, and a model of what he might do. Often a helpful starting point.

He was not perfect, like all of us he made mistakes, and sometimes enemies, but he was our friend and we loved him. We will miss him. He leaves both a void and a great many people who he trained to fill it. Ross was a giant and he helped us stand on his shoulders. He showed us that humans could be heroes.

—Daniel Thomas

Ross Anderson invited me to lecture more than twenty years ago at the computer lab at Cambridge. Since then, I have had the honor of meeting with students and faculty almost yearly to present information about locks and their insecurity. I will miss our discussions, lectures, and Friday afternoon sessions.

A few years ago, while interacting with his students and colleagues, I realized I should consider writing a book about lock manufacturers' insecurity engineering to complement his *Security Engineering*, which has become the gold standard for analyzing what can go wrong in computer-based systems.

I discussed the idea with Ross, and he was entirely in favor of such work, mainly because he did not understand locks and could not open his office file cabinet! Ross connected me with Wiley, his publisher, reviewed the text, and made suggestions during the three-year writing process. In no small measure due to his efforts, the result was *Tobias on Locks and Insecurity Engineering*, a seven-hundred-page treatise on why physical security systems can often be compromised.

The security world will miss Ross Anderson's insight and expertise. I counted him as a friend, colleague, and mentor. He left us too soon, and his imprint will remain forever.

—Marc Weber Tobias

Ross sat on the committee that interviewed me for my first job at Cambridge and was the first person to take me for a walk around the building and outside on a sunny day when I arrived. We discussed various topics, and my initial impression was that he knew everything so thoroughly, while I knew nothing.

I went back to Vietnam six months later due to the pandemic, then returned to the UK in late 2020 to renew my visa. I got stuck in a room far from the lab due to restrictions. Ross came to help me collect and scan all necessary documents, not once but twice. When I concerned about the infection risk and suggested waiting until I finished self-quarantine, he reassured me: "*Don't risk the visa, though. I can handle hazardous materials. Look, I pick up dog poo every time I take the dogs for a walk. I can't imagine that your passport is more hazardous!*" I deeply appreciate his care for me, and I'm certain he cared for others too.

Ross cared about my family as much as he cared about me. My uncle was diagnosed with craniopharyngioma in 2023. Once Ross learned about it, he tried everything to connect me with the best surgeons in Cambridge and India. My uncle unfortunately did not get to travel, but Ross's help meant so much to us. He was incredibly generous, always spending his time and patience correcting my mistakes, not just in research but also in my English. He often told me, "Your English is broken," but always explained why it was wrong and how to fix it. He gave me compliments when I did good work, even for minor achievements, and that encouraged me greatly. I truly felt reassured having him by my side.

The last major thing we did together was moving his bookshelf to the new office, as Cambridge forced him to retire. He of course did not like that. It took us a few weekends. He told me he had been in the old office for almost 30 years and would miss it. He hoped he could stay in the new office for another 20 years. I wished the same. He showed me a card his mom and dad had given him long ago, and with his great smile, I knew he deeply cherished it. I always wanted to have a picture with him when I graduated, and I promised to give him a copy of my thesis later this year. Sadly, I will never have that chance and honour.

Our last interaction was just before his passing. I saw him editing his webpage to make all the chapters of his book publicly available. He had always wanted to do so but had been blocked by copyright restrictions. Later, he knocked on my door – just as he always did to say goodbye before heading home when we were both working late – and told me he would be in Edinburgh for a few days and would see me after Easter. Sadly, it was the last time I saw his smile.

I admire Ross not only for his vast contributions in many ways, his enthusiasm, his boundless energy, his passion, and his inspiration, but also for his kindness and the way he treated students and colleagues. He always seized every opportunity to lift me (and his students) up and introduced me to those he thought could help. I know nature is cruel, and that death is part of life's beauty, but it has been incredibly heartbreaking to lose him so early and so suddenly. His life was very well-lived, and his immense contributions will never be forgotten by many generations of students, colleagues, and friends. I miss him terribly.

