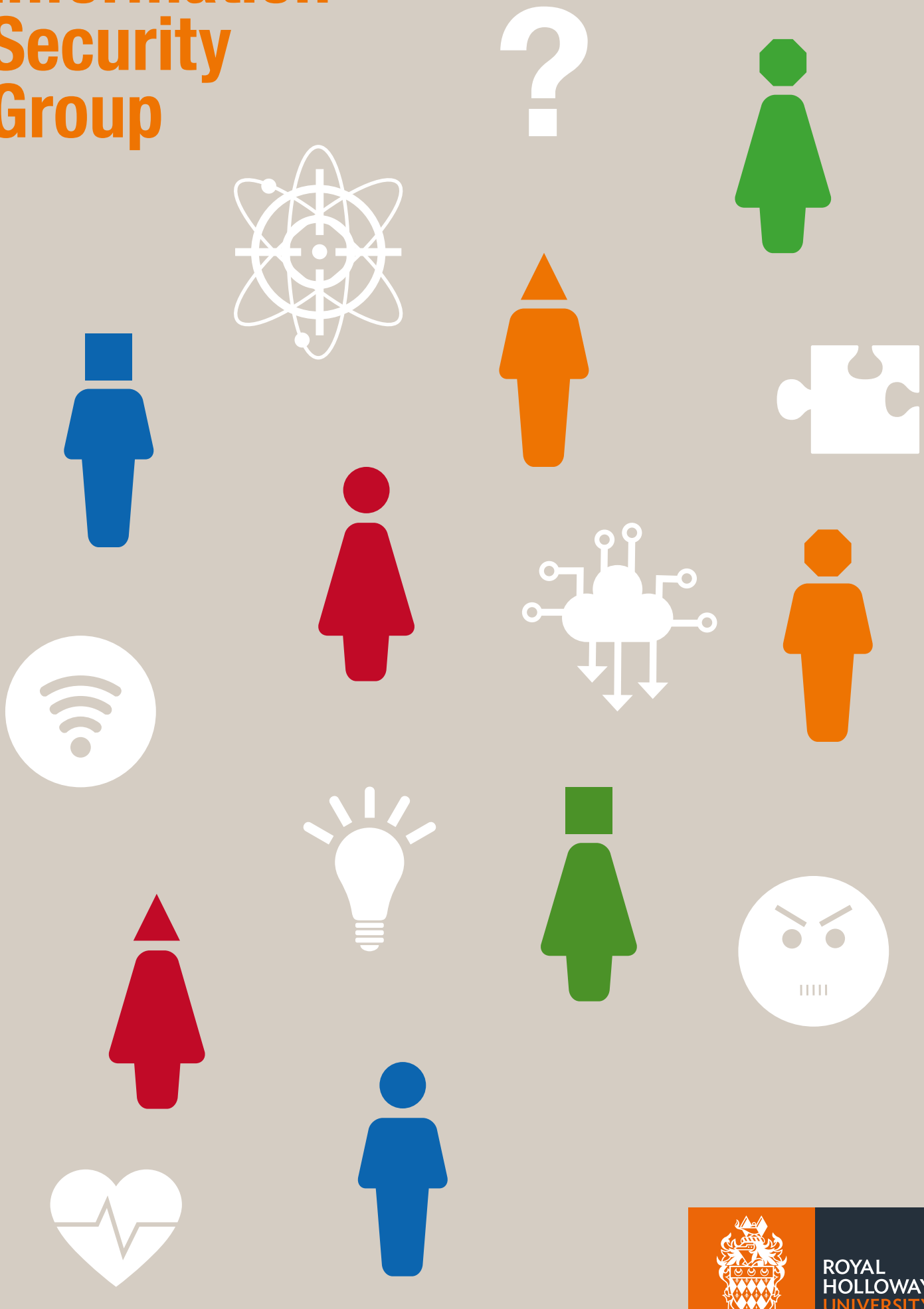
Information Security Group

Review 18/19



ROYAL HOLLOWAY UNIVERSITY OF LONDON

WELCOME — LIVING WITH CHANGE

Peter Komisarczuk

> Professor ISG, Director of the Information Security Group

Welcome to the 2018-19 ISG review. This issue finds the ISG living through some changes and this introduction provides a brief overview of some of the developments over this past year and some of the changes to come. There are many aspects around this review that remain similar to last year – more students and more teaching, more successes in research funding and research outputs and further work nationally and internationally, as well as winning our bid to continue our Centre for Doctoral Training re-envisioned around "Cyber Security for the Everyday". There are also review articles that provide a remembrance; we celebrated the life of Professor Mike Walker who passed away in September and we say farewell to Professor Kenny Paterson who has left the ISG to join ETH in Zurich.

The academic year 2018-19 saw the formation of the new School of Computer Science, Information Security and Mathematics on 1st August 2018, which had taken a considerable effort to form during 2017-18. However, after just a few days, we saw the disillusion of the new school as the College decided to undertake a much more extensive restructure.

The College is now well underway in its move from a faculties-based structure to a new schools-based structure. The drivers are many-fold and include more autonomy and flexibility at a school level, closer integration of departments and, from a College perspective, the optimisation of administrative functions. This restructure is nearing completion with ISG to join the new school of Engineering, Physical and Mathematical Sciences on 1st August 2019. The school brings together the ISG with Computer Science, Mathematics, Physics and Electronic Engineering.

This academic year has brought other challenges as several colleagues have decided to leave the ISG/College for pastures new. In September Professor Lorenzo Cavallaro left to join Kings College, in March Professor Kenny Paterson left to join ETH and Dr Bertram Poettering left in April to join IBM Zurich. This has been the largest change in the makeup of the ISG for many years and we are in the process of filling 3 lecturer positions (which includes one new position funded through research successes) and a Professorial/Reader position. The aim is to see these positions filled in 2019. This circumstance provides an opportunity to reflect on how we may grow and change, which we are embracing through some vision and strategy workshops.

April saw the ISG moved into the refurbished Bedford building which we share with Computer Science. This allows the ISG to come together under one roof. There are new facilities for the research groups with lab space for the Smart Card & IoT Centre, the S3Lab and extended teaching lab space that provides around a 150% increase in specialist teaching labs. The top floor also includes a significant open plan area for our PhD students and a CDT room on the lower ground floor. Additionally, as announced in a news item on 19th December 2018, we have more facilities in the pipeline with a new Cyber Security and Big Data Innovation Centre, to be built over the next few years, with funding from the College and £5 million from the Enterprise M3 Lep (EM3). This new building will incorporate several features specifically for cyber security as well as space for business incubation and to develop student entrepreneurship.

Overall, the outlook is looking very positive for the year ahead, with new opportunities and capabilities. I am sure we will see more exciting and interesting opportunities and challenges over the next few years as we see additional facilities put in place!

INDEX

MSC UPDATE
Jorge Blasco Alis

> Lecturer ISG. MSc Course Director

The MSc in Information Security was launched in 1992. The MSc was the first of its kind anywhere in the world. From its inception it has always been aimed at meeting the needs of the real world, and the ISG has continued to maintain and develop its strong links with industry and government, whilst reaching out to wider local and (inter)national communities.

In its first year, the MSc had 7 full-time students and 3 part-timers. Today, we have more; quite a few more! In fact, we now have more than 300 MSc students and a network of more than 4000 MSc alumni spread across the world. Our student population has not only grown, it has also become increasingly diverse. During these years, we've been introducing new modules, updating the contents of the core ones and introducing a new range of assessment and teaching methods for our students.

However, we can always do more. In the last few years, we've seen how information security has gone from being a field strongly tied to computer science and mathematics to becoming a truly multi-disciplinary field bringing together a wide range of perspectives and approaches to understanding one central topic: security. An example of this is our most recent optional module: "Human Aspects of Information Security and Privacy". In just two years, it has attracted more than 100 students overall. This evolution also needs to be reflected in our MSc programme. During the next few years, we will therefore be updating the contents and structure of the programme to reflect this change and to keep our MSc at the forefront of Information Security.

In addition to supporting wider disciplinary diversity, we are also working hard to attract more women into our field. Last year, women represented 25% of our student population. Although, historically, this was our most successful year in this regard, and way above the 11% of women making up the cybersecurity workforce, we still need to work harder.

The Women In the Security Domain and/Or Mathematics (WISDOM) group has been working towards this end very successfully during the last year. Of course, the WISDOM group is also open to our MSc students so that they can benefit from a range of events and activities during their time at Royal Holloway.

Each year there are two £500 prizes that are awarded during our December graduation ceremony. The first of these is awarded to the most outstanding MSc student of the year. This year the prize was awarded to Gage Boyle who achieved an overall average of 92% – an outstanding performance. The second prize is awarded to the student that achieved the highest mark for the MSc dissertation. The prize was awarded to Alex Kerr. Of course, both these students received a Distinction grade for the MSc – truly deserved!!

FAREWELL KENNY

Keith Martin

> Professor ISG, Director of the CDT in Cyber Security

Everyone in the ISG would like to wish Prof. Kenny Paterson all the very best on his appointment as a Professor of Computer Science at ETH Zurich. This is a magnificent achievement since ETH Zurich is regularly cited as a "top ten" world university, and is a reward for Kenny's tireless drive to conduct and promote research in applied cryptography.

Kenny has now left Royal Holloway three times, so there is little evidence that this will be his last departure! His first spell was as a PhD student, between 1990 and 1993. I first came across him as "Mike's wee brother", where Mike was a fellow undergraduate in the mathematics classes I was attending at the University of Glasgow, and his "wee brother" was occasionally skipping ahead a few years to attend some of our classes. In 1990, Kenny became the fourth in a batch of Glasgow maths graduates who were attracted south to Surrey's leafy suburbs after having been introduced to coding and cryptography during a "Maths for Communications" module, and further encouraged by Glasgow lecturer Dr Mick Ganley who, unbeknownst to us, was an undercover agent for Fred Piper.

Following his PhD, Kenny scoped Zurich out for a year as a postdoc at the Swiss Federal Institute for Technology, clearly filing away a secret passion for banks, jewellery shops and trains that run on time. He returned to Royal Holloway as a postdoc between 1994 and 1996, before joining Hewlett-Packard Laboratories, where he spent the next five years sizing up an industrial career. Alas, the magnetism of Fred proved all too much for Kenny (as for many before him) and, in 2001, he joined a rapidly expanding ISG, becoming a professor in 2004.

Careers are not established in single moments, but there is no doubt that Kenny's award of an EPSRC Leadership Fellow in 2010 was transformational in terms of the impact of his research. Freed from the tyrannies of staff-student committee meetings and exam marking, Kenny spent the next five years dedicated to his project on bridging theory and practice in cryptography. Prior to this, there was an established community of applied cryptographers who engineered the cryptography used in real systems. In a somewhat parallel universe, methodologies for modelling cryptographic security were under development, but these typically failed to capture many of the important practical aspects of deploying cryptography. Kenny's project intended to bring these two communities together.

Kenny is not someone who does things half-heartedly and he fully intended to make a success of this fellowship. I know that he felt under real pressure to deliver. However, he did much more than that. The legacy of his fellowship is not just a series of outstanding research papers on the security of important internet protocols such as SSH and TLS, it's the establishment and consolidation of an entirely new field of cryptographic research. Kenny co-founded the Real World Cryptography series of international workshops, which are now the best-attended cryptography research events in the world. Theory and practice in cryptography no longer needs a bridge – Kenny played a major role in pushing these two communities together.

As a result of his endeavours, Kenny walked tall amongst the cryptographic research community and many of the top international stars such as Mihir Bellare started beating a path to Egham. Gongs and positions of responsibility followed: a Google Distinguished Paper Award, an IRTF Applied Networking Research prize, an Award for Outstanding Research in Privacy Enhancing Technologies, Programme Chair at Eurocrypt 2011, Editor-in-Chief of the Journal of Cryptology, Fellow of the IACR and, of course, ISG Director of Research Impact 2018.

It's true that the ISG is losing someone who has achieved undoubted excellence in their field of research, but what we will miss more is Kenny the colleague, Kenny the supervisor and Kenny the role model.

For me, I greatly appreciate Kenny's West-of-Scotland, no-nonsense approach to the workplace: aim high, work hard and compete; yet, never fail to see the funny side of life. As a colleague, I have always regarded him as a "voice of sanity" and a reminder that we should never settle for second best if a grade higher is achievable. He has the gift, as a teacher, of explaining complex ideas with simplicity and clarity. He has supervised some of the finest PhD researchers that the ISG has ever produced (apart from Kenny himself, obviously!) and mentored some outstanding postdoctoral researchers. Just as many researchers mentored by Fred ended up working at the ISG, now several mentored by Kenny do so.

Kenny never planned to stay so long in Egham. In his own words: "Royal Holloway gets under your skin. I'd particularly like to thank Fred, whose hand has been on the tiller throughout my career, invisibly guiding me. I will miss the many interactions with colleagues, MSc and PhD students. I've especially enjoyed working with the Centre for Doctorial Training and am impressed how far ahead these students are of where I was at the same stage. I am confident about the future of the ISG, so long as the goodwill and teamwork that epitomizes the ISG continues. Both myself and the ISG are undergoing changes - change is scary and difficult, but some change is good."

Perhaps the thing I am going to miss most is Kenny's delightful edge. Kenny never hesitates to call a gardening implement what it truly is! Few PhD students ever forget the task that Kenny sets them on the whiteboard when they come to interview. Others have told me of their clawing fear when giving a seminar and seeing Kenny's hand go up. But, perhaps much more because of this edge than despite it, Kenny is someone who generates enormous respect. Here are some answers from our staff and PhD students when asked to describe Kenny in a single word: scrupulous, inspiring, standards (no pun intended), committed, witty, friendly, charismatic, sharp, kind, approachable, giving, unassuming (really??), mentor, fierce, Walkman, missed, tall, Scottish, 561, sprightly, no-prisoners, supportive, authoritative, unicycling, dynamic, RC4-nemesis, focused, shoeless, cryptoprince (that's my favourite!), semi-scary, …

Farewell cryptoprince, we look forward to your cheese fondues.

HOW STABLE ARE TODAY'S STANDARDS FOR CRYPTOGRAPHY?

Chris Mitchell

> Professor ISG

I have been involved in helping write cryptography standards for over 30 years, and in that time much has changed. In many ways the situation is much more stable than it was in the late 1980s, when there was a shortage of well-accepted candidates for many types of cryptography, e.g. for cryptographic hash functions. By contrast, with the exception of the potential impact of large-scale general-purpose quantum computers on asymmetric cryptography, current cryptography standards are in a fairly mature state. Over the last twenty years, complexity-theoretic models for most cryptographic techniques have been developed and used to prove a wide range of schemes and protocols secure, subject to assumptions about the difficulty of certain well-known 'hard' computational problems. This has helped provide a robust and stable set of standardised algorithms, suitable for use in most applications.

Supporting the stability claim, since cryptographic standardss started appearing in the 1980s, very few internationally standardised techniques have been broken. This suggests that the standards process is reasonably effective in adopting robust algorithms. There are, of course, exceptions, for a variety of reasons. In this piece we look at key examples of 'failed' algorithms, or algorithms which failed to be standardised because of suspicions about them, in the hope it will provide lessons for the future. Because of my involvement, the discussion is biased towards ISO/IEC standards.

