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.

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.