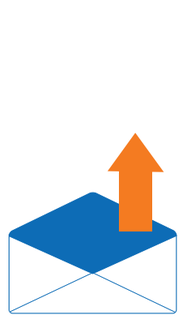
Information Security Group

Review 21/22

ROYAL HOLLOWAY UNIVERSITY OF LONDON

INDEX



INTRODUCTION
Chris Mitchell

> Prof. ISG, Head of Department, Information Security

Welcome to another ISG Review. When I joined Royal Holloway back in 1990 to become Head of the Department of Computer Science, I hardly imagined that over 32 years later I would be the new, albeit very much interim, head of a stand-alone Department of Information Security, having assumed the role in August 2021. Of course, I always knew that Information Security was important, but back then the idea of a separate academic department devoted to the subject, something I believe is unique in the UK, would not even have entered our heads. How things have changed!

I must first give huge thanks to my predecessor as Head of Department, Professor Peter Komisarczuk, for his tireless efforts in leading the department through some very difficult times over the last three years. When he took over as head back in the summer of 2018 he could hardly have envisaged having to manage the ISG through a global pandemic, with a move to online teaching and a January student intake happening almost overnight. That we have survived largely intact is a miracle in itself, and is down to Peter’s leadership and the hard work of all our colleagues.

It has been another very challenging year for the department, and, of course, for the world. Whilst we have largely moved back to campus teaching for the 2021/22 academic year, we are still feeling the effects of Covid-19. We have had to continue live-streaming all lectures for the benefit of students unable to make it to campus, and some colleagues have been obliged to continue delivering material online as they are and/or their partners are vulnerable. In January 2022, our second cohort of ‘January start’ MSc students arrived, meaning that for the second year in a row we are teaching every masters course twice (and those in block mode three times).

On a more positive note, I believe that we can finally see light at the end of the tunnel. There is genuine hope that from the start of the 2022/23 academic year we will return to something close to normal, with a single student intake, allowing us the time and space to think about new courses and new ways of delivering and assessing our existing material. It has, and continues to be, a year of change for the department. Two long-standing members of the department have departed, at least in terms of their roles as members of staff. Professor Carlos Cid is leaving for new opportunities in Norway and Japan, after nearly 20 years of valuable service to the department. Professor Keith Mayes is retiring, but will continue to be active as an Emeritus Professor (as he describes in an article later in this newsletter). We will greatly miss them both, and I would like to personally think them both for the huge amount they have done for the ISG over the past two decades.

At the same time, the 2021-22 academic year has seen (and will see) the arrival of at least six new members of academic staff. As I write (in March 2022), Dr Guido Schmitz and Dr Saqib Kakvi are on board as new lecturers in Information Security. Dr Christian Weinert and Dr Santanu Dash are expected to join us as lecturers in April, with Dr Fauzia Idrees joining us as a Senior Lecturer and Director of the new Cyber Security Distance Learning MSc soon afterwards. Finally, we expect Dr Andrew Dwyer to join us as a further new lecturer in September. I confidently expect this influx of new talent to enhance and develop our research and teaching, and I am sure you will hear from them in future editions of the newsletter.

There are also many exciting new developments in teaching and research to report. We are in the process of launching a new distance learning MSc in Cyber Security jointly with the University of London and Coursera, as reported on in more detail in Peter Komisarczuk’s article in this newsletter. The Centre of Doctoral Training continues to go from strength to strength (see Keith Martin’s article later in this newsletter). Late last year the ISG received an Academic Centre of Excellence in Cyber Security Education (ACE-CSE) Gold Award recognising excellence in cyber security education and good practice from the National Cyber Security Centre (NCSC). Also, by the time this newsletter reaches you, the ISG will have another new Head of Department, as my short-term interim headship comes to an end, and I wish her or him all the very best in further developing and enhancing the work of the department.
In summary, despite the huge difficulties over the past couple of years, we find ourselves in a great position to continue to grow and develop, and this newsletter provides an overview of some of our many activities. We hope that you enjoy the articles, and that if any of the topics mentioned spike your interest, please do get in touch. Exciting times are ahead!

STAFF PROFILE: GUIDO SCHMITZ

How did you become interested in Computer Science?
When I was in primary school, my parents got me one of these typical 90's learning computers that run quizzes and other educational programs. It did not take long for me to find out that there was also a BASIC interpreter on this machine, and I took my first steps in programming. Although that machine was quite cumbersome, as the device only had a 16x2 LCD character display, it fascinated me a lot! Also, I got hold of my sister's C64, and that classic computer allowed me to learn much more on the topic. A few years later, I joined the local computer club and quickly became the administrator of their network, a perfect playground for exploring and trying many different things. I also discovered my passion for teaching there and held programming courses.