Back in 1993, the US National Institute for Standards and Technology (NIST) published FIPS PUB 180, standardising the Secure Hash Algorithm (SHA), now referred to as SHA-0 although it was never officially called this. In 2005, shortly after publication, it was withdrawn and replaced by SHA-1, a slightly modified version, where the '1' denoted 'revision 1' but has since been used to denote one in a series of standardised hash-functions. The reason for the revision was the presence of a flaw in the original design, although the flaw was not published by NIST. Subsequent academic research confirmed the presence of significant weaknesses in the SHA-0 design, which were not present in SHA-1. SHA-1 was subsequently included in ISO/IEC 10118-3. Ten years after its NIST adoption, Chinese cryptographers Wang, Yin and Yu described new cryptanalysis showing that SHA-1 was much weaker than previously thought, and that collisions (i.e. two inputs giving the same input) could be feasibly found. Although a colliding pair was not known, this serious potential weakness led to new uses of SHA-1 being deprecated by NIST and ISO/IEC, and users were instead encouraged to adopt members of the SHA-2 family (also promulgated by NIST), such as the SHA-256 scheme. In fact, it wasn't until 2017 that a SHA-1 collision was published (see https://shattered.io/).

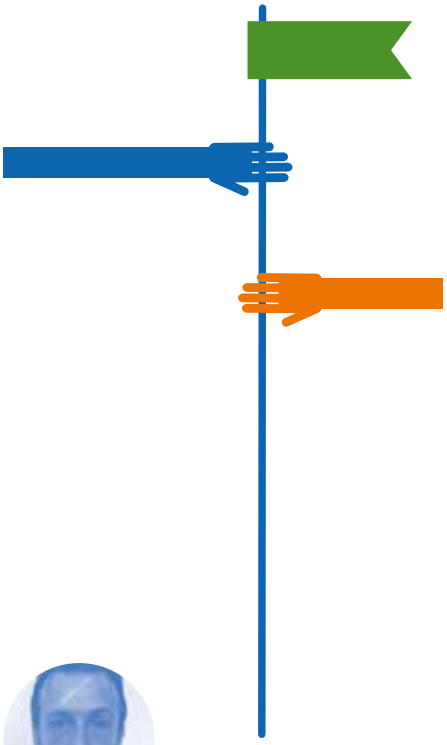
The second example is rather infamous; it involves a pseudo-random bit generator known as Dual EC DRBG (Dual Elliptic Curve Deterministic Random Bit Generator) that was included in a NIST standard and in ISO/IEC 18031. The following quote from 2016 summarises the situation: 'it seems that a random bit generation algorithm of dubious security ... was included in ISO/IEC 18031, along with a set of [NIST-provided] "recommended parameters". Only because of Snowden did the world suddenly realise that the technique had originally been designed to allow the scheme to be broken if the parameters are chosen carefully (but only by the chooser of the parameters). Moreover, the "recommended parameters" were of unknown provenance'. As soon as this became known, Dual EC DRBG was removed from both NIST and ISO/IEC standards.
That is, it is widely believed that the US government had engineered a set of parameters which ensured that they could 'break' the scheme, but that no one else could. It also emerges that pressure was put on some major software providers to make Dual EC DRBG the default method of random bit generation, e.g. as used to generate cryptographic keys. As might be imagined, this series of events hugely damaged the reputation of US cryptography standard makers, such as NIST. The resulting catastrophic loss of trust played a major part in the next issue.

Over the last five years, a major controversy has arisen over two NSA-designed block ciphers (SIMON and SPECK) proposed for adoption by ISO/IEC. After a long battle it was decided in 2018 not to standardise them, despite the fact that no one has found any significant weakness even after major efforts world-leading cryptographers. The main issue was one of trust, and in particular whether NSA might have included hidden backdoors in the ciphers – this lack of trust is a direct consequence of the furore over Dual EC DRBG. My own view is that the negative reaction to these algorithms has been over-played, and that new algorithms proposed by other governments (e.g. China and Russia) have not had the same level of scrutiny. The designers of SIMON and SPECK were required to provide detailed design rationales which have not been asked of other proposers of new algorithms, setting a precedent which may cause future problems.

Very recently (in late 2018), OCB 2.0, an authenticated encryption scheme included in ISO/IEC 19772, has been broken. OCB 2.0 is a method for using a block cipher to encrypt data so its confidentiality is protected and its integrity can be verified. This break was completely unexpected as OCB 2.0 has a mathematical proof of security produced by Philip Rogaway, a very highly respected cryptographer. Unsurprisingly, the 'proof' of security has been shown to be flawed. Whilst this result does not invalidate the use of mathematics to prove security (far from it), it does demonstrate the importance of carefully checking proofs. Clearly, in this case no careful check was done, perhaps because of Rogaway's reputation.

Even more recently, doubt has been cast over two Russian algorithms: Streebog, a hash function recently added to ISO/IEC 10118-3, and Kuznyechik, a block cipher which is being added to ISO/IEC 18033-3. Recent research results of Perrin et al. (see https://eprint.iacr.org/2019/092) suggest there is algebraic structure in an S-box shared by Kuznyechik and Streebog. This seems deliberate, and the presence and purpose of this structure has not been divulged by the algorithm designers. Indeed, this finding appears to contradict https://eprint.iacr.org/2014/501.pdf, which reveals that the Kuznyechik designers claim that they chose a randomised S-Box meeting basic differential, linear, and algebraic requirements. Unless a satisfactory explanation is provided, it seems likely that Kuznyechik will not become a standard, and Streebog may also be de-standardised.

Even though this list is non-trivial, my belief is that the set of standardised algorithms is stable. Only two cases of cryptanalysis have arisen in 30 years, and most other cases are algorithms which appear to have been deliberately engineered to have certain questionable properties, including Dual EC DRBG, the GSM A5 encryption algorithms (about much has been written elsewhere) and Kuznyechik/Streebog. Moreover, for SHA-1 there was a gap of 12 years been the vulnerability being discovered and an actual collision being found, so algorithm users had plenty of time to switch. The only case where the cryptanalysis of an algorithm has caused an immediate break – with the implication that the algorithm is immediately vulnerable – is OCB 2.0. This case is worrying, but it seems reasonable to hope that this is a 'one off'; it is also less serious than it might be as OCB 2.0 has not been widely adopted.



ONLINE GLOBAL CAPTURE THE FLAG: ROYAL HOLLOWAY PHD STUDENTS WIN GLOBAL CYBER-SECURITY CONTEST

Daniele Sgandurra

> Senior Lecturer ISG, S3Lab

Capture the Flags (CTFs) are cyber-security challenges where teams of players compete against each other to test their cyber-security skills. There are two kinds of CTF competitions, namely Jeopardy CTFs and Attack & Defense CTFs.

Figure 1: Capture the Flag Competition (Source: https://ctfd.io/whats-a-ctf/)

Jeopardy CTFs revolve around a set of cyber-security challenges that are provided by the competition organizers to competitors. Each challenge is designed so that when a team solves it, a "flag" is revealed. The flag is then submitted to a website with a scoring engine in exchange for points. The amount of points rewarded is typically relative to the difficulty of the challenge. Teams have several hours (typically over the course of a weekend) to solve as many challenges as possible. Figure 2 shows an example of a Jeopardy CTF with a set of competitions, including binary analysis (e.g. disassembly), network traffic analysis, and penetration testing of websites.

Figure 2: Example of Jeopardy CTF (Source: https://ctf.zone/ctfinfo.html)

In an Attack & Defense CTF, teams are each given the same set of vulnerable server software. Before the competition, teams have to setup and test the vulnerable software (typically residing in a virtual machine). At the start of the competition, teams will connect their servers to an isolated network to join the CTF. Within this network, teams can launch cyber-attacks against each others' servers in an effort to exploit the vulnerabilities they've previously found. Similarly, teams will need to properly patch their software so that it is protected against these exploits and functions normally. Teams receive points for obtaining flags, defending their flags, and keeping their servers secure. Figure 3 shows an example of an Attack & Defense CTF with four teams, each defending their team server and attacking the three other servers.

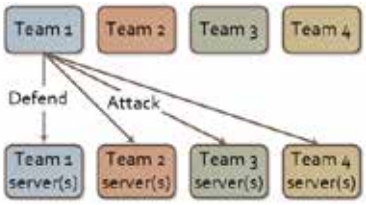


Figure 3: Example of Attack & Defense CTF (Source: https://ctf.zone/ctfinfo.html)

On 1st November 2018, the first global online CTF competition was launched. This CTF was supported by Sasakawa Peace Foundation USA, HyperQube and patronized by the InterNational Cyber Security Center of Excellence (INCS-CoE). The context required a series of machines to hack, and beginner to advanced intermediate skills were required. The context included two phases: the Elimination Phase contained 4 separate machines with 4 flags, while the Final Phase contained a multi-stage environment with 7 machines and 7 flags. Royal Holloway participated in the global CTF competition with a team composed of PhD students from the Information Security Group and Computer Science. The CTF competition was played by 150 students from leading universities all around the world, and the Royal Holloway team faced contenders from Cambridge, University of Tokyo, Keio University, Oxford and MIT, among others.

The results were announced during the 7th International Cybersecurity Symposium held at Keio University, Tokyo on 27 November 2018. The international symposium was attended by Daniele Sgandurra, who leads the Systems and Software Security Lab (S3Lab) at Royal Holloway, and who presented the online CTF initiative during the event.

Emanuele Uliana was awarded first place on the overall CTF competition, and Claudio Rizzo (S3Lab) came second -- both are PhD students in Computer Science at Royal Holloway. In addition, the 'Ethical Disclosure Award' was given to Roberto Jordaney, a PhD student in the Information Security Group (S3Lab) at Royal Holloway, who was praised during the ceremony for his findings - discovering a vulnerability in the platform - and his ethical behaviour for reporting the vulnerability to the provider for fixing.

Figure 4: Global CTF winners: Claudio Rizzo, Emanuele Uliana and Roberto Jordaney (Left to Right)

The context provided awards in three categories:

Winners
1. Emanuele Uliana, Royal Holloway, acquired 7 flags
2. Claudio Rizzo, Royal Holloway, acquired 7 flags
3. Atsushi Kanda, IISEC Japan, acquired 6 flags

Team with Most Points
1. Royal Holloway, 71 total points
2. Cambridge, 43 total points
3. University of Tokyo, 19 points

Royal Holloway's Roberto Jordaney received an Ethical Disclosure Award.

Overall, it was an outstanding result for the team from Royal Holloway who were successful in scoring the highest number of points, (flags) achieved, with 71 points, ahead of Cambridge who came second with 41 points and Tokyo who came third with 19 points. Royal Holloway also came second for securing the highest average points per student.

MICHAEL WALKER, OBE: 1947-2018

Keith Mayes, Fred Piper

> Professors ISG

It is with regret and sadness that we marked the passing of Professor Michael Walker OBE FREng FIET CMath FIMA, on the 27th September 2018, following a long battle with cancer. Throughout his illness, “Mike” conducted himself with dignity and determination, rarely complaining and remaining very active and supportive to his family, friends and colleagues. Mike achieved a great deal during his life, and a career which included major contributions to the fields of telecommunications, information security, international standardisation, and outstanding achievements working in industry, and with academic research and innovation.

One of Mike’s enduring academic connections began in 1966 when he joined what is now Royal Holloway, University of London. He first successfully completed his BSc in Mathematics, and then went on to become the second PhD student to be supervised by Prof. Fred Piper, who founded the Information Security Group (ISG); with which Mike was to have a lifelong association. With his PhD obtained in 1973, Mike was awarded a Royal Society Research Grant and moved to the Technical University of Kaiserslauten, before progressing to an academic staff position at the University of Tübingen in 1974. Having reached the rank of Reader, the award of Dr rer. nat. habil., and with various visiting positions, Mike’s path looked set for a successful academic career. However, in 1984 Mike returned to the UK and switched to an industry career, becoming the head of the Mathematics Department at Racal Research, in Reading. This gave Mike the opportunity to turn his mathematical skills to applied real-world problems in the areas of telecommunications, engineering and security; a role for which he was perfectly suited.

He remained at Racal Research until 1991, when he was spirited away by one of Racal's risky new spin-off ventures. Today this successful global giant is known as Vodafone, but in those early days its success was not certain, as there were serious security problems with the cloning of mobile phones. Mike and his team helped Vodafone by introducing an effective interim method of authentication to combat this. This experience took Mike into the world of telecommunications standards, where he was to have a major impact. This was not just embedding security into the design of future networks, but rising to the most senior position in the European Telecommunications Standard Institute; Chairman of its Board.

As his reputation and activities grew, along with the rapid expansion of Vodafone, Mike set up the UK-based Communications Security and Advanced Development team; which later evolved into Vodafone Global Research and Development; with Mike as the Director. Mike was greatly respected within Vodafone, being also appointed as a Director of Vodafone Ventures and of the Vodafone Pension Scheme, and eventually becoming the first Fellow of the Vodafone Group.

Despite his many industry activities, Mike never lost his keen interest for academic research and for many years he held the Vodafone chair as Professor of Telecommunications at Royal Holloway; as part of the ISG. In 2002, Mike was instrumental in founding the ISG Smart Card Centre which continues today.

He retired from Vodafone in 2009, but was certainly not idle. Notable activities included a period as Head of the School for Natural and Mathematical Sciences at King’s College London. He was also a member of the UK Technology Strategy Board, and a member of the UK Government’s OFCOM Spectrum Advisory Board. He was also an advisory board member of Surrey University, where he had earlier been a visiting professor. When he could find time to spare, he loved to spend it with his family, or wood-working, or watching “the cricket”.

Mike had so many recognition awards. If we begin with Royal accolades, he received his OBE in 2009 for his services to telecommunications, and he is also a Fellow of the Royal Academy of Engineering. He is a chartered mathematician and a Fellow of the Institute of Mathematics and Applications, as well as a Fellow of the Wireless World Research Forum.

Perhaps the best accolade is that Mike achieved so much on merit, from following his curiosity rather than from ambition, and remaining a thoroughly fair and decent person. There was no better example of a “Scholar and a Gentleman”, and he will be sadly missed.

Professor Keith Mayes, Professor Fred Piper

(This article was originally published on LMS Newsletter issue no.481, March 2019. Reproduced with kind permission.)

Pictured from left to right:
Rob Carolina (coach), Georgia Crossland, Amy Ertan, Lydia Garms, Angela Heeler.

ISG <3 CYBER 9/12
Andreas Haggman

> Research Manager Willis at Towers Watson, former CDT PhD student

The Cyber 9/12 Student Challenge is a cyber security policy and strategy competition for university students. The ISG has sent participating teams to the Challenge since 2017, accumulating multiple awards in the process, and since 2018 has also been represented on the organising committee of the UK version.

How It Works

The Challenge is organised under the auspices of the Atlantic Council, a US think tank that runs a Cyber Statecraft initiative, creating dialogue with key stakeholders to further knowledge and understanding of the important cyber security issues of our time. In the same way that Capture the Flag (CTF) competitions enable students to exercise their technical abilities, Cyber 9/12 is intended to enable students to practice non-technical abilities often underrated in cyber security. Starting in the US in 2014, Cyber 9/12 events now exist globally, including Europe (Geneva), UK, France, and Australia. All events follow the same format, with thematic content created for local contexts.