—Anh V. Vu

It is hard to overstate the impact that Ross Anderson has had on my life over the last 25 years. His invitation for me to join him for a summer internship with the Cambridge security research group opened up a new world of research and friendship. Leigh and I remember clearly a rattling drive through the countryside with David Wheeler to join Ross and Shireen for the security-group summer garden party that year. The internship led to an invitation to return for a PhD—an offer that I only took up six years later, once Leigh had begun her own PhD at Cambridge. It is extremely difficult to imagine the halls of the Lab without the sound of his voice and his excitement about the latest ideas in the world of computer security (and beyond). He was always just a few doors down, having become a colleague but still always a mentor. It is comforting to know that there remain so many people, both at the Lab and across the many international communities he worked with, who likewise benefited not just from his research, but also his generously given mentorship and friendship. We will miss him deeply.

—Robert N. M. Watson

Ross was a **pragmatic visionary**. He critically observed situations, identified how the situation should be, determined what would be needed to get there, and made it happen. He not only applied this strategy very successfully to his own career, but to the careers of many of us, changing our lives for the better.

Ross was a serial **community builder**. With other bright minds, he founded new disciplines and communities, including WEIS and SHB. Ross and I set up Decepticon, which is still a vibrant research community today. Ross would attend all conferences and religiously take notes for lightbluetouchpaper.org.

Ross taught me to **think big**. How do we get the key researchers in our scientific committee? How do we get this research on the front page of the New York Times? Or even, how can this work lead to a Nobel Prize? He encouraged his students to do cutting-edge, meaningful research and to share it widely.

Ross believed in **cross-disciplinary synergy**, that one plus one could be so much more than two. He hired grad students and postdocs from various backgrounds, including computer scientists, criminologists, economists, lawyers, and psychologists like me. This led to vibrant Friday lab meetings where security topics were discussed from a variety of angles, leading to unexpected insights.

Ross was **idealistic**. His papers, books, MOOCs, he would make sure they were freely accessible to everyone. He believed that academic information should be open, but private information be protected. He demonstrated the fallibility of anonymizing sensitive data and that documents can often be retrieved from a wiped smartphone. Ross dedicated his career to protecting people's privacy.

Ross was famous for advocating his **strong opinions**. I believe one of his quotes ended up on a wall at GCHQ. But I admire most that he always listened with an **open mind**. He was **endlessly curious**, read more and about a wider range of topics than anyone could comprehend. But if you disagreed with him and posed a solid argument, he would use this input to update and, when relevant, change his opinion. Ross always gave me the feeling that what I said mattered.

Ross was **part of a team**. When Ross organized a conference at the lab, Shireen would be there to host it, making everyone welcome. When I felt torn between staying or moving back to the Netherlands, Shireen took me to the pub to listen. The next morning, Ross would come into my office to offer a solution.

Ross was a **great mentor and friend**. He was one of the most generous people I have ever met. Ross had a strong influence on the careers and lives of many, mine included. **He cared this deeply for many people.** When I left Cambridge, Ross threw me a goodbye party, serving pink prosecco. Since, we have enjoyed many little trips. Listening to Ross in the Smithsonian's National Air and Space Museum made me regret not studying aerospace engineering.

The last contact we had was the day before Ross passed away. We were planning to meet up during his next visit to the Netherlands. I was already looking up art exhibitions, wondering which one he would like best. With Ross' passing, academia lost a great mind, society lost an advocate for human rights, and we all lost a truly great friend who will be missed dearly.

—Sophie van der Zee

Part IV

Family eulogies
Churchill College
22 June 2024

from Iain Anderson

Ross.

It's hard to know how to describe my unique brother.

Brilliant, big, awkward, loving, blunt, loyal, curmudgeonly, international authority, gourmand, champion of the underdog, organiser, teacher, bagpiper, multilinguistic, Professor at one of the oldest and foremost universities in the world and adviser to two of the companies that underpin our modern world, Infosys and Google. And like his hero Newton, an FRS. He was neurodivergent in more than one sense of the word and certainly a polymath in every sense of the word.

More importantly, he was a loving husband, father, grandfather, friend and brother. And there is now a great big Ross-shaped hole in our lives.

Our Aunt Kathleen, now over 90, recounts how our mum struggled to get him to leave his number tables and go outside to play. Maybe a future pointer.