How did you become interested in Information Security?
While working with networked environments, security became a hot topic for me. During my computer science studies at the University of Trier, I also worked part-time as the computer science department's system administrator and became responsible for some central infrastructure (including some production systems of DBLP). Here, security was an essential aspect of my job. As-luck-would-have-it, at that time, Ralf Küsters joined our university as a professor in information security and cryptography and introduced several fascinating modules on that topic. This combination of practical work and the academic view on the subject got me profoundly engaged with information security.

Tell us about your research.
I am working on formal methods to analyse the security and privacy of protocols. Using this approach, we can detect flaws and errors in their specifications and even identify new classes of attacks. Based on these insights, we can develop fixes and (if these are sufficient) prove strong security and privacy properties. I have co-authored the web infrastructure model (WIM), the most comprehensive formal model of the web infrastructure to date. With the WIM, we have uncovered several severe security flaws in central protocols of the web, including single sign-on and authorisation protocols such as OAuth and OpenID Connect. This work has even sparked a new conference series, the OAuth Security Workshop, that I am organising in collaboration with the IETF.

Furthermore, with colleagues at INRIA, University of Stuttgart, and IIT Gandhinagar, we are developing a new framework, DY*, for tool-supported and modular analysis of such systems. Using this approach, we will be able to ease further analyses while eliminating human error. So far, we have already applied DY* to prove strong security properties for protocols like Signal and ACME. DY* will also be the foundation for mechanising the WIM, which is hard to achieve with existing tools.

Your research facilitates the discovery of new vulnerabilities. Isn't that a double-edged sword?
My primary motivation is to make systems secure. To this end, it is essential to have tools to systematically and rigorously analyse a system for its weaknesses. Knowledge of these problems is key to eliminating them and making a system secure. If we do not have such methods at hand, it is up to chance and creativity whoever finds such problems first. If you are out of luck, the “evildoers” could already leverage these vulnerabilities without the good team knowing about their existence. Hence, my research enables the good guys to identify and eliminate problems before these can be exploited.

What are the joy and challenges of being a lecturer?
The academic world comes with many benefits, such as freedom and independence of research and the opportunity to teach and engage students with your subject. It is a great combination to explore and conquer new fields of knowledge while at the same time educating the experts of tomorrow. While there is a lot of freedom, you are also part of a rather large, complex organisation that demands and develops your organisational skills. When I started at the University of Stuttgart, I was part of a team to set up a completely new institute/department and developing new modules on information security for their degree programmes. We began this start-up-like journey from scratch, and that was a major adventure since we had to integrate into a huge administrative body typical for large German universities.

How did you cope with the impact of the pandemic on university life?
When the pandemic started, I was teaching in Germany. We didn’t have any experience with distance learning or online teaching in our group. Moreover, we were just a few weeks away from starting teaching in the summer term when everything came to a standstill in March 2020. It was pretty challenging to move all teaching online in such a short time. As the lead of our institute’s task force, I was responsible for sorting out didactic and technical challenges for our teaching activities. It was gratifying for our close-knit team to get very positive feedback from our students in response to our efforts. When I joined the ISG last December, it almost felt natural doing the lectures online. Nonetheless, I am looking forward to returning to in-person teaching!

It has been rumoured that you have a strong neck for Raspberry Pi(e)?
While I enjoy baking, for example, German Apfelkuchen, I honestly haven’t made a Raspberry Pie yet, although I have “baked” projects with the Raspberry Pi. This fascinating little device significantly reduced the barrier for everyone, including school kids, to get engaged with computer science. When the device was announced in 2012, some friends and I at our university had the idea to organise a workshop/mini-conference, which we called “Pi and More”. We brought a good set of people together at this first event and had many exciting talks, discussions, and tutorials.
As this was a big success, we continued to organise follow-up events and professionalised them with a non-profit association we founded. That quickly evolved into the longest-running and largest Raspberry Pi event series within Germany, with more than 350 participants at later events. While our in-person events are still suspended (our latest event was supposed to take place on the day Germany went into lockdown), we kept the spirit of the events alive in a virtual format and are eager to resume this popular event series.

KEITH MAYES “A NEW CHAPTER”

Chris Mitchell (with support from Keith Mayes)

> **Prof. ISG**
> **Prof. ISG**

Prof. Keith Mayes transitioned to become an emeritus Professor at Royal Holloway on the 1st May 2022, after nearly two decades employed as an ISG academic staff member … I caught up with him recently to find out more about his reflections in 20 years as an academic and his exciting future plans.

How did you end up joining Royal Holloway?
Serendipity! I had been working in industry and had decided to leave my current job as the Vodafone Global SIM Card Manager to set up my own consultancy company. I had one leg out of the door when Prof Michael Walker (head of Vodafone R&D) suggested I apply for a new post in the ISG. I was uncertain until a meeting at an M4 service station café with the legendary Prof Fred Piper. Fred encouraged me to apply, and I was fortunate to be offered the post as the Founder Director of the ISG Smart Card Centre (SCC), which was a collaboration between the ISG, and two companies that I knew well; Vodafone and Giesecke & Devrient.