Taking place over two days, the Challenge sees participants – competing in teams of four with a faculty staff member to coach them – stepping into the roles of government advisors as they are presented with an evolving fictitious scenario to which they must recommend policies. The scenario is delivered in the form of intelligence packs which contain information from a variety of sources, including classified briefings, industry reports, media articles, social media posts, and other documentation. Participants receive the first intelligence pack a few weeks before the event and must produce a written brief based on the material and prepare a 10-minute oral brief of their proposed policy recommendations.

On the first day of the event all teams deliver their prepared oral briefings to a panel of judges comprised of senior industry and government cyber security experts. The teams are scored based on criteria including their understanding of the scenario situation and appropriateness of their suggested policies. A number (around 12) of the highest-scoring teams progress to the second round of the Challenge and are given a new intelligence pack at the end of the first day, which they must analyse overnight and prepare a new oral briefing to deliver the next day. After the second round the highest scoring teams (3-4) progress to the final where they are given a mere 20 minutes to analyse a new intelligence pack and prepare a full 10-minute oral briefing. The format is intense to say the least! But purposefully so: it simulates the timescales and stress faced by real policymakers.

Alongside the competition rounds, the event also contains activities to help students build their skills and networks. There are keynote talks by senior government and industry representatives, training sessions, and career fairs with Challenge sponsors. All of this ensures every participant, no matter how far they progress in the Challenge, comes away enriched with new knowledge and contacts.

ISG Love-In With Cyber 9/12

Together with three other CDT students, I was part of the first ISG team to take part in Cyber 9/12 in Geneva in April 2017. The team, comprised of a mix of technical and non-technical students, performed well, advancing to the second round and taking home the award for Most Creative Policy Response. On the back of this, I was also invited to join the organising committee of the UK version of the Challenge, which was being set up at the time. Taking the role of Scenario Development Lead, I was responsible for writing the scenario story and creating the intelligence packs in conjunction with our government and industry stakeholders.

At the inaugural UK Challenge, held in BT Tower in London in February 2018, the participants tackled the scenario I had created (involving cyber attacks against airports). In addition to my involvement, the ISG had representation from a team of four CDT students: Georgia Crossland, Amy Ertan, Lydia Garms, and Angela Heeler, coached by Robert Carolina. Facing stiff competition, the team managed to win the whole Challenge! As if that was not enough, the team also went on to scoop 'Cybersecurity Student of the Year' at the 2018 SC Awards. The same team reached the semi-finals in the Geneva Challenge in April 2019.

At the 2019 UK event, with myself again having created the scenario (this time involving poorly patched fuel distribution systems), the ISG was represented by two CDT teams, one of which advanced to the second round and picked up the award for Most Creative Policy Response.

The consistent success of ISG teams is no coincidence. The environment fostered by the interdisciplinary ethos of the CDT, is highly conducive to producing people with an advanced knowledge and understanding of diverse cyber security issues, combined with the diverse skills (teamwork, communication) required to perform under pressurised situations. ISG teams have so far embodied the undeniable notion that cyber security must be addressed through a variety of disciplines, both technical and non-technical.

Pete Cooper, Director for Cyber 9/12 UK, says: *"When I started the competition, it was to help kick-start awareness of the diverse cyber skills that we need, over and above the technical and reinforce how all of those disciplines need to be able to work together. Royal Holloway has long had great mixed discipline studies around the topic of cyber security and it's great to see how the output of these efforts is producing some real talent that directly align with the national cyber workforce we need."*

I look forward to seeing more ISG participants, and hopefully more success, in 2020!

APPS ON YOUR PHONE: UNDERSTANDING ACCESS ISSUES TO HEALTH APPS

Joshua Wuidart Gray

> PhD student

Type 2 diabetes is a problem that looms over policy makers and healthcare officials as they strategize ways to tackle a condition that has seen its number of sufferers treble in roughly the last twenty years (Diabetes UK, 2018). Joshua Wuidart Gray (a Leverhulme Magna Carta PhD student) is working under the supervision of Prof. Jon Gabe, Dr. Michelle Webster (School of Law) and Prof. Lizzie Coles-Kemp (ISG) to examine issues of access to diabetes management apps and to assess how access shapes the effectiveness of such apps. Here, he looks at how we can open up a conversation with patients about the flows of information that typically take place around the environment of a doctor's surgery and asks how digital technology could assist or hinder this process.

The Project

The aim of the project is to gain a better understanding of the ways in which digital technologies assist patients and healthcare providers to achieve various healthcare objectives related to managing type 2 diabetes and the access issues that are experienced in this context. This brief review summarizes the first engagement with professionals and patients involved with a practice in Oxford. We used creative engagement methods as a simple way of capturing individuals' narratives involving everyday information sharing. By having a group of people map out their experiences through the use of LEGO, we were able to provide our participants with a tool that they were all familiar with, opening up subjects that they otherwise may have been reticent to talk about. We looked at the ways in which day-to-day information was shared between individuals, the ways in which this information was shared, and what sorts of phenomena could create barriers to beneficial information being shared.

Methods

Lizzie, Claude Heath from the ISG and myself held two workshops that ran for 60 to 90 minutes. These began with initial remarks and questions on how patients decided to manage their diabetes. These questions were given the added dimension of discussing how GPs and other health professionals have a role in diabetes management, and what this role is. The discussion then moved on to looking at whether mobile technologies (ranging from smartphones to dedicated healthcare devices) had an influence on this, and what the nature of this influence might be. These questions were used as prompts to help participants create a story of what typical interactions around this environment might be. This story was played out on a LEGO board that could be built upon. The LEGO could be used in a way that physically portrayed what sorts of information was needed to manage diabetes, as well as how some of that information was shared, managed, disseminated and protected by individuals all operating as links in that exchange. Participants were encouraged to talk at length about challenges they faced in these day-to-day experiences; specifically, how sometimes information that they held, or needed, had to be manipulated or withheld in order to achieve desired outcomes for healthcare professionals and their patients. Fieldnotes were taken, and images captured of the LEGO scenes that were created.

Results

"When discussing the apparent imminent revolution in healthcare driven by the new digital technologies, the terms 'patient engagement' or 'patient empowerment' are frequently used (Lupton; 2012). But what can we uncover by using creative methods as part of the discussion on mobile, wearable health technologies?"

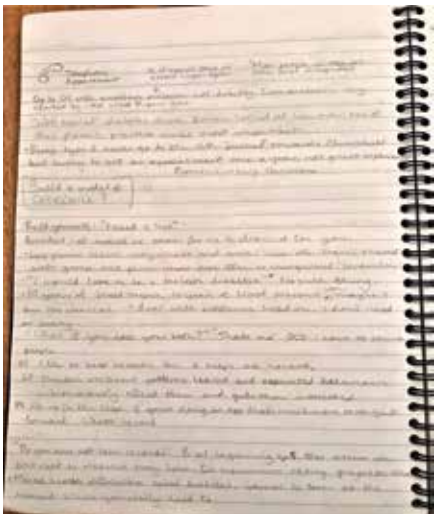
Control came up as a major issue across both sessions. This concept acted as a broad theme, under which sat sub-themes such as "patient chaos", "barriers to access", "complexity of type 2 diabetes" and "looking for solutions to different problems" (to name a few). This final sub-theme revealed itself as a salient point after the conclusion of the workshop in discussion between the researchers. It appears that patients and healthcare providers might be approaching the subject of managing their illness from different perspectives; that there was a lack of overlap between the groups and this disharmony contributed to negative healthcare outcomes.

There are actors within the topic of diabetes management that represent key points within the control discussion: patients, the GPs, Nurses, Administrative staff and the Data Officer. They all had roles to play in ensuring that information flowed in a constructive manner; and they all benefitted from different access to information from other actors. Language such as 'signposting', 'records' and 'chaos' floated around the discussion on these actors and how they mobilized information into resources that patients could use.

Concluding Remarks

"The more chaos you have, the harder it is to reduce diabetes"

It could be said on the basis of this short summary that what resulted from these workshops, then, was a clear need to establish forms of technology that minimized the impact of 'chaos' that was so harmful to successful management. It might therefore be worthwhile starting to look into what creates blockages in the flow of information; access and relationships play a large part in how information was shared between actors. What this first engagement does show, is that projects like these enable researchers interested in healthcare from a digital technologies perspective to communicate with patients and professionals in a multi-layered, multi-dimensional approach. This might just foster and give birth to digital technologies that could have a lasting impact of a group of individuals facing a lifechanging condition. Further engagements are required, and are planned for the summer, about which I hope to share with you in the near future.



Fieldnotes captured during the workshops (author's own photo).

THE ALL PARTY PARLIAMENTARY GROUP IN CYBER SECURITY

Dear Readers

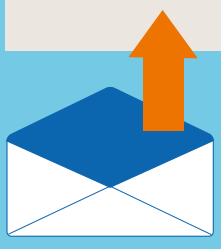
As a parliamentarian, businessman and a citizen of the UK, I am acutely aware of the growing threats to cyber security, and I am determined to help make the UK one of the safest and most secure countries in which to live and work. I therefore needed little encouragement to take over the chair of the APPG in Cyber Security, when Vicky Ford MP was promoted to be a PPS; and I thank her for her valuable efforts.
My fellow officers of the APPG now include the following MPs: the Rt Hon George Howarth, Bob Seely, Marion Fellows, the Rt Hon Richard Benyon and from the Lords:, Viscount Waverly, Admiral the Rt Hon Lord West of Spithead GCB DSC PC ADC DUniv, the Rt Hon Lord Arbuthnot of Edrom, the Rt Hon Baroness Neville-Jones, Baroness Neville-Rolfe, Lord Alderdice, Baroness Finlay of Llandaff, Lord Mackenzie of Framwellgate OBE; with Professor Keith Mayes and Andrew Henderson representing the ISG as secretariat.

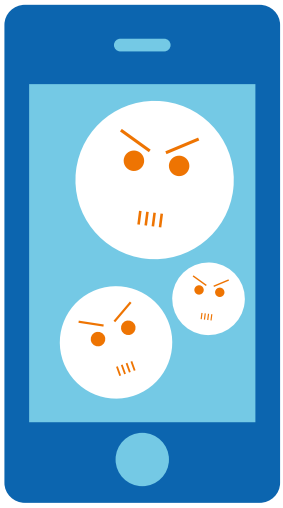
We got off to a busy start for 2019 with a notable APPG meeting in early February that included an important debate on the Cyber Security Skills Strategy Document from the Department of Digital Culture Media and Sport (DCMS), with presentations from academia and business. This resulted in a formal report to DCMS, summarising the APPG's opinions on the strategy proposals. The most recent meeting had the topical title of "How do we bridge the growing cyber trust deficit between China and the West?", in which our guest speaker, Bill Majcher, gave a fascinating and frank insight to the current problems, and to underlying cultural differences.

Looking to the future, I see no shortage of important topics for the APPG meetings with sessions being planned on Financial Services and Maritime Cyber Security, and my goal is to further ensure that the valuable outputs from our discussions are captured and used to influence parliamentary strategy. In this venture I am most grateful for the assistance of the ISG, not only for supporting the secretariat, but for the cyber security expertise that it brings to the APPG discussions.

Yours Sincerely
James Morris MP

APPG Chair and Member of Parliament
for Halesowen and Rowley Regis





INFORMATION SECURITY, PSYCHOLOGY AND LAW – AN INTERDISCIPLINARY PERSPECTIVE ON CYBERCRIME

Konstantinos Mersinas

> Lecturer ISG

Cyber security is widely acknowledged to be an increasing priority in modern society. However, the issues surrounding online behaviour transcend single academic disciplines and require an integration of perspectives and techniques. This realisation has led a group of academics at Royal Holloway to join forces and attempt to answer cybercrime related questions. Individual visions were combined to create HIVE, which stands for Hub for research into Intergenerational Vulnerability to Exploitation (http://pc.rhul.ac.uk/sites/hive). Researchers in the hub are: Dawn Watling (Psychology), Jane Marriott (Law), Joshua Balsters (Psychology), Jennifer Storey (Law) and Konstantinos Mersinas (ISG). We have attracted funding from the Higher Education Innovation Fund (HEIF) and initiated our collaboration with two crime-related projects, focusing on specific sectors of the population:

a) Protecting adolescents from cyberbullying and cyberstalking,
b) Protecting the elderly from financial abuse.

HIVE's research goals include building an understanding of how people make decisions in risky and uncertain situations. This ranges from how people decide to communicate and connect with others online, to how methods of social engineering and persuasion shape perceptions of risk. The ultimate goal is to propose policies and build early-detection mechanisms for offensive online behaviours, raise offline and online awareness and suggest frameworks that will allow for reporting, prosecuting or preventing offences. Currently, there is no consensus on which actions might best assist these aims, e.g. increased monitoring and detection, enhanced awareness, giving a face to victims, and legal consequences are all possible approaches. It becomes apparent that combatting these crimes requires a combination of cyber, legal, social and behavioural mechanisms to be achieved.

HIVE uses methods from experimental psychology, economics, politics, sociology and law. Current HIVE research on adolescent online behaviours includes assessing the risk effects of multi-platform social media usage, adolescents' perception of risk, and the justification of parameters behind action and intervention against cyberbullying and cyberstalking. In terms of elder financial abuse, we examine how being online affects identity and behaviour; indicatively, there is a lack of understanding of how social engineers manipulate people into, for example, falling for the same scam twice.

In order to focus on research which addresses real-world key issues, we have held workshops where we have engaged with industry, charities, and other relevant stakeholders. Our external partners include the London Metropolitan Police, the National Cyber Security Centre (NCSC), Age UK and others. Below are some of HIVE's findings from research undertaken in its two target sectors.

a) Protecting adolescents from cyberbullying and cyberstalking

Our initial findings from these workshops indicate that an unresolved key issue is defining cyberbullying and cyberstalking. For example, all the relevant stakeholders agreed that these crimes should not be merged under one heading, as they bear significant differences. There is no clear understanding amongst young people as to what can be considered freedom of speech, and what constitutes a harassment crime. Moreover, the boundaries between non-criminal and criminal behaviour with regards to cyberstalking activities are hard to identify, with authorities often waiting for physical stalking to take place before intervening. And, importantly, such offences are constantly underreported.

We have additionally conducted focus groups with school pupils in order to discover their perceptions of cyber behaviours and crimes. One worrying observation is that the prevalence of the phenomena has reached such a level that children might see borderline criminal behaviours as normative and, thus, not report them. An additional difficulty is revealing underlying motivations of involved parties, for example, schools tend to not report cyberbullying incidents as they do not have policies in place to manage the problem.

The online environment has two significant effects: on the one hand, anonymity and detachment allows for disinhibition effects resulting in different online behaviours to the ones revealed in face-to-face interactions. On the other hand, our senses are usually constrained to visual-only information online, allowing for paths of deception that would not have been as easily possible in face-to-face interaction (e.g. victims often report an 'addiction' to the communication). On the legal side, routes of accountability can be difficult to determine with social media companies and state authorities, demanding the other constrain the offences. We have identified requests for the use of cease and desist orders via our partners, and also a need for more effective use of existing legislation on harassment and anti-social behaviour whilst preserving users' fundamental rights.

b) Protecting the elderly from financial abuse

Consultation with relevant stakeholders revealed that elder financial abuse comes in a variety of forms. In the case of one-off scams, many victims report afterwards that they felt that something was wrong. In long-term scams, however, victims had often developed a relationship or bond with the scammer (or the scammer utilises an existing bond, such as a family connection) with the result that victims do not feel that something is wrong. Instead they are entirely convinced that they have not been victims of a scam. The difficulties in coping with fraud include a reported lack of operational capacity and resources for state authorities. Additionally, the relatively low amounts of elder life savings involved – in contrast to millions in white collar crime – do not attract the attention of the authorities. At the same time, in these elder abuse cases, the human impact tends to outweigh any monetary losses. Another identified issue is that warning signs are not correctly identified or calibrated by the authorities, and scams are often run internationally creating jurisdictional difficulties for prosecuting the perpetrators.