Ross grew up just outside Glasgow, in a culture famed more in the 1970s for stoicism and conformity than for breadth of vision or diversity. Ross was different: he excelled at school in Glasgow rather the local one—good in some ways, but hard in others.

While most played football, Ross played the bagpipes and competed in Highland games, even Pibroch, the obscure complicated pipe music of the expert.

He took his exams early but things weren't easy. Different school, different looks, different hobbies, different brain... Cambridge was a welcome haven.

After University he wanted to travel and set off for Iran—to see some ancient mathematical writings. Unfortunately, the Islamic revolution got in the way and he ended up backpacking in the Yemen, where he came much closer than one would wish to a factional shoot-out in his hostel. Thereafter, busking around Europe playing his pipes in his kilt was a comparative stroll.

Shortly after we spent a memorable day together at an early Notting Hill carnival, Ross decided to forsake a rather interesting squat in Lambeth where floor boards appeared optional and headed for South Africa: a journey that changed his life for ever for the better, as it was in SA that he met Shireen.

Eventually Ross came back to do a PhD then join the staff at Cambridge, becoming an international expert and Professor in Computer Security Engineering. His talent and hard work led to the highest recognition. Winner of the Lovelace Medal—the UK's top award in computing and a Fellow of the Royal Society. Becoming FRS may not be exclusive in Cambridge but it certainly is in almost any other academic environment. His achievements made his family all extremely proud and I pinch myself at all he accomplished: lauded author of the foremost book in his field, 302 published papers, honorary degrees and fellowships but nicer still were the sentiments expressed in the online obituaries. Touching quotes praise his ability to show equal interest in students and colleagues of all levels.

While much of his work is obscure to the lay person, it also included how you and I choose secure passwords for our apps. On the web you'll see him lecture

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

with engaging yet simple clarity. As he put it, "Real work for real people with real adversaries".

Just as Ross's work could reach downwards from these ivory towers it reached upwards and outwards. Ross could tie together IT with politics, economics and psychology and wasn't afraid to do so.

He was unwilling to let others be trampled by governments, industry or institutions. A man of principle, of fairness and of fearlessness in speaking up—in bank fraud, health records, freedom of information and music: a breadth of engagement that is, frankly, astounding. He fought injustice relentlessly, to the very end. As Bavani said, a moral fibre made of steel ran through him. Yet a glance at his wiki page—there is almost nothing explicit on his own achievements.

It has been said that a gentleman knows how to play the pipes but chooses not to and, other than the occasional outburst, Ross mostly forsook his Scottish pipes for social propriety but found other smaller versions with which to entertain his family, and indeed, anyone else who would listen. Ross organised piping groups, was an expert on piping music and its history and composed pipe music—he named one piece after a favourite dog, Dogmatix. It's wonderful to hear his pipes played today.

He adored his dogs and walked them every day—doubtless they became experts in calculus, coding and pibroch, amongst many other things, from the phone calls he often made as they walked.

Ross also liked good food and trees, the former, of course, enhanced by marrying wisely.

Ross could be brusque and misunderstood. He could be intense, blunt and emphatic. He was that way because he cared. So please pause to consider this question. How did someone with Ross's social and interactive limitations come from a background where conformity was the norm, to achieve and interact so widely and so laudably?

His academic surroundings contributed but there is no doubt that the enduring driving force of his greatness was love.

Love from Shireen and from Bavani and their family all of whom Ross adored and from whom who he drew joy and grounding.

Ross was also very close to his grandchildren to Ivan, Lily Rani, Temujin-Ved and he shared a particular understanding with Bella.

Shireen transformed Ross, smoothed his rough edges and steered and supported him in his many social interactions, never mind his dress sense. Shireen, you gave him the confidence, space and interactive skills to progress as he did. Ross was immensely proud of you, Shireen, in too many ways to list but that included your love, patience, your active engagement in his work and the College life that meant so much to him. Shireen, you made him so much more than he could have been without you. He really appreciated that and I'm so sorry you've been robbed of more time together.

Ross told me often, over the years, how much academic and College life meant to him. The breadth of discussion from young and old—admiration for the old and particular enthusiasm for the views of young colleagues. He talked about

community and the stimulation it gave him. He loved life here, wanted to share it with others and fought for it to continue while he still had so many active ideas to pursue.