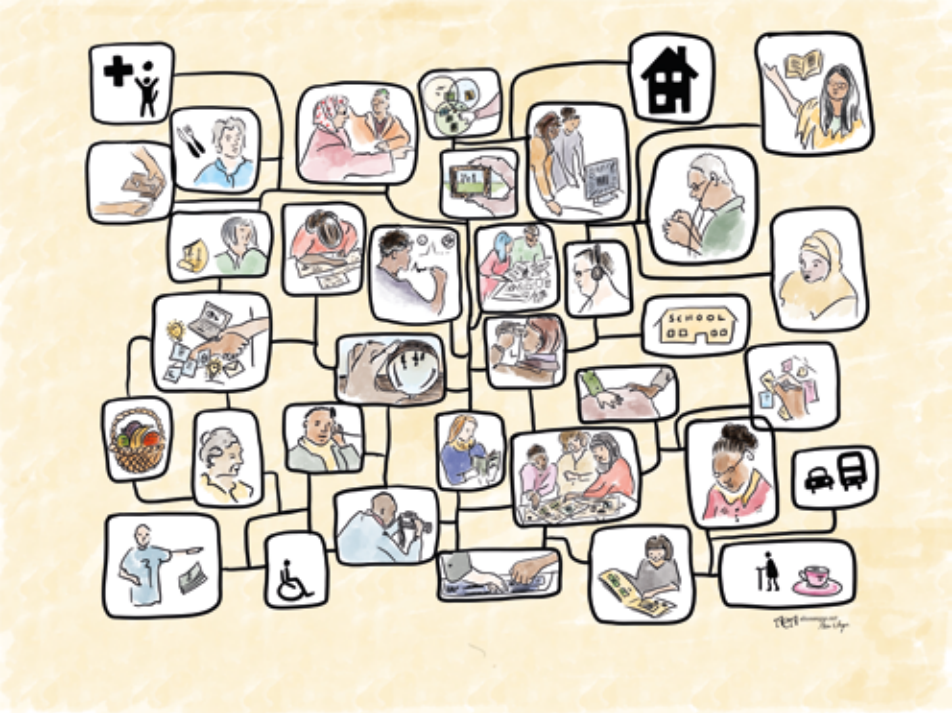
To conclude, we created HIVE to synthesise the strengths of our research expertise, methods, and our government, NCSC, industry and charity links. Our consultations have highlighted that current issues in cybersecurity amongst young and elderly individuals are multifaceted, culminating in legal, policy, social and behavioural challenges. As such, HIVE advocates interdisciplinarity as a means for providing expertise and solutions on a range of issues in cybersecurity.

ISG INAUGURAL LECTURES

The ISG recently celebrated two new professors when Lizzie Coles-Kemp and Konstantinos Markantonakis delivered their inaugural lectures, in October 2018 and March 2019 respectively.

"Inaugural lectures represent an important personal and professional milestone, and are an opportunity for us to recognise and showcase the academic achievements of our staff here at Royal Holloway. They provide an opportunity to hear about the research that is being carried out at the University and are an important part of our public events programme." **Professor José Fiadeiro, Acting Dean (Science)**

Both Lizzie and Konstantinos were awarded their professorships in 2016. In this piece, they reflect on their individual inaugural lectures.



Digital Security is Needed by Everybody (illustration: Alice Angus (https://aliceeangus.net/).

INAUGURAL LECTURE
Digital security for all: why an inclusive security approach matters

11th October 2018

By Lizzie Coles-Kemp, ISG

When I was awarded a professorship in 2016 it was, of course, a proud moment. I had come into the ISG 9 years earlier from security practice and had adopted a research position that ran against the orthodox ways of looking at information security. Two years later I gave my inaugural lecture. In preparing for that lecture, I took a long and reflective look at my research journey.

I initially joined the ISG in 2007 to teach information security assurance and principles on a biomedical informatics undergraduate course that we were contributing to at St. George's Hospital, University of London. Re-reading a Staff Profile article that I wrote for the 2007/2008 newsletter (which can still be found on our website) reminded me of how I came into the ISG with an interest for furthering my understanding of how social, economic and political conditions affect the success of security technologies and processes. Shortly after that article was written, I completed my PhD and started my first research project, Visualisation and Other Methods of Expression (VOME). It was a project that I led for 3 and a half years and it took me on a path that I couldn't possibly have imagined when I wrote that first newsletter article in 2008.

When we started VOME, there was relatively little research that focused on people and how they interact with security technologies. One of the pioneers of this research area was Angela Sasse at UCL who was making great strides in opening up the field of usable security. Angela was fighting the belief that "humans are the weakest link" and conducting research that showed that if information security technologies produce unnecessary overhead and do not provide a reliable or understandable experience, they won't be used – it was poor technology design and ill-conceived technological security approaches, not users, that were the enemy. The research perspective that Angela was championing was a significant shift from the orthodox information security thinking. I wasn't a technologist or a psychologist and whilst I had a working knowledge of security technology, my roots were firmly in the humanities – so it was a natural move for me to look at the economic, political and social landscape that formed the backdrop to Angela's research topics. In VOME we started to work with marginalized and underserved communities and I found the social, economic and political backdrop to human computer interactions, fascinating: not just in terms of what this told me about those communities themselves but also what it told me about fundamental relationships between being secure and information security.

After VOME, I have gone on to be a part of a further 6 research projects and have been awarded an EPSRC research fellowship in security for everyday essential services that will continue until August 2021. The VOME project taught me that it is impossible to assess the risks to information and technology if you don't also assess the potential risks that information and technology pose to your intended technology users. This is because people's information sharing and protection practices are shaped, in part, by the trust and confidence they feel when using that technology. If the technology is deploying a service that people regard as either not contributing to or even damaging their wellbeing, then the technology becomes an annoyance or a threat. The other important lesson that this research has taught me is that people engage with technology on a benefits realization basis, not on a risk management basis. This means that people first think about the benefits that they will gain by using a technology or service and then will consider the risks in relation to that benefit. This is why it is so important that we design security technologies and services for people as they are, not as we think or want them to be. The research also shows that the security of technology and data and the security of people using that technology are not always and in the same and we need to appreciate this difference when we design security architectures and develop security policies.

The inaugural lecture in October 2018 was an important opportunity for me to both acknowledge and say thank you to the people and communities that had given so much to my research over the last 11 years. It was also an important way of showing the diversity of the ISG research environment and the importance of the humanities to an area that is often characterized as technological and scientific. You can see a film of the lecture here:

https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/news/professor-lizzie-coles-kemp-to-deliver-inaugural-lecture

INAUGURAL LECTURE
Embedded system security, bridging theory and practice, towards a new era of Internet-of-Things (IoT) devices
26th March 2019
by Konstantinos Markantonakis, Smart Card and IoT Security Centre (SCC), ISG

//

There is no doubt that the award of my professorship in 2016 was a memorable moment that, to some extent, epitomised my journey into academic life. Therefore, when I was approached as a new professor to deliver my inaugural lecture, there was no doubt in my mind that I should take the opportunity to highlight the significance of this on-going journey.

When I was trying to convince my parents, as a teenager, to buy me my first home computer (Amstrad CPC 6128), I could have never imagined the effect that this was going to have in my later life. Soon after I started developing my first commercial computer software programs, I realised that there is so much more that I needed to learn about computers. This led me to Lancaster for my BSc and then to RHUL for my Masters and PhD.

Undoubtedly, a lot has changed since then. IoT devices have permeated into our daily lives and day-to-day mundane tasks now involve a number of embedded and cyber physical systems. Therefore, satisfying the requirements for trusted, reliable and secure embedded devices is more vital than ever before. During my inaugural lecture, I attempted to highlight the current landscape in terms of embedded system security; how we have challenged some of the existing norms, whether we are learning from our past successes and mistakes, and, finally, how we attempt to inspire the next generation of information security professionals.

The fact that IoT devices are almost everywhere, they are interconnected and their development is outsourced to a number of manufactures, reiterates the plethora of potential attack vectors and raises fundamental questions as to where we should place our trust. I attempted, through a number of selected real world use cases, including banking (EMV), transport (Mifare), satellite TV, and game console protection, to demonstrate that information security is highly related to cost, embedded devices have fundamental limitations, information security is a never-ending battle, and to question ourselves as to whether we are repeating past mistakes.

I am very fortunate to have been involved in a number of high-profile research and consultancy projects that have shaped my academic career. SHAWN was one of our Innovate UK projects aiming to develop the technology required for a robust, secure and high-bandwidth wireless communication system for intra-aircraft avionics digital data networks. The project bridged information security theory and practice through our contribution, as the information security authority, in the evaluation and design of future proof secure, and robust attestation and communication protocols. We have conducted extensive work in the automotive industry by identifying some weaknesses and improvements in the E-safety Vehicle Intrusion Protected Applications (EVITA) Project.

Our work on evaluating the performance of natural ambient sensors in mobile devices has challenged their suitability as an anti relay countermeasure with the ultimate creation of artificial ambient sensing enviroments. We also challenged the traditional norms in relation to side channel analysis for instruction profiling for the identification of hardware trojans and validating the secure execution of an application. Our current EPSRC project, DICE, examines how we can improve customer experience while ensuring data privacy for intelligent mobility. Through this thread of work, we created a worldwide patent that “records an event and its impact on the data during the lifetime of data – specific to individual entities represented in the data”, which is currently under commercialisation.

During the lecture, I also highlighted our contributions to secure hardware and software binding mechanisms for embedded devices along with some innovative techniques for mobile phone forensics. I concluded my lecture by highlighting the importance of undergraduate student (UG) participation in research and commercialisation activities that have produced notable results and the development of research outputs and papers being published with our UG students as first authors.

The inaugural lecture provided an important opportunity to acknowledge all those that played an important role in my current academic journey, including Prof Fred Piper, Prof Keith Mayes, Dr Raja Naeem Akram, our students and, of course, the sponsors of the Smart Card and IoT Security Centre (SCC). At the time of writing, the audio recording of the inaugural lecture is being processed and it will become available through the SCC website at https://www.scc.rhul.ac.uk/inaugural_markantonakis

WHY QUANTIFIABLE DOES NOT EQUAL SCIENTIFIC: THE CASE OF CVSS

Martin R. Albrecht
& Rikke Bjerg Jensen

> Reader ISG & Lecturer ISG

When you can measure what you are speaking about, and express it in numbers, you know something about it; when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science. — Lord Kelvin [3, p. 73]

In academia as much as in industry and government, the application of mathematics to derive meaning is often equated with something being scientific; in fact, the seeming need to demonstrate quantifiability underpins much scholarly work regardless of the field of study or research enquiry. Perhaps not surprisingly, the ability to "express it in numbers", has a wide appeal beyond mathematical sciences. For completeness we note that quantitative statements do not reign supreme in mathematics: no mathematician would claim to have understood the ring ZZ_7681[x]/(x^256+1) when knowing it has 7681^256 elements. Approaches with a scientific aesthetic are thus held in high regard across a wide spectrum of society where the ability to measure trumps the nuances provided by qualitative interpretations. This is not new, but it means that there is a clear – we might say worrying – tendency to blindly translate qualitative observations into numerical values. Such quasi-quantitative approaches are, however, far from always relevant or, indeed, produce meaningful insights. In some cases, these abstractions are empty, wrong and misleading and may, as a result, pose significant risks.

Information security is not exempt from this critique. There is an abundance of examples within our field which rely on mathematical abstractions to reduce or, indeed, redefine qualitative meanings to fit pre-defined quantitative scales. Take for instance the Common Vulnerability Scoring System (CVSS), which is widely relied upon to score vulnerabilities, with some standards such as PCI DSS 3.0 requiring its use.

CVSS takes various characteristics of a vulnerability such as the attack vector (e.g., network or local), complexity ("Low" or "High"), required privileges ("None", "Low", "High") and undermined security goal ("Confidentiality", "Integrity", "Availability") to produce a CVSS vector string which essentially concatenates these classifications. Then, a CVSS score is computed from this vector by assigning real values to these components and computing, essentially, a weighted sum of these numerical values. This sum ought then to be interpreted as a severity from Low to Critical. The introduction to the third iteration of the framework – CVSS v3.0, published in 2015 – discusses itself as follows.

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score to reflect its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. [6, p. 5]

This reliance on a single scoring method for all environments does not take into account differing organisational requirements or contexts, which may have a direct impact on how vulnerabilities are understood and responded to. It also disregards the individual characteristics that shape how information systems are implemented and used within different organisational settings. Rather, its appeal lies in the ability to boil down complex data to a single value [6]; thus, producing a scoring system which is able to accommodate all vulnerabilities by degenerating to a single score to be applied in all contexts.

However, several abstractions and redefinitions have to be made in order for CVSS to generate its vulnerability score: characteristics such as complexity need to be coded as "Low" or "High", these classes need to be translated to numerical scores, these numerical scores need then to be combined using some chosen weights. Finally, the resulting number between 0.0 and 10.0 can then be translated into one of the severity categories. With each level of abstraction, the relationship with the initially observed vulnerability is reduced to a point where it no longer carries meaning. Additionally, as noted by Spring et al. [6], CVSS provides no guidance on how the scores should be interpreted nor does it argue how and why its formulas were derived. Thus, these scores are arbitrary at best.

Moreover, the CVSS scoring formula has been criticised by Spring et al. [6] for committing a "data type error" by taking ordinal data to construct a novel regression formula. This is done by using unclear and unjustified methods, which assign "relative importance rankings as ratio values." Highlighting the difficulties of capturing the distinct characteristics of complex systems by translating such qualitative notions into quantitative measures, the authors suggest "the way to fix this problem is to skip converting qualitative measurements to numbers". This, of course, will require a re-configuration of how security metrics are constructed and deployed, and necessitate a re-thinking of how their resulting data is interpreted.

The critique of CVSS is only a (timely) illustration of a far deeper trend in the wider field of information security and beyond. Indeed, the drawbacks of translating qualitative statements into quantities, which can then be algebraically manipulated, are a subject of active debate in the wider social and behavioural sciences, see e.g. [4, 5]. For example, in economics, e.g. Kay [2] criticises the "modern curse of bogus quantification" and points out that the "index […] is not telling us anything we have not already told the index […]" [1]. While the quantifiable certainty provided by mathematical and statistical analysis is appealing, it is generally not translatable or applicable to qualitative phenomena.

Thus, in contrast to Lord Kelvin's assertion that "[w]hen you can measure what you are speaking about, and express it in numbers, you know something about it", we may argue that by insisting on expressing qualitative data and observations in numbers, we know nothing about it.

References

[1] J. Kay. 2009. "Do Not Discount What You Cannot Measure." Financial Times. https://www.ft.com/content/08a7f396-a7a7-11de-b0ee-00144feabdc0.
[2] J. Kay. 2011. Obliquity: Why Our Goals Are Best Achieved Indirectly. Profile Books.
[3] Lord Kelvin. 1883. "Electrical Units of Measurement". Nature Series: Popular Lectures and Address 1: 73-136.
[4] W. Kuzon, M. Urbanchek, and S. McCabe. 1996. "The Seven Deadly Sins of Statistical Analysis." Annals of Plastic Surgery 37: 265–72.
[5] J. B. Pornel, and G. A. Saldaña. 2013. "Four Common Misuses of the Likert Scale." Philippine Journal of Social Sciences and Humanities University of the Philippines Visayas 18 (2): 12–19.
[6] SIG, CVSS. 2015. Common Vulnerability Scoring System V3.0. FIRST.
[7] J. M. Spring, E. Hatleback, A. Householder, A. Manion, and D. Shick. 2018. "Towards Improving CVSS." Software Engineering Institute, Carnegie Mellon

COMPUTER WEEKLY ISG MSC INFORMATION SECURITY THESIS SERIES 2019

Siaw-Lynn Ng

> Senior Lecturer ISG

The ISG has a long tradition in cybersecurity research, and is one of the largest academic cybersecurity research groups in the world, consisting of academics and research assistants, and a large group of postgraduate research students, working on a wide range of topics in information security. Alongside this research, the ISG also has a proud tradition of information security education. Founded in 1992, the ISG's flagship MSc Information Security masters degree programme has now produced over 4000 graduates from more than 100 countries around the world.

One core part of the MSc programme is the MSc project. This is a major individual piece of work aimed at demonstrating an understanding of a specific area of information security or dealing with a practical aspect of information security. Because our students come from a range of different backgrounds, from new students seeking a foundation for a professional career in information security, through to subject experts seeking to widen and deepen their knowledge of information security in general, our MSc projects cover a wide variety of topics. Past topics include the provision of privacy in social networks, how to deal with insider threats, the policing of cybercrime, and the security of wireless protocols relied upon for the Internet of Things.

Every year, a number of outstanding MSc projects are chosen for the Computer Weekly awards. These MSc projects are re-written in collaboration with the individual ISG project supervisor to make them accessible to a general professional readership. These short articles are published online on the Computer Weekly website (https://www.computerweekly.com/) and are also made available on our website: https://intranet.royalholloway.ac.uk/isg/informationfornewreturningstudents/mscproject/thesisprizes.aspx

This year there are four articles covering topics such as Internet, as well as the Internet of Things (IoT), security, examining the behaviours of users and organisations from different points of view.

The article "How long does it take to get owned?" by David Wardle (supervised by Jorge Blasco Alis) investigates the amount of time that it takes for stolen credentials to be used by a hacker. David designed fake "honey identities" and a monitoring infrastructure to study how quickly a stolen credential is used by an unauthorised person, and what activities this person might be interested in.

Colin Putman (supervised by Chris Mitchell) describes one of the key weaknesses in the Neighbor Discovery Protocol of IPv6 in “Can I trust my neighbours? - Proving ownership of addresses in IPv6 networks.”. This protocol is vulnerable to address-spoofing attacks within the same network. Colin explains the deficiencies in the cryptographic methods which were introduced to prevent these attacks and gives examples of how they can be improved, justifying the need for a new, unified improvement to the protocol.

The current widespread use of poorly secured consumer IoT products, while the underlying knowledge and technology that are necessary for IoT security are already widely available, is the topic of the article "Rethinking the cybersecurity of consumer Internet of Things (IoT)" by Joo-Huat Ng (supervised by Robert Coles). The article investigates how innate psychological factors can influence the thought processes of consumers when assessing the cybersecurity risks of IoT, and how this perception eventually leads consumers and enterprises to make economic decisions that harm the security of the Internet. The insights gained are then applied to formulate a framework that incentivises enterprises to design and make consumer IoT products that are more secure.

Finally, the article "20 years of Bleichenbacher's attack" by Gage Boyle (supervised by Kenny Paterson) investigates how even the most reputable websites may be exposed to a 20-year-old attack if HTTPS is not properly implemented. The presence of ``HTTPS'' at the start of a website URL usually provides enough security confidence to a user, but unless implemented properly, it can still be vulnerable to this 20-year-old attack that may result in the session key being discovered. The article concludes with some recommendations of steps to prevent this.

These articles are distilled from the full project reports and necessarily omit many details. Readers interested in particular articles can obtain the full reports from the ISG website: https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/

NEW EPSRC CENTRE FOR DOCTORAL TRAINING IN CYBER SECURITY FOR THE EVERYDAY

"The call in 2019 for EPSRC Centres for Doctoral Training was an important one for the College as the awarded centres bring significant resource and profile. The success of the ISG in renewing their centre is major recognition in a highly competitive environment. The format of the new centre, bringing in supervisors from across the College, is a great example of a cooperative way of working that draws on College strength, which provides an example we are hoping to build on. ISG continues to lead the way within the College."

Professor Ken Badcock, Senior Vice-Principal (Academic Strategy, Partnerships and Resources), RHUL

Since the turn of the 21st Century, the subject of information security has experienced growing diversification both at a practice – industry and government – and at an academic level. This move towards increased diversity is reflected in the funding calls, the interests of our MSc and PhD students and in the research challenges presented by many of our key stakeholders. Whilst information security still maintains an important and strong information and technology protection focus, this focus now sits alongside a broader purpose of securing people and society in a digital world. The process of extending the scope of and the approach to our research and teaching, whilst upholding a strong connection with our data and technology protection roots, is illustrated particularly clearly in the story of our Centre for Doctoral Training (CDT) in Cyber Security.

With our first CDT having taken its final cohort last year, we were delighted to be successful in the latest round of awards for UKRI centres for doctoral training. This means that our CDT has been awarded new funding for a further five intakes of ten PhD researchers from September 2019. This is fantastic news, and a testament to the efforts of everyone who has supported the CDT since it launched in 2013. With the new funding comes an important change to the CDT. While we have always welcomed multidisciplinary research projects, going forward there is a stronger emphasis on this. The new CDT welcomes both single discipline and multidisciplinary researchers with the common goal of understanding how cyber security is woven into everyday lived experiences. This is reflected in a new title: the EPSRC Centre for Doctoral Training in Cyber Security for the Everyday. This is a truly multi-disciplinary initiative that brings together students from the mathematical sciences with those from the social sciences and humanities, by focusing on two main security research challenges: those presented by emerging technologies and those that emerge from increasingly connected societies. In bringing these two challenge areas into one CDT, we are developing upon the ISG's tradition of high-quality research in technology and data protection as well as demonstrating our ability to lead emergent research in the securing of people, communities and society at large, in an increasingly connected and digital world.

The success of this CDT application lay, in part, in our ability to build upon on-going, successful partnerships with industry and government stakeholders as well as with colleagues from a wide range of disciplines and departments across Royal Holloway. Our previous CDT established strong connections with Computer Science, Geography, Psychology and the School of Law. At the same time, the ISG was also involved in the Leverhulme funded Doctoral Training Centre (DTC) on Freedoms and the Rights of the Individual in a Digital Age where, in addition to working with our CDT collaborators, we developed collaborations with Media Arts, Politics and International Relations and Classics. In envisioning and developing the CDT in Cyber Security for the Everyday, we brought together these different supervisory networks, connecting them through the ISG's expertise in security technologies and practice. We did so to establish a foundation upon which a spectrum of both single-disciplined, with an interest in wider disciplinary positions, and multi-disciplinary research can be encouraged and supported.

In our new CDT, we are looking forward to welcoming new colleagues, partners and collaborators into our network and exploring new stakeholder engagements. Not only shall we be working further on our approaches to multi-disciplinary PhD research but also learning from each other and our student cohorts as to what security education and training is needed for this type of multi-disciplinary programme. This is important so that the new CDT becomes a space that supports a wide spectrum of multi-disciplinarity; from single-disciplinary approaches with an appreciation for wider disciplinary positions to truly interdisciplinary PhD studies. Hence, a multi-disciplinary approach to PhD research, whilst not replacing a single-disciplined outlook, extends and broadens the ways in which cyber security is researched and taught.

One of the greatest features of the CDT approach to PhD training is the bringing together of cohorts of diverse researchers, where diversity appears in many ways, including: academic background, research discipline, age, gender, ethnicity and professional experience. Of course, such diversity brings different views and perspectives that don't always align and this requires students and academics to embrace difference and work carefully with any tensions that might emerge. More than this, however, diversity provides opportunities. As we progress with what will, inevitably, be a more diverse CDT, it is through a respect for diversity in all its forms, and by everyone involved, that these opportunities can be seized and great research outcomes can emerge.

The CDT uses different engagement methods to bring together several disciplinary perspectives.

The NTNU main building in Trondheim.

View from the University of Trømso

AN INTERNATIONAL PERSPECTIVE FROM NORWAY ON INFORMATION SECURITY RESEARCH AND TEACHING

Stephen Wolthusen

> Professor ISG

The "Norway Model" holds a certain appeal to some. It is therefore instructive to review the model more closely. I have been affiliated with what is now the Norwegian University of Science and Technology (NTNU) for well over a decade in a number of roles, giving me a reasonable basis for comparison between Norway and the UK.

The university sector in Norway is almost completely in state hands, which also implies a more direct oversight role in areas of quality assurance for education - provided by the Norwegian Agency for Quality Assurance in Education (NOKUT)- and occasional direct intervention from the policy level. This is quite unlike the UK where universities are generally constituted as charities and operate at arms-length.

Part of the reason for this setup, however, is the fact that education from primary school to the second higher education (postgraduate, MSc or M.A.) cycle is paid for out of general tax. This means that students do not have to pay tuition fees; they can also take out a subsidised but means-tested loan for their cost of living and will usually receive a small stipend ("book money") for their undergraduate degree, while postgraduate students can still apply for subsidised loans – which can be augmented with a stipend for new parents. Because of this, the number of study places is regulated and candidates must compete based on grades also at postgraduate level. However, NTNU has been very successful lately in securing funding for study places in information security as the Norwegian government has made this a national priority over a number of years. Typically, 2-3 students apply competitively for each seat in the information security MSc. programme, with a mixture of students continuing directly from their undergraduate programmes, those seeking to enhance their standing after spending some period working in the field, and part-time candidates following the programme while on part-release from their workplace.

Once admitted to a degree programme, NTNU's MSc in Information Security and universities offering information security specialisations for their Computer Science programmes follow the European (Bologna) model. This consists of a first cycle, usually a 3-year 180 ECTS undergraduate degree forming the basis of a 2-year (120 ECTS) postgraduate programme. For most MSc or MA degrees, the dissertation takes up six months and is augmented by a course on research methods and research project planning. This 2-year degree then forms part of the admission requirements for PhD degrees; e.g. NTNU offers degrees and specialisations in information security at the BSc, MSc, and PhD levels. Whilst this limits mobility of UK candidates somewhat, it is still possible to take advantage of European (Erasmus) mobility programmes - NTNU candidates are also encouraged to spend some time at other universities if possible.

While there are no fees charged for PhD studies, the cost of living and constraints of supervisory activity generally limits the availability of PhD positions to those supported by grants from national, European, or industry sources. PhD studies are normally expected to take 3.5-4 years and include 30 ECTS of taught courses in addition to the research usually undertaken in PhD by research in the UK.

Research, whether undertaken by PhD students or others, is supported through a number of channels. Universities are allocated funding by the Ministry of Education, allowing them to support research time of academic staff and a limited number of PhD students, while other research is then supported via competitive grants awarded by the Norwegian Research Council (Forskningsrådet), other government ministries, industry, and the European Union's framework programmes such as Horizon 2020 including e.g. ERC and Erasmus+ actions. The latter is made possible by Norway participating in the EU research programmes as a contributing non-member state.

At NTNU, academic staff and researchers are also supported by a long-term public-private partnership with industry and a number of government agencies in the form of the Centre for Cyber and Information Security (CCIS) and hosting also e.g. the Norwegian Cyber Range in co-operation with the Norwegian Cyber Defence Force (Cyberforsvaret).

Besides universities, other contributors to the research landscape exist in the form of foundations; the most important of which is SINTEF. SINTEF started as a foundation for more applied research of NTNU in 1950, but now consists of seven laboratories with locations across Norway and conducts more applied research in a number of domains including e.g. materials science, biotechnology technology, energy, and also touching on information security; a similar role is also filled by Simula, originally spun out of the University of Oslo but since then spread also to Bergen. Simula conducts research on social aspects of resilience and security in Oslo, and on cryptography in Bergen, traditionally a strong area at the University of Bergen.

The composition of academic staff and student bodies in the information security field is quite international in outlook. This is not surprising in a country with a relatively small population, but it is also in part driven by a competitive labour market where many MSc students entering their second year of studies are already holding firm job offers. Moreover, the relatively small but closely-knit information security community is also supported by an ongoing joint research school (COINS) supported by the Research Council of Norway; this school organises both summer and winter schools (the latter usually at the Finse ski resort), allowing the community to meet regularly and particularly offering opportunities for networking to PhD students in the field.

Right: Ethnographic fieldwork onboard container ships in European waters, 2018 (photo: author's own).

NAVIGATING SECURITY AT SEA: INSIGHTS FROM AN ETHNOGRAPHIC STUDY

Rikke Bjerg Jensen

> Lecturer ISG

"On a scale from one to 10, I would say that Internet connectivity is an eight in terms of importance. The only thing that is more important than connectivity is food." (Research participant, container ship crew, 2018)

Online connectivity and security at sea have been two of the major talking points of the decade in the maritime industry, which has been slow to adopt technology enabling improvements across the world's commercial fleet. While some studies have employed quantitative surveys to try to establish the rate of online connectivity, none – to my knowledge – have explored its relation to security or indeed taken an ethnographic approach, driven by participatory observations onboard ships and engagements with seafaring communities, as their starting point. This study, funded by the Sailors' Society and Inmarsat, did just that. As an ethnographer and a social researcher in the Information Security Group, my research starts from the ground in order to understand how everyday lived experiences shape and reshape information security practices; through engagements with people and communities affected by technological change and the wider security implications that come with that change.

Last year, I spent four weeks onboard two container ships in European waters to better understand how limited online connectivity during long periods at sea impacts on feelings of safety and security, from the perspective of the seafarers themselves. Such an approach goes beyond a focus on the state of online connectivity and technological security – and what seafarers do with that technology – and attends instead to how and why seafarers navigate and negotiate a web of connectivities and securities – in the plural – and the meanings they ascribe to their experiences of doing so. It does so to impact on the development of future digitally enabled initiatives at sea and the design of technology that is more attuned to the everyday lived (security) experiences of seafarers.

By not separating technology from the social relations in which it is embedded, the study brought to bear the underlying security logics that influence how seafarers engage with technology whilst at sea; either through limited and constrained onboard Internet provision or through the purchase of individual mobile phone SIM cards during port stays.

"In most ports, mobile phone SIM card sellers come onto the ship to sell their stuff. We call them 'the Mafia' because they cannot be trusted but we're reliant on them to stay connected with family and friends […] We have no other option since there is no Internet on the ship." (Research participant, container ship crew, 2018)

Exploring online connections at sea in this way enables a nuanced understanding of the wider security implications of connectivity, no connectivity, poor connectivity, constrained connectivity, and their combining, particularly on how seafarers' feelings of security influence their online practices. Access to digitally enabled relations with wider kin and friendship

networks beyond the confinements of the ship, therefore, also shape the security worries that are embedded in the everyday rhythms and routines of life at sea. More specifically, the study uncovered how uneven and unreliable connections disrupt the patterns of everyday life, work and rest, whilst linking the security worries of the individual seafarer with technological security. This link was evident through the creative ways in which seafarers engage with digitally enabled technologies in order to maintain strong ties and intimate relations during times of separation from family and friends, including: circumventing access restrictions to benefit from a particular online service; sharing account passwords; buying mobile phone SIM cards in ports; rationing data usage; and monitoring ship positions to predict when mobile phone signal will be available. The practice of bypassing technical security controls was thus directly linked to the feelings of security that emerged through communications with loved ones.