Ross, my wonderful brother, gifted beyond my comprehension, his leaving has been hard to comprehend. I'd much I still wanted to ask and learn from him but besides his achievements and talents, I treasure his desire for fairness, his treatment of all as equals and his complete embrace of diversity ahead of his time. A glance at the obituaries and comments from many around the world confirms that I'm far from alone in that. We can celebrate a full life, well lived in the love of Shireen and family and the friendship of his colleagues here and around the world.

The young Ross piped in competitions at Luss Highland games on the Bonnie Banks of Loch Lomond, a beautiful place about which there is a well known traditional Scottish song. The song describes a story of love and imminent execution of a Scots warrior in England after which the departed soul will return immediately to Scotland via the Low road of death while the grieving will return slowly via the High road. Exiled Scots often pine for their homeland but I don't think Ross will do that. His heart and soul will be happy here, close to the love of his family and friends in this famous institution of whose history he will now become part.

from Lily-Rani Anderson

Despite the tragic reason we are here today, I'm glad that I'm learning all this stuff I would never have known about my Grandfather. The only thing I can think of is how cool he always was. The stories about him I heard at the funeral and in all the condolence letters that were sent make me appreciate him in a whole different way. His life was all so much bigger than I imagined.

My mum and I used to call the short jobs he did and events he went to "Sidequests" because he was always busy with multiple things and no one in our family knew exactly what they were about. We think of him as James Bond because he could be in another country at any time on a Sidequest and we wouldn't know about it until afterwards. When I told him that recently he laughed a lot and that made it so much funnier.

Just knowing he was there was comforting. I still feel his support when I play the musical instruments that he bought me or remember him telling me that I needed more motivation to start my driving lessons. He will always just be Dada to me. He reminded us often that we have to walk the dogs even when it's cold and he could answer almost any question we ever asked him.

I guess now he won't ever have to eat a Brussel Sprout at Christmas again—even though—let's be real—the last few years he got away with eating just half a Brussel Sprout a year.

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

from Bavani Anderson

I am Ross' daughter. Together with my mother and his 4 grandchildren I am here to celebrate Ross Anderson as a unique and irreplaceable father, grandfather and husband who loved us, his family, unconditionally.

In my life, I have met more computer scientists than any other group of professionals—since my Dad started his academic career, countless computer scientists have been in our home to enjoy my parents' hospitality. Even so, when a friend asked me recently what exactly my Dad did as a Security Engineer—I didn't have a snappy answer to hand. The person who I would have asked is no longer here—so I did the next best thing and checked his book. His book, *Security Engineering—A Guide to Building Dependable Distributed Systems* is, according to very many posts online, regarded as the greatest achievement of his professional career and possibly his most influential legacy.

I would say that my Dad's most notable achievement was, in fact, falling in love with my mother and getting her to fall in love with him in return. Together they were a powerful team. Having my mother's love and support at his back gave him the courage to go out and conquer the world every day for decades.

In his book my Dad said:

> "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."

I am not a computer scientist, but reading this made me think that my Dad was indeed a very wily fox. It seems to me that he utilised these same principles to build a family and raise a child and grandchildren.

My Dad's personal set of core values were very simple, but they were unshakeable and unbreakable. Once he had thought through a proposed plan of action, and decided to commit to it, he set his course and would not be swayed. Before becoming my father, he thought it through for some time—and from the moment that he made his decision he committed himself wholeheartedly to fulfil the role to the best of his abilities—come hell or high water (or hormonal teenagers) he never wavered from his decision to be a good father—and, later, grandfather.

Unconditional love as in unlimited, unqualified, unreserved, unrestricted, complete, absolute and unequivocal love is a challenge for most parents to show their children, in practice, but my Dad pulled it off—and he made it look easy without any fuss.

My Dad's contributions to the field of Security Engineering, and in campaigning for the protection of human rights, may have been his life's work, professionally speaking, but his family was also his life's work. He loved being

In F. Stajano (Ed.), *Rossfest Festschrift*, privately published, 2025. Not peer reviewed.
© retained by the author(s). Licensed under CC BY-NC-ND 4.0.

a husband and father and a grandfather. He didn't really have two halves to his life—his professional and personal lives were based on the same values and approach.