" You may have planned to message someone or speak to your family when you're in a certain port on a certain date, but when the schedule then keeps changing these plans are disrupted and you feel terrible and isolated. We will do almost anything to be able to connect."
(Research participant, container ship crew, 2018)

Hence, for seafarers – as with other mobile and isolated communities living and working within confined spaces – security does not simply mean security and online does not simply mean online. Rather, they refer to a myriad of connections, networks and relations that exist within and beyond the confinements of the ship and they come with a number of information security challenges, including: to understand how the security worries of seafarers connect with technological security; to protect increasingly uneven information flows between ship and shore; to understand how limited online connectivity affects the security decisions seafarers make and the security-safety of the ship itself; and to develop and implement security technologies and approaches attuned to the lived experiences of seafaring communities.

One of the overarching arguments from ship owners for not providing onboard Internet facilities has been that it would disrupt work and rest hours onboard ships, which could ultimately compromise safe and secure ship operations. However, insights from this study show that, in fact, not having access to reliable networks significantly disrupts such patterns and could have wider, negative, implications for security. As a result, and citing this study, in April 2019, Inmarsat launched a new digital service package for crew – Crew Xpress – as part of their wider Fleet Xpress, which enables more stable and reliable online connectivity for seafarers.

Regardless of whether shipping companies provide more onboard Wi-Fi facilities, seafarers navigate and negotiate several interwoven connectivities and securities every single day. They do so largely to minimise emotional stresses and pressures of being separated from family and friends for up to nine months every year. From a security perspective, providing consistent onboard Internet access does not solve all challenges facing the maritime community – far from it. Yet, instant, regular and stable technologically facilitated contact with wider kin and friendship networks helps build emotional resilience among seafarers. However, such connections may also introduce new pressures requiring particular onboard support mechanisms to be in place. Navigating multiple (digitally enabled) connections and networks at sea thus has a direct effect on how security is experienced, performed and maintained within and beyond seafaring communities.

Left: As an ethnographer I engage with people and the spaces they inhabit (photo: author's own)

All photo's by Dan Tsantilis

THE TLS 1.3 PARTY — YOU'RE INVITED!

Thyla van der Merwe

> Cryptography Engineering Manager at Mozilla, former CDT PhD student

"Connecting people, things and data together, in safe, smart, secure, trustworthy and productive ways" is the Engineering and Physical Sciences Research Council (EPSRC)'s definition of a Connected Nation. Recognised as a major driver of economic growth, the development of a fully Connected Nation relies on innovation in the areas of mathematical, physical, computing and engineering sciences. With this target in mind, the EPSRC sent out a call to doctoral candidates across the UK, framed as a competition that would recognise research that was contributing to this important and substantial goal.

Encouraged by my supervisor, Professor Kenny Paterson, I answered this call and my Connected Nation competition journey began! Comprised of three stages, the competition involved video-making, exhibit-building, and idea-pitching, a gruelling challenge for anyone willing to take it on. However, the topic of my PhD research, the Transport Layer Security (TLS) protocol, made for a very suitable entry. This critical protocol is used by millions, if not billions, of users on a daily basis, and works tirelessly in the background to protect our online purchases, our emails, our Facebook logins, and our instant messages - we trust it with our passwords and our banking credentials! TLS is such a crucial part to the plumbing of the Web and most of the time we, the users, aren't even aware that we're using it. But without it, cyber criminals could impersonate us online, drain our bank accounts, and completely disrupt e-commerce.

TLS has had a very turbulent history, and the ubiquitous nature of the protocol has, especially in recent years, made it an attractive target for security researchers. Since the release of TLS 1.2 in 2008, the protocol has suffered many high-profile and increasingly practical attacks. Coupled with pressure to improve the protocol's efficiency, the deluge of identified weaknesses prompted the Internet Engineering Task Force (IETF), the custodians of this important protocol, to develop a new version, namely TLS 1.3. In contrast to previous versions, the IETF welcomed academic analyses of the protocol prior to its official release, so as to catch and remedy weaknesses before the protocol enjoyed widespread adoption.

My PhD work contributed to this newer, collaborative standardisation effort, covering both sides of the TLS design transition: I helped to find attacks against TLS 1.2 and below that uncover user passwords. Hence, helping to motivate the need for a new protocol version, and working together with excellent collaborators, I analysed TLS 1.3 prior to release, uncovering a serious attack which called for a fix of the protocol. As the TLS 1.3 draft was a rapidly moving target, our team went on to confirm a stable draft of the protocol, showing that after four years of development, the logical core of the protocol seemed sound. This confirmation, along with analysis from other academic teams, gave the IETF confidence to release the protocol, and in August of last year, TLS 1.3 was let loose in the wild. Since then, adoption of the protocol has increased steadily, with SSL Pulse stating that nearly 14% of sites surveyed support TLS 1.3, and Facebook claiming that 50% of its traffic now makes use of TLS 1.3. As a result of my work, I have been listed as an official TLS 1.3 contributor, and I foresee the techniques developed in my TLS 1.3 work contributing to a new era of analysis for cryptographic protocols. Specifically, one which employs the use of state-of-the-art automated tools for protocol checking.

All of my work was incorporated into my competition exhibit. Using LED strip lighting and a cork globe, I built a representation of the Web, right the way through from client to server; using a different lighting colour to represent the different versions of TLS, many of which are still in use today. Starting with the older, weaker versions, the globe progressed through a range of colours - red for SSLv2 and becoming less menacing as the version numbers increased, ending with a bright, flashing green for TLS 1.3. The "party globe" (as it affectionately became known), proved very effective in showing the development of the TLS protocol over the course of its twenty-four-year lifespan, and highlighted that my work has contributed to a faster, safer protocol.

At the official awards ceremony in Manchester on November 20th, 2019, I was announced as the winner of the Safe and Secure Cyber Society category. The party globe did very well to beat out some excellent competition, and it landed me a rather modern-looking glass trophy. A trophy like this, however, doesn't really belong to one person. It belongs to all of those who helped, supported and guided me throughout the course of my PhD. It belongs to all of the researchers and industry professionals who have worked so hard to produce TLS 1.3. And the award recognises the importance of this protocol - in its role as the security backbone of the Web, we're not only talking about a safely Connected Nation, we're talking about a safely Connected World.


PRIVATE INFORMATION RETRIEVAL IN DISTRIBUTED STORAGE SYSTEMS

Chatdanai Dorkson & Siaw-Lynn Ng

> PhD student, Department of Mathematics & Senior Lecturer ISG

WHAT IS PRIVATE INFORMATION RETRIEVAL?

The efforts to preserve the confidentiality of retrieved data from public online databases have prompted extensive research interest over the past few years. A private information retrieval (PIR) scheme presents itself as a promising solution to such a privacy concern by allowing a user to download records from the database without revealing any information about the identity of the desired records. This is highly relevant to real-world scenarios where privacy interests are at stake; for example, an investor might want to keep the identity of the interested stock secret to avert any impact on the market price, or a researcher may want to carry out a search of existing patents.

One trivial solution is to download a copy of the entire database and look up the desired information, but this could be inefficient, especially when the database is large. Here we give a short description of the academic research into finding a more practical solution, and our contribution to that effort.

ORIGINAL SETTING & EXAMPLE

The database in the original setting of PIR, studied by Chor et al. [1], is replicated among n nodes. They showed that if there is only one database then downloading the whole database is the only possible solution. However, if there is more than one database, substantial efficiency savings can be made. The following example illustrates how this might work. Suppose there are 3 one-bit records in the database X_1,X_2,X_3 replicated across two nodes. Assume that a user wants the record X_1. The user generates a 3-bit vector (u_1,u_2,u_3) uniformly at random. Node 1 and node 2 are given the queries (u_1, u_2, u_3) and $(u_1 + 1, u_2, u_3)$, and then requested to return $u_1X_1 + u_2X_2 + u_3X_3$, and $(u_1 + 1)$ $X_1 + u_2X_2 + u_3X_3$, respectively. The record X_1 can be reconstructed by computing the XOR of answers from both nodes.

THE USE OF ERASURE CODES

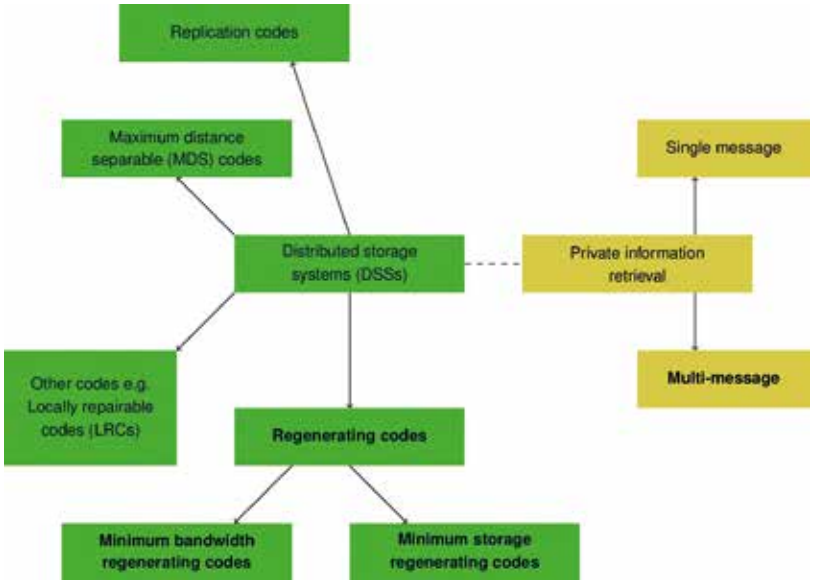
An erasure code is a code that transforms a message of k symbols into n symbols with a property that the original message can be recovered from a subset of the n symbols. Due to high storage costs when a replicated database is used, erasure codes capture researchers' attention where only a fraction of the entire database is stored in each node. Shah et al. [2] were the first to explore PIR in these code-based schemes. They proved that only an extra bit of download is needed to retrieve the desired record. Subsequently, various researchers expanded the model to PIR in codes with different useful properties, such as codes with lower storage costs, and codes that allow recovery from any subsets of k symbols (these are called Maximum Distance Separable (MDS) codes), which gives high reliability. Much work has also been done to study and derive the trade-off between storage cost and private retrieval cost, and many schemes achieving optimality were proposed.

VARIATIONS OF PIR MODELS

Lately, many variations of PIR have been explored. For instance, PIR with colluding nodes where some nodes can share information, symmetric PIR (SPIR) which also ensures the privacy of undesired records from the user. One interesting scenario is when a user wants to retrieve more than one record. Obviously, the user can repeatedly use a single-message PIR scheme, but we wish for a more efficient way to reduce the download cost. This is the multi-message PIR (MPIR) problem.

REPAIR PROBLEM

A common problem when the database is stored using erasure codes is node failure. We want to ensure that if some nodes failed, the data could be reconstructed from the functioning nodes. There was a study [3] on the Facebook warehouse where an MDS code is used for the storage. They found that approximately 1% of nodes are unavailable per day, and 10-20% of the total average of 2 PB/day network traffic is for node repair. In an MDS code, a failed node is usually repaired with the simple method of reconstructing the original database. Downloading these amounts of data to only repair one node is extravagant. Recently, there have been much research on constructing new codes that have much less repair cost compared to this naive method. One interesting result is the new concept of a regenerating code which was introduced by Dimakis et al. [4].



WHAT WE DID

Minimum storage regenerating (MSR) and minimum bandwidth regenerating (MBR) codes are classes of regenerating codes that are optimal in terms of the storage cost and repair bandwidth trade-off. In our work, we propose a general MPIR model where a widely known class of regenerating codes is used for storage. We analyse a trade-off between storage cost and retrieval cost, and then construct MPIR schemes that achieve the optimal curve of the trade-off. The use of regenerating codes reduces the repair cost when a node failure occurs in the system, hence our scheme obtains more efficient repair compared to schemes using MDS codes. Our research paper can be found at https://arxiv.org/abs/1808.02023.

References

NB. We have only included very few references due to space restriction. Please refer to our paper and the references therein for a fuller bibliography.

[1] B. Chor, O. Goldreigh, E. Kushilevitz and M. Sudan. Private Information Retrieval. J. ACM, 45, 6 (November 1998), 965-981.

[2] N. B. Shah, K. V. Rashmi and K. Ramchandran. One Extra Bit of Download Ensures Perfectly Private Information Retrieval. IEEE International Symposium on Information Theory, June 2014, pp.856–860.

[3] K. V. Rashmi, N. B. Shah, D. Gu, H. Kuang, D. Borthakur, and K. Ramchandran. A Solution to the Network Challenges of Data Recovery in Erasure-coded Distributed Storage Systems: A Study on the Facebook Warehouse Cluster. Proc. 5th USENIX Workshop on Hot Topics in Storage and File Systems, San Jose, CA, USA, 2013.

[4] A. G. Dimakis, P. B. Godfrey, M. Wainwright and K. Ramchandran. Network Coding for Distributed Storage System. IEEE International Conference on Computer Communication, May 2007, pp.2000–2008.

POST-QUANTUM STANDARDISATION: AN UPDATE

Martin R. Albrecht

> Reader ISG

At this point the efforts to standardise post-quantum cryptography, i.e. cryptographic primitives that run on ordinary computers but resist attacks using quantum computers, are well underway. ETSI has a Working Group for Quantum Safe Cryptography, ISO has WG2 Standing Document 8, the Cloud Security Alliance has published position papers through its Quantum-safe Security Working Group and the IETF has standardised stateful hash-based signature schemes (which are only applicable in some settings, the IETF has no further post-quantum plans at this point). However, what unifies all global post-quantum standardisation efforts is that they are essentially waiting for the US National Institute of Standards and Technology's (NIST) Post Quantum Process to conclude. In other words, the number one post-quantum standardisation effort to pay attention to is that of NIST.

In 2017, NIST asked for submissions of post-quantum secure digital signature schemes and key encapsulation mechanisms (KEMs). In November 2017, it accepted 69 such submissions as “complete and proper”. In January 2019, NIST announced which of these were kept for Round 2: 17 key encapsulation mechanisms and nine signature schemes. Researchers from the ISG are involved in three of these submissions: NTS-KEM, NewHope and Round5. NIST expects the final standard some time in 2022 to 2024.

While there are plenty of submissions to the second round of the NIST PQC process, they rely on the difficulty of a handful of mathematical problems. Three for KEMs and three for signatures, with one in common. Out of 17 KEMs, eight rely on the difficulty of decoding: take an error-correcting code with a hidden decoding algorithm and use the error positions as the entropy for the shared key. The oldest of such proposals is from 1978 due to McEliece and thus, by now, we have some confidence in its security. On the other hand, such schemes often have fairly large public keys (~1MB). While smaller, more efficient variants exist those are less well studied. SIKE is a KEM submission that relies on the Supersingular-Isogeny Diffie-Hellman (SIDH) problem. The hard problem here is to find rational maps preserving structure between elliptic curves, as opposed to Elliptic Curve Diffie-Hellman (ECDH) which relates to discrete logs on one such curve. SIKE has relatively small public keys and ciphertexts, but it is slow compared with other submissions. The problem itself is also fairly new and thus not that well studied yet.

Among the signature schemes we find two that are secure if secure hash functions or block ciphers exist: SPHINCS+ and Picnic. These construction have relatively large signatures and slow computation time but are very conservative. Interestingly, these schemes also highlight an important distinction between what is usually taught in Crypto 101 classes and how cryptographers conceptualise different schemes. While the former discusses public-key encryption and digital signature schemes as one class of algorithms (“asymmetric”) and block ciphers, stream ciphers and hash functions as another (“symmetric”), we can build digital signature schemes from hash functions but we do not know how to do that for public-key encryption. This is why, theoretically speaking, cryptographers distinguish between block ciphers, hash functions, digital signatures on the one hand (“Minicrypt”) and public-key encryption (“Cryptomania”) on the other hand. That said, most efficient digital signature schemes in use today rely on the same mathematical assumptions as public-key encryption, but as SPHINCS+ and Picnic highlight this might change in a post-quantum world.

Another class of signature schemes are those that rely on the difficulty of solving quadratic multivariate equations: MQ. Of those one submission truly reduces to this problem (MQDSS) and three rely on related problems with more structure. An appealing feature of these MQ signature schemes is that they are usually extremely efficient in terms of computation time, but the public keys or signatures can be somewhat large. There have been attempts to build public-key encryption from MQ but those were unsuccessful and the resulting schemes broken. It is thus an open question as to whether this can be done at all or if, rather, MQ only permits constructions in Minicrypt.

Finally, nine KEMs and three signature schemes rely on the difficulty of finding short vectors in lattices. Equivalently, we may think of these schemes as relying on the difficulty of noisy linear algebra modulo some prime q. Here, too, we have a choice between unstructured and structured schemes, where the former is less efficient but more conservative and vice versa. Indeed, (structured) lattice-based cryptography is often faster than elliptic curve cryptography, but public keys and ciphertexts/signatures are a bit larger, typically around 1KB in size. While candidate solutions exist that promise public-key cryptography in a world where quantum computers exist, a lot still needs to happen before they can be deployed. For starters, the underlying assumptions need further investigation to increase our confidence in the security of these schemes. Furthermore, as we are understanding these problems better, we are also refining our understanding on how we should pick parameters to balance security and performance requirements.

But there are also many open questions that go beyond such foundational inquiries: can our protocols cope with those post-quantum primitives? For example, OpenSSH packets cannot currently hold McEliece public keys, they are too big. But even if a protocol allows for larger keys or ciphertexts, what would break on the Internet if we were to actually deploy these schemes? Similarly, when protocols rely on the non-interactive version of the Diffie-Hellman key agreement, they are in for a rude awakening; the only post-quantum candidate (based on SIDH) for this variant is very slow. Thus, there is a lot of exciting research to be done before we can deploy post quantum cryptography.

IOT SECURITY FAILURES AS PRODUCT DEFECT: THE COMING WAVE OF STRICT LIABILITY

Robert Carolina

> Executive Director of the Institute for Cyber Security Innovation and ISG Senior Visiting Fellow

As connected devices increasingly control or influence systems capable of inflicting death or personal injury, a new wave of liability is set to wash over the world of cyber security: strict liability for defective products. Control devices are connected and enter the Internet of Things (IoT) world, and risks caused by cyber security failures thus grow from mere risk of financial loss to risk of death and personal injury. When death and personal injury are on the line, liability rules change dramatically.

Victims of defective products are not required to demonstrate the "fault" of a product manufacturer. It's enough to demonstrate the existence of a defect in the product that causes harm. Under European laws, "a product is defective when it does not provide the safety which a person is entitled to expect taking all circumstances into account…" [1] at Art.6; [2] at s.3.

Product strict liability has always been a source of concern for manufacturers (and importers, who are subject to the same liability). They are obviously concerned about liability in the absence of fault. Unlike many other forms of liability (like warranty), manufacturers are practically unable to limit this liability to victims who sue alone or collectively in a class action.

Two important conditions must exist before a victim can succeed on a strict liability claim:

1) There must be a "product" which is defective

2) A victim harmed by a defective product can only use this legal theory to claim compensation for death or personal injury (or damage to non-commercial property under the laws of the EU). Economic harm, business interruption, loss of business revenue, etc, are not recoverable under this theory.

These two conditions made strict liability a niche topic or an intellectual curiosity for most lawyers working in the fields of software development and cyber security and meant that it was traditionally overlooked in these fields. For decades we have taken comfort in the widely shared legal opinion that software, as such, does not fit within the definition of "product" under European or American laws. Even if software was to be viewed as a product, we reasoned, opportunities for defective software design to cause death or personal injury seemed exceedingly rare.

One long-understood risk of strict liability concerns defective software control systems as a component in safety-critical hardware. The manufacturer of the resulting defective hardware is subject to strict liability claims, irrespective of the source of the defect.

This risk can be illustrated with the example of the Therac-25 radiation therapy machine. Between 1985-87, six patients treated using the Therac-25 were exposed to massive radiation overdoses (100x intended dose). Three of these patients died as a result of the overdoses. The design of the machine's system control software is widely cited as a cause of the overdose incidents, which were thankfully rare.

Under a strict liability analysis, the Therac-25 device as a whole is a "product". If the machine failed to provide the "safety which a person is entitled to expect," such a product would be defective and the manufacturer strictly liable for personal injury or death. The fact that the flaw originated in control software would be irrelevant.

For decades, my legal colleagues and I rested comfortable in the belief that software errors (including software security flaws) rarely killed anyone. Today, by contrast, the IoT presents a rapidly growing set of opportunities for "death by software". A net-connected software-controlled product (e.g., an autonomous vehicle, an industrial control system, a pacemaker, a vehicle using fly-by-wire) that fails to deliver appropriate safety, is defective whether the safety is compromised through the design of electrical, mechanical, software, or security, systems.

Thus strict liability applies to products whether safety is compromised through errors in algorithmic decision-making (e.g., an autonomous vehicle decides to swerve into oncoming traffic after misreading road markings) or security errors (e.g., a broken authentication scheme permits a remote hacker to divert the same vehicle into oncoming traffic).

While the hardware product manufacturer (or importer) is clearly subject to the risk of strict liability, what about those in the upstream supply chain? What if, for example, the manufacturer of the Therac-25 had purchased their control software from a third party as a component, or the autonomous vehicle manufacturer adopts and installs a defective authentication package embodied in third-party software?

Under current law, defective component "product" manufacturers face strict liability. A manufacturer of defective brakes, for example, is strictly liable for personal injury caused by automobiles which become defective because the defective brakes are installed.

Software (on its own) is not currently thought to be a product in this area of law. The author of a defective software component probably cannot face a strict liability claim from an injured victim – even if the software caused the hardware product to harm the victim.

This may be about to change.

More than three decades have passed since the 1985 adoption of the European Directive on product strict liability [1]. The reliance society places on software and online services has become a central feature of everyday life. European policy makers have noticed, and the tide of product liability policy appears to be shifting.

The European Commission completed a comprehensive evaluation of European product liability law in 2018. The term "software" features prominently, and repeatedly, in the 108-page report [3]. The Commission openly questions the extent to which "digital products" (e.g., software as a product, SaaS, PaaS, IaaS, data services, etc.) should be redefined as "products" and thus subjected to strict liability analysis when defects cause death or personal injury [4].

A Commission Expert Group on liability and new technologies is currently examining possible changes to the law. Expanding the definition of "product" is central to this review.

We seem to be accelerating towards a world in which cyber security failures in the IoT will create increasing risk to life and limb. Manufactures of tangible IoT products already face strict liability if their product is unsafe – including cases where safety is compromised by poor cyber security. It appears that software developers, SaaS providers, and other cloud service providers, may soon be required to step up to this same stringent standard of responsibility throughout Europe. We hope they'll be prepared for the challenge.

References

[1] European Economic Community, Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), vol. L210, 1985, p. 29.

[2] Consumer Protection Act 1987.

[3] European Commission, Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the liability for defective products, Brussels, 2018.

[4] European Commission, Liability for emerging digital technologies, Brussels, 2018.

UPDATES ON SYSTEMS & SOFTWARE SECURITY LAB (S3LAB)

DANIELE SGANDURRA & JORGE BLASCO ALIS

> Senior Lecturer ISG, S3 Lab & Lecturer ISG, S3Lab

The Systems & Software Security Lab (S3Lab) in the Information Security Group (ISG) at Royal Holloway was established in September 2018 to research novel techniques and tools to protect systems against malicious threats. S3Lab evolved from the Systems Security Research Lab (S2Lab), which was founded by Lorenzo Cavallaro in September 2014. Although we are still in a bootstrapping phase, this has been a very thriving period for the S3lab, and its members have been involved in several activities, some of which are described in this article. Please visit our website (https://s3lab.isg.rhul.ac.uk/) to find out more about our ongoing activities and projects.

ONGOING PROJECTS: FOCUS ON FUTURETPM

Future TPM (Future Proofing The Connected World: A Quantum-Resistant Trusted Platform Module). Trusted Platform Modules (TPMs) are currently incorporated into over a billion computers worldwide. A TPM is a security anchor, also known as root-of-trust, which is commonly used in domains with a strong requirement for security, privacy and trust, such as finance and banking (secure mobile payment), wearables (activity tracking) and device management. S3Lab is part of the consortium working on the H2020 Project 'FutureTPM', which is focusing on developing next-generation security solutions to mitigate against quantum computers. These computers are anticipated to be able to break some of the cryptographic algorithms currently used in existing TPMs. You can find more information about FutureTPM on the project website: https://futuretpm.eu/

HIGHLIGHTS OF EVENTS

1st Workshop on Quantum-Resistant Crypto Algorithms. On the 19th of October 2018, S3Lab members organized and participated in the 1st Workshop on Quantum-Resistant (QR) Crypto Algorithms suitable for inclusion in TPMs, which took place in Lisbon, Portugal. At this workshop we presented a first set of preliminary results from the FutureTPM project in researching QR cryptographic algorithms that are suitable for inclusion in a TPM. The workshop was attended by more than 60 academic and industry experts from the quantum-safe cryptography community.

Smallpeice Residential Capture the Flag. Members of the ISG and S3Lab organized the "Smallpeice Residential Capture the Flag (CTF)" event on 2nd April 2019 at Royal Holloway's campus in Egham, which was attended by 60 Year 9 students. The main goal of Smallpeice Residential CFT is to provide a fun and compelling learning experience for students through a set of online and offline cyber-security challenges. The philosophy underpinning this event is to inspire young students to consider cyber-security from a different perspective — that of cyber-attackers — as a practical step to understand how vulnerabilities get exploited in real systems and how to mitigate them. The activities were led by Joe Rowell, a first-year ISG PhD student in the EPSRC Centre for Doctoral Training (CDT) in Cyber Security. Joe collaborated with S3Lab in setting up the environment with the cyber-security challenges to be solved.

HIGHLIGHTS OF RESEARCH ACTIVITIES

Cyber Security Academic Startup Acceleration Program. We have been selected in CyberASAP (Cyber Security Academic Startup Acceleration Program) with a project to secure Bluetooth Low Energy enabled devices. CyberASAP is an academic start-up acceleration program funded by DCMS and run by InnovateUK where academics are mentored to transform research into business products.

Paper Accepted At 28Th Usenix Security Symposium 2019. In a recently published paper (https://arxiv.org/abs/1808.03778), to be presented at the 28th USENIX Security Symposium in August 2019, Pallavi Sivakumaran and Jorge Blasco Alis analyse the number of Bluetooth Low Energy devices that have application layer security and therefore are protected against attacks by applications co-located on the same device. You can find the tool we developed for the paper at: https://github.com/projectbtle/BLECryptracer.

Paper Accepted At 16th Dimva Conference 2019. In a paper to be presented at DIMVA 2019 on 19th/20th June 2019, Daniele Sgandurra, in collaboration with Ziya Alper Genç and Gabriele Lenzini, from the Interdisciplinary Centre for Security Reliability and Trust (SnT), University of Luxembourg, analyse existing decoy strategies and discuss how effective they are in countering current ransomware by defining a set of metrics to measure their robustness. To demonstrate how ransomware can identify existing deception-based detection strategies, they have implemented a proof-of concept anti-decoy ransomware (available at: https://github.com/ziyagenc/decoy-updater) that successfully bypasses decoys by using a decision engine with few rules.

HIGHLIGHTS OF PHD STUDENTS

Security And Privacy Concerns With Data On Bluetooth Low Energy Peripherals (Pallavi Sivakumaran, CDT). Bluetooth Low Energy (BLE) is an IoT-enabling technology, which is rapidly gaining popularity, particularly for consumer applications. Despite BLE being a technology with many potential applications, it has not been studied widely in terms of security. In particular, application- or domain-agnostic security research has been fairly limited. The overall aim of this research is to identify security-related issues with the BLE standard or its implementations (including those on mobile devices), which affect the data residing on BLE devices, and to come up with solutions for improving the security of BLE-enabled systems.

Malware Attribution (Jason Gray, CDT). Attributing a piece of malware to its creator or user is a difficult problem. It relies upon the ability to disassemble binaries efficiently to gather sufficient features to de-anonymise the author(s). In the modern world of cyber warfare and cyber criminals, public attribution is being used to ensure justice, apply political pressure and enforce sanctions to deter cyber attacks. However, attribution requires a lot of concrete

evidence which is often a complex and time-consuming manual task. It often takes at least a year to publicly attribute, if not longer. This is due to attackers using several techniques (e.g., obfuscation) to hide their identity and prevent others from understanding their goal(s). Even though attackers go to extreme lengths to hide their identity, there are often unique traces (their "signature") which we can find to link them to other pieces of malware. Unique author styles have been identified in source code, yet there remains a lot of research to identify the same styles in compiled source code. Further, there is a big demand for automating malware author attribution due to the continued increase in attacks and an insufficient number of analysts to match the malware analysis demand.

Android Data-Flow Analysis (Marcos Tileria, CDT). My first year in the CDT led me to my current research as part of the S3Lab. In the CDT, we explored a variety of topics in different areas, which left me with many positive experiences and lessons learned. This approach also gave me a broader view of Information Security research and opened my mind to new perspectives. The foundational year finished with the summer project and marked the start of my main PhD research. The summer project was not only an amazing experience, it also helped shape my PhD research approach. I worked on the problem of Key Management for the Interplanetary Internet. It might sound a bit Sci-fi, but it is a real problem that space agencies and standardisation bodies have been studying for the last 10 years. I even had the chance to visit the Operation Centre of SSTL at Guilford, and I kept in constant communication with two senior NASA JPL engineers during this project. Now I am part of the S3Lab and my research focuses on Android vulnerabilities. Android provides a secure mechanism to protect sensitive information, but apps can still carry out malicious action through inter-component and inter-app communication. I am sure there are new exciting experiences and possibilities just around the corner and I am very much looking forward to continuing with my research.

INTRODUCING YOU SHAPE SECURITY – NEW SECURITY GUIDANCE FROM NCSC

Through its participation in the UK's Research Institute in Science of Cyber Security, the ISG has contributed to the development of new people-centred security guidance from NCSC. Lizzie Coles-Kemp's work on creative security engagements is one of the examples of interaction types that NCSC features when talking about approaches that security practitioners can adopt when forming and maintaining positive interactions.