In raising me, his goal was to raise a child capable of remaining dependable in the face of malice, error or mischance. He enabled me with the tools, processes and methods that I need to live my life fully and independently and adapt as my environment evolves.

My Dad's approach to parenting was that his child—and then grandchildren—were just short humans who would hopefully one day grow taller. He answered any question we put to him as if he were speaking to a short, intelligent person—he didn't censor his answers and if he didn't know the answer he would research it and come back to the conversation later. After a couple of grandchildren, he did learn to tailor the delivery of his answers to fit the attention span of his audience. He enjoyed our curiosity about the world instead of being annoyed by it. The questions I have heard him answer over the years range from the mundane to the epic—"How do trees eat?" "What is God?" "How do steam engines actually work?" "Why do we have elections?" "Why doesn't the Forth Bridge fall down" "Why do I have to wash my hands" "Why can't boys have handbags?" "Why can't I eat a tadpole?" "Can birds fly in the rain?" "Why do other people think I'm weird?" "Why do suns explode?" "Why is life so unfair?".

He wasn't just all talk though—he did get stuck in on the practical side to—he spent an inordinate amount of time in Addenbrooke's Hospital Accident and Emergency Waiting Room (usually at night) with various grandchildren. He travelled all round the country to take one of us visit steam railways—he spent hours in the bird sanctuary when one of us went through a bird watching phase—he went on lots of tree spotting walks with the one of us who loves trees—and he always went to a couple of pantomime shows every year.

My Dad was a genius, he was born with an amazingly gifted mind—he was a musician, engineer, scientist, humanitarian, linguist... the list is long—he was interested in the bagpipes, opera, art, philosophy, politics, dogs and nature. None of us in his family can match his wide range of interests—but luckily for him—there are benefits to having 6 of us—between us he never lacked at least one interested companion to join him in attending the opera, concerts or plays, fine dining, visiting art exhibitions, hanging out with the dogs, looking for interesting trees or discussing human rights, politics or philosophy.

He has never told me who to be, what to believe, what to do, what to wear, what to eat or who to vote for. To paraphrase a quote from Bruce Schneier:

> "An alien thinks as well as a human but not like a human—Ross is one of those rare people who can think like an alien and then explain that thinking to humans."

My dad hated lazy thinking—that and idleness. He said lazy thinking and idleness lead to bad engineering. Bad engineering is a term he used regularly, and it could apply to everything from bad engineering of governmental and large organisational policies, the design of petrol pumps and multi-storey car parks as well as any decision that I needed to make.

He taught me how to think—he invested a lot of effort in teaching me how to think. I will share with you a conversation I had with him about 25 years ago—whenever we spoke told each other if we had come across anything interesting—that day he said he had read an article about Picasso and the writer had said, the really interesting thing about Picasso was that he trained as a fine artist and his skills as a classical portrait artist were exceptional—so he learnt the rules of fine art before he broke them. My Dad was very annoyed by this—he said "What's so interesting about that"—there was some swearing about lazy thinking on the part of the journalist—then he said learning the rules and then breaking them is easy—the interesting part is thinking about who made the rules? Why did they make the rules? What was their motivation? Whose interests were the rules designed to protect? When were the rules made—are the rules still fit for purpose in the current environment or social structure? "Our kid", he said, "if you are going to break the rules, first decide if they need to be broken."

So my Dad used his brilliant, blinding, kaleidoscope of an alien mind to teach me how to think for myself. Any time I faced a difficulty or a crisis, he would try to help me think of a solution myself. He allowed us to develop by making our own mistakes and finding our own goals and aspirations.

He never burdened us with his expectations.

Sometimes even he admitted that the only solution was to endure—when all else failed he would say—"Come on, how do you eat an elephant? One bite at a time, our kid, and you will get through it. Slog through the mud and the muck until you get to the other side."

He was the structural support of our family—he was always there, and often his support was invisible—if there was any issue I couldn't solve myself—as soon as I asked him for help he would be there—he would step in, on request, to fight battles for me, he always had my back—whether the issues were big or small. Day or night, wherever he was in the world he would answer my calls. I called him once while he was abroad and the first thing he said was—"I've got exactly 7 minutes before I go into the conference room—I'm on as keynote speaker—if you need me now I'll tell the organisers to re-arrange my slot—if not I'll call you tonight".

All I had said up to that point was "Hi".

Many people have said that my Dad was a rebel, a fearless warrior, a tireless campaigner. Those people are wrong. There were things he was afraid of—he feared harm coming to the people and principles that he cared about—so he fought to protect them. He did get tired from the stupendous amount of work that he did protect us—his family—and to protect and educate others—he got tired from taking up the fights that others were either not courageous enough, or capable enough to take up.

He wasn't a rebel—he made conscious decisions to either disregard, or campaign to change, rules which were not fair or fit for purpose. He wasn't a fighter—he was a protector and a teacher.

Some have said that he could be intimidating. Well—the only thing about him that I found intimidating was his ferocious work ethic. Alongside all that

work, he made time to look after us. For example, when I mentioned about 10 years ago that I was going to get a mobile phone for my daughter he just said "Mmm", but a few days later he sent me links to a lot of research on the negative effects of social media exposure on the mental health of young girls. Later—when one of his grandsons became a teenager—he did a lot of work looking into the disturbing undercurrents on the web that could influence teenage boys to think that misogyny and gender-based violence are acceptable manly attitudes. In the last week that he was with us, he sent me an email to say that he had been keeping track of various drug trials that could benefit his granddaughter who has potentially life-threatening allergies, and he was happy about a new drug that had been approved for use here.

All of the innumerable strands of his thoughts, actions and interests were entwined with his love for his family.

He didn't set much store by fame and fortune or accolades and awards. Once he had achieved something he just moved on to the next thing he wanted to do.

As a parent he didn't try to instil his principles or views in me, but because he parented by example, I have turned out to be a lot more like him that he had anticipated.

He said a few times, "Ahh, your life would be so much easier if you took after your mother instead of after me!"

My Dad was always honest—he was honest with himself too—he taught me that self-awareness is vital—you need to know your own shortcomings so that you can either overcome them—or work around them.

Well, unfortunately I don't have my mother's beauty, grace, elegance, or sociable and easily lovable nature.

Thanks to my Dad, I take after him in that I am capable of being the structural support for my family, of standing up to injustice, of being a self-sufficient, independent thinker who is hard working, loyal, kind and open-minded.

Just like my Dad I also often also swear like a trooper, don't suffer fools easily, have terrible parking skills and I love my family deeply, fiercely and quietly.

My Dad was the only person in the world who truly understood me and, even knowing my shortcomings, he loved me unconditionally. We have never once fallen out with each other. Other than the time I spent studying, we have never lived more than 10 miles away from each other. That is a conscious decision that I made—a bit of good engineering on my part.

We spoke all the time about anything and everything—and, despite his shortcomings, I loved him unconditionally too. To me he was perfectly imperfect. I have no regrets about our relationship—there is nothing that I would have liked to do with him or say to him that I didn't do or say.

At some point I went from being "our kid" to being "Daughter Dear". The last thing I said to him was "I love you." and he said "I love you too, Daughter Dear"—which is how we ended every conversation—and both of us meant it, every time.

My Dad had a lot of joy in his life—he weaved many small moments of joy into his days—he was happy every time he went for a dog walk, played his pipes,

told us one of his small repertoire of Dad jokes or even smaller repertoire of slightly saucy limericks, chatted with his grandchildren, read a book on the sofa surrounded by his dogs, sneakily ate a Bounty bar, had a good meal with people whose company he enjoyed, had an interesting conversation with a friend or a decent glass of wine with my mother.

I am Ross Anderson's daughter, and I wouldn't feel like I do now, if he hadn't been a fantastically quirky and brilliant father.

He left me without warning. It was like a supernova—the catastrophic explosion of my guiding star—blinding, shocking, unforgettable and silent. The silence that he has left in my life is deafening. This heart-rending pain of living with that silence is the worst pain that I have ever felt. However, there is a certain honour to be found in grieving the loss of such great and irreplaceable love. I feel privileged not only to be his daughter—I feel very privileged to feel this magnitude of loss.

Thank you.