In this article Ceri from NCSC tells us a little more about the new guidance called You Shape Security.

The NCSC has long recognised that people are part of the solution when talking about Cyber Security, not the problem. The idea that people are the cause of all security infractions because they are weak, lazy or malicious is one that is increasingly outmoded. In a competitive world where organisations must adapt, changing function and focus in response to changing markets and trends, it is unsurprising to see the people in those organisations also adapt to meet those challenges. Security processes often become an area where things that work get adopted, and things that don't get adapted or dropped.

With the help of our academic partners across many different universities and through RISCS (Research Institute in Science of Cyber Security) we have focused on understanding the people, their drivers and motivations when choosing whether to follow the security practices demanded by their organisations. For the NCSC, whilst we have been building knowledge and expertise in this crucial area of security, we have also been using it to inform the blogs and guidance we have written, and the talks we have delivered over the last 4 years. But until now we haven't met the challenge of pulling all that research through and formally expressing it in the form of NCSC guidance.

That has changed with the publication of "You Shape Security". We haven't created an easy to adopt tool or framework; we even hesitated to call it guidance. Instead we wanted to disrupt those more traditional views that technology equals security and challenge the belief that the further people are kept away from security the better.

You Shape Security recognises that breaking down barriers and opening the dialogue around security is not easy. If people have brought some creative thinking into how they deal with security in order to get the job done organisations need to recognise the competing priorities and stresses that have driven that adaptation. Equally, people shouldn't fear security but should feel they can work with it and know it's a place that can and will support them in working safely and securely.

People's work environment is often managed for them and therefore they lack the autonomy and authority to make changes to the way security procedures have been set out for them. What we hope people take from the You Shape Security work is encouragement to reflect on how security works within their organisation, their team and their role. And that organisations begin looking at what is proportionate and realistic in relation to balancing their security needs and their changing organisational needs; to begin to recognise that all the policies and training in the world does not equal good security.
To build in feedback loops and resilience across an organisation that adapts to change instead of being stuck with policies and processes that were written for a time that no longer exists. Or written with a view that they are theoretically secure, without understanding how they work in practice across different areas of the business.

We also recognise that we can't keep expecting security professionals to have all the answers either. We all have a story to tell, experience to add, and ways from which an organisation can learn what security really needs to look like to work effectively and efficiently. It should be a truly collective consideration.

An organisational security culture based on the premise that people are the weakest link is never going to move the organisation or its security forward. What we say in You Shape Security is that organisations should be listening to and learning from those who are expected to blindly follow rules or policy, even when they can't. Businesses need to move from security being something it does to staff to being one where security is baked into an organisation's operations. Issuing security edicts, warning about threats and running blanket one-size-fits-all training needs reshaping into a function that can support people, that encourages engagement and can adapt.

Finally, I would like to thank for all the support, mentoring and inspiration from all those involved in making this guidance a reality.
--
The guidance can be accessed through the NCSC website: https://www.ncsc.gov.uk/collection/you-shape-security

THE ISG SMART CARD AND INTERNET OF THINGS SECURITY CENTRE (SCC)

Konstantinos Markantonakis

> Professor ISG, Director of the SCC

In 2018, we celebrated the successful completion of four students supervised by the SCC. They are: Dr Carlton Shepherd, “Techniques for Establishing Trust in Modern Constrained Sensing Platforms with Trusted Execution Environments”; Dr Iakovos Gurulian, “On Enhancing the Security of Time Constrained Mobile Contactless Transactions”; Dr Robert Lee, “Schemes and Applications for Binding Hardware and Software in Computing Devices”; and Rashedul Hassan, “Cheat detection and security in Video Games”. All four were supervised by Prof Konstantinos Markantonakis. Well done to them! At the same time, the SCC is expanding its research efforts in its established research threads, including payment systems, automotive, blockchain and smart contracts, secure application execution, and we are looking for hard working and ambitious PhD candidates to join our research team.

The SCC initiated and designed the SCC Summer Internship Programme (SCC-SIP) in order to provide undergraduate students with first-hand experience of research and development at the highest level. This enables them to work with experienced researchers on real-world problems related to cybersecurity and privacy. We provide support and direction in selecting a real-world research question, co-developing it, finding the core issues and proposing realistic solutions. The programme has a significant research and programming (development) component, and an emphasis on exploring commercialisation opportunities. During the summer of 2018 we worked with eleven amazing students, investigating a range of topics, including data provenance, machine/deep learning, visualisation, blockchain, smart contracts, e-voting, syscall and database monitoring. Five papers resulting from some of this work [1, 2, 3, 4, 5] were published in international conferences.

One of these internship papers presented a proof of concept for open, transparent, fair and independently auditable government procurement systems using blockchain technology [3] and was also reported in online publishing platform Medium. Independently of the SCC work, researchers from The World Economic Forum (WEF) engaged in a project to develop an open government procurement system in conjunction with universities in the USA and Colombia. The SCC team are now acting as advisors to the WEF project “Smart-Contract based Digital Procurement System in Colombia.”

In March 2019, Dr Raja Naeem Akram and Prof. Konstantinos Markantonakis, secured two grant awards from the Innovate UK Cyber security academic start-up accelerate programme (CyberASAP). Prof. Markantonakis will lead “Transparent Compliance”, a project that will develop technology that generates real-time analysis of the security and privacy compliance of an organisation. Dr Akram will lead “AISecure”, a project that will develop novel tools for evaluating the security and privacy resilience of an AI algorithm against a comprehensive set of threat vectors.
For the latest generation of encrypted mobile devices (BlackBerry’s PGP, Apple’s iPhone), data extraction is a complex task which provides a significant challenge to forensic experts. In 2018, the SCC welcomed Dr Thibaut Heckmann from École Normale Supérieure (ENS) as an academic visitor. While visiting the SCC, Dr Heckmann collaborated with the Forensic Science Laboratory of the French National Gendarmerie (IRCGN) to develop physical recovery of data on encrypted systems for the purpose of forensic analysis. This resulted in two publications [6, 7] and Dr Heckmann was awarded the "European Emerging Forensic Scientist Award 2018-2021" at the European Academy of Forensic Science (EAFS) conference.

Other SCC highlights:

- In February 2019, the SCC hosted a PhD Student from ENS, Mr Georges-Axel Jaloyan, who is working on demonstrating that RISC-V, a new instruction set architecture for embedded systems, is vulnerable to Return-oriented programming (ROP) attacks.
- In March 2019, Prof. Markantonakis, delivered his inaugural lecture “Embedded system security, bridging theory and practice, towards a new era of Internet-of-Things (IoT) devices”.
- On 28th August 2019, the SCC will be celebrating its 17th anniversary by hosting the SCC Open Day, with a mixture of exhibits from industry and SCC researchers. Please get in touch if you wish to exhibit at this event.
- The SCC is in discussion with partners about the development of a Capture-the-Thing (CtT)™ event dedicated to embedded systems and IoT devices. If you are interested in involvement as a sponsor, co-developer or contributor to this exercise, please contact Prof. Markantonakis.

Finally, after 17 years located in Royal Holloway’s iconic Founders Building, the SCC is in the process of relocating to the newly refurbished Bedford Building, where we will join the rest of our colleagues from the ISG. While we have always been an integral part of the ISG, this closer proximity to our colleagues can only enhance our activities.

References

[1]Julia Meister, Raja Naeem Akram, Konstantinos Markantonakis, “Deep Learning Application in Security and Privacy - Theory and Practice”, the 12th WISTP International Conference on Information Security Theory and Practice (WISTP'2018). Blazy, O. & Yeun, C. Y. (eds.). Brussels, Belgium: Springer-Verlag,– BEST STUDENT PAPER AWARD

[2]James Tapsell, Raja Naeem Akram, Konstantinos Markantonakis, “Consumer Centric Data Control, Tracking and Transparency – A Position Paper”, the 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, New York, United States, 6 Sep 2018.

[3]Freya Sheer Hardwick, Raja Naeem Akram, Konstantinos Markantonakis, “Fair and Transparent Blockchain based Tendering Framework – A Step Towards Open Governance”, the 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, New York, United States, 6 Sep 2018.

[4] James Tapsell, Raja Naeem Akram, Konstantinos Markantonakis, “An Evaluation of the Security of the Bitcoin Peer-to- Peer Network”, the 2018 IEEE Conference on Blockchain, Halifax, Canada, 22 May 2018.

[5] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, Konstantinos Markantonakis, “E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy“, the 2018 IEEE Conference on Blockchain, Halifax, Canada, 22 May 2018.

[6] Thibaut Heckmann, Konstantinos Markantonakis, David Naccache, Thomas Souvignet, “Forensic smartphone analysis using adhesives: Transplantation of Package on Package components”, Journal of Digital Investigation, Vol. 26, 09.2018, p. 29-39.

[7] Thibaut Heckmann, David Naccache, James McEvoy, Raja Naeem Akram, Konstantinos Markantonakis, “Removing epoxy underfill between neighbouring components using acid for component chip-off”, accepted in the Journal of Digital Investigation

TEES: A BRIGHT FUTURE FOR CLOUD COMPUTING SECURITY?

Dan O'Keeffe,

> Lecturer, Dept. Computer Science, RHUL

A fundamental security problem when hosting applications on cloud platforms is the increased risk of sensitive data loss (e.g. due to negligent or malicious employees of the cloud provider). Unfortunately, existing approaches to mitigating such attacks have serious limitations. For example, simple encryption techniques like client-side encryption limit the ability to compute over cloud-hosted data. More advanced homomorphic encryption schemes allow for encrypted computation, but either impose a very large performance penalty in the case of fully homomorphic encryption, or do not support arbitrary programs in the case of partial homomorphic encryption.

Background

An exciting new approach to mitigating cloud insider attacks are hardware-enforced trusted execution environments (e.g. Intel SGX), recently available on commodity CPUs [1]. Intel SGX allows for the creation of secure enclaves on remote cloud computers, such that enclave code and data is protected from an underlying malicious operating system or hypervisor, and also from physical attacks. Demand for these powerful security guarantees is evident from the rapid emergence of commercial SGX offerings in major cloud providers (e.g. Microsoft Azure Confidential Computing).

Intel SGX research overview

Despite commercial availability of SGX hardware, migrating complex legacy applications to SGX enclaves is non-trivial. An important restriction of the SGX model is that only user-level (ring 3) code may execute within an enclave. Operating system calls (e.g. to perform I/O) must therefore be executed outside the enclave, raising the possibility of so called Iago attacks, where a malicious OS returns invalid system call results in order to subvert an enclave. Furthermore, enclave transitions impose a high overhead due to various security bookkeeping operations (e.g. translation lookaside buffer flushes). Another important caveat is that Intel SGX does nothing to prevent bugs in enclave code from exposing sensitive data. Existing security principles such as reducing the system trusted computing base (TCB) and overall attack surface (i.e. enclave code and interface sizes) are therefore still key for enclave applications.

Migrating legacy applications to Intel SGX

Researchers have explored several points in the design space to address the above concerns. On one end of the spectrum, library operating system approaches allow to execute mostly unmodified binaries within the enclave [2]. Although convenient, from a security perspective including an OS inside the enclave increases the TCB significantly. On the other hand, the library OS approach potentially allows for a much narrower enclave interface in comparison to the complete system call API (e.g. POSIX), simplifying the task of hardening against Iago attacks.

At the other end of the spectrum, automated application partitioning techniques have been proposed to identify the subset of application components that require access to sensitive data and place only those within the enclave [3]. This can result in a significantly smaller TCB, but for some applications may result in a larger enclave interface and performance overhead due to an increase in the number of transitions.

A middle ground between the above two extremes is SCONE [4]. Instead of a full library operating system, it includes only the C standard library (libC) within the enclave, resulting in a reduced TCB in comparison to a complete library OS at the cost of a slight increase in enclave interface size. Conversely, in comparison to partitioning SCONE has a larger TCB but smaller enclave interface. SCONE also introduces an asynchronous system call technique that significantly improves performance by avoiding expensive enclave transitions.

Side-channel attacks on Intel SGX

In addition to systems software support for enclave applications, another important line of security research relates to the susceptibility of enclaves to a variety of side-channel attacks. Although already important for cryptographic libraries, and more recently for general purpose cloud computing due to the risk of inter-VM side channel attacks, the powerful threat model espoused by Intel SGX significantly increases the risk potential. In comparison to inter-VM settings where at least the hypervisor is trusted, in the SGX model the system software is potentially malicious. This allows for powerful attacks such as deterministic side channels based on page-faults [5], in addition to a variety of cache and DRAM attacks.

Most recently, speculative execution side-channel attacks have been demonstrated that effectively dismantle the security guarantees of Intel SGX [6]. Although some mitigations for side-channel attacks have been have been announced, this will be an active area for future research for the foreseeable future.

SGX applications

Apart from systems support and side channel research, the availability of a TEE with near-native performance on commodity CPUs opens up opportunities for a variety of interesting new applications beyond cloud computing. For example, recent work has explored how to leverage Intel SGX in the context of blockchains. Proposals include using SGX to increase scalability through secure off-chain payments [7] and to support private execution for smart contracts [8]. Another promising application area is to support privacy preserving secure Edge Computing e.g. for accelerating Internet of Things and Augmented Reality applications with low-latency requirements by offloading computation to nearby base stations or even other mobile devices.

Royal Holloway SGX research

At Royal Holloway, ongoing work is investigating how to harden code inside enclaves. A challenge here is that hardening techniques cannot rely on kernel support (e.g. for process isolation), since the OS is untrusted, increasing the importance of compiler-based hardening techniques. Another exciting line of research relates to potential risks of SGX-like technology. In particular, SGX raises the possibility of a new class of powerful malware that execute within enclaves, invisible to existing signature-based anti-virus tools [9]. Exploring the risks of such malware and also potential mitigations will be increasingly important as SGX becomes more widely available.

References

1. Software Guard Extensions Programming Reference, Ref. 329298-002US. https://software.intel.com/sites/default/files/managed/48/88/329298-002.pdf, 2014
2. Shielding Applications from an Untrusted Cloud with Haven, Baumann et al, USENIX OSDI '14.
3. Glamdring: Automatic Application Partitioning for Intel SGX, Lind et al, USENIX ATC '17.
4. SCONE: Secure Linux Containers with Intel SGX, Arnautov et al, USENIX OSDI '16.
5. Controlled-channel attacks: Deterministic Side-Channels for Untrusted Operating Systems, Xu et al, IEEE Security & Privacy '15.
6. Foreshadow: Extracting the keys to the Intel SGX kingdom with transient out-of-order execution, Van Bulck et al, Usenix Security '18
7. Teechain: A Secure Asynchronous Blockchain Payment Network, Lind et al, https://arxiv.org/abs/1707.05454
8. Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution, https://arxiv.org/abs/1804.05141
9. Practical Enclave Malware with Intel SGX, Schwarz et al, https://arxiv.org/abs/1902.03256

Facebook:
Information Security Group (ISG) RHUL Official
facebook.com/ISGofficial

Twitter:
twitter.com/isgnews
@ISGnews

LinkedIn:
linkedin.com/groups?gid=3859497

You Tube
youtube.com/isgofficial

CONTACT INFORMATION:

For further information about the Information Security Group, please contact:

Information Security Group
Royal Holloway, University of London
Egham, Surrey, TW20 0EX
United Kingdom

T: +44 (0)1784 276769
E: isg@royalholloway.ac.uk
W: www.royalholloway.ac.uk/isg