How was your transition from industry to academia?
It was initially a culture shock. When my colleague Kostas Markantonakis and I moved into the first SCC home in Orchard building, we had one chair and one light bulb between us, and our equipment was a box of donated old laptops and card readers. We eventually overcame many hurdles and properly established the SCC in Founders; its long-time home.

In industry I worked hard, often under stressful conditions and time pressures, however the scope of an individual task was relatively narrow. So it came as a surprise that as an academic I was expected to be simultaneously great at research, teaching, external engagement, consultancy, bringing in funding, having real world impact, serving the academic community, management and of course authoring world-class academic papers and books!

Briefly tell us about your career with the ISG
When I worked in industry I knew of the ISG by reputation, so I was proud (and a little intimidated) to join it in 2002. As someone who fell into academia by chance, I was very pleasantly surprised to become a professor in 2011. The first 13 years of my academic career were tied up with leading the SCC and supporting its teaching, research and external engagement activities. I handed the SCC baton to Kostas in 2015 when I became the ISG Head of Department, and then a year later the Head of the School of Maths and Information Security. In 2020 I served as the ISG Director, sharing ISG leadership responsibilities with Peter Komisarczuk, and then in 2021 I was appointed as the Director of the Royal Holloway Research Catalyst, “Transformative Digital Technologies, Security and Society”. For 2022 I am also the chair of the International Cyber Security Center of Excellence (INCS-CoE).

What did you enjoy best about being and ISG academic?
As I never abandoned my former self or interests, I consider myself to be an engineer having a life-chapter entwined in academia; however the 2002 imposter-syndrome version of myself would have loved being called an ISG academic! The most fulfilling aspects involved interaction with people, and especially where I knew I went the extra mile to help students and colleagues; in turn I am grateful for all the help that I received. I get bored with repetition, but I don’t remember being bored at Royal Holloway; in fact the diversity of activities and opportunities has given me many positive experiences that I could not have imagined.

What have been your main research interests during your time at Royal Holloway?
Technology and engineering are in my blood. I took a schoolboy’s electronics hobby into an engineering degree, PhD and my early career, eventually becoming a Chief Engineer at Racal and much later a Fellow of the IET. My work at Vodafone further expanded my interests in mobile and wireless communications and it was the SIM card that started my security research interests in the ISG/SCC. The focus on communications and SIMs expanded and evolved into payment cards, then passports and IDs, RFIDs, transport ticketing, NFC phones and generic attack-resistant hardware and implementation security in systems. As I answer this question I am distracted by flashing LEDs on electronics for securing power grid measurements, my current work in conjunction with colleagues at Imperial under the CyberASAP programme.

What is the rationale behind the transition to emeritus status?
I have numerous personal reasons, but after nearly two decades as an RHUL employee I feel overdue for a new chapter in my life. As an emeritus I can stay close to RHUL and dip into those activities that I consider interesting and rewarding, without being worn down by workload, and have more freedom to explore other life interests while I am still fit and able to do so.

What would you like to regard as your legacy?
I will always be proud of the SCC and its longevity, but more recently I am very pleased with my work in establishing the Digital Research Catalyst and its community of academics. I am particularly excited that the College accepted my proposal to create the Omnidrome drone and robotics centre, and I am really keen to see how it will develop. Some of my work relating to eSIMs ended up in ETSI and 3GPP standards, and I would hope that my modest contribution to the deployment of billions of eSIMS is some kind of legacy. Having said all that, my most significant legacy is probably the collective achievements of the students that I helped to educate.

What are your plans going forward?
For 2022 I agreed to continue my support for INCS-CoE, and the All Party Parliamentary Group in Cyber Security and to participate in the Digital Catalyst; beyond that I have no grand plans as yet. I could do some work through my private company, but perhaps paid work is over-rated! I have recently got into running so I will have more time for training and events, and during Covid I became a transport volunteer and can be seen driving my town’s minibus. As serendipity did a good job getting me into the ISG, I will give it a chance to define the next chapter of my life.

Can running teach us anything about life?
You can only achieve your maximum potential if you can get used to feeling uncomfortable.

THE CISO AS SOOTHSAYER

Joe Da Silva

> PHD Student, ISG

Many organisations employ a Chief Information Security Officer (CISO) to lead their cyber-security programmes. CISOs perform an important, challenging, and yet poorly understood and ill-defined role, and my research seeks to understand its purpose, both expressed and unexpressed. One of my central findings is that the role of the CISO is very much akin to that of a modern-day soothsayer, which I explore in a recent paper [1]. In this article, I briefly highlight some of these aspects.

First, I would like to clarify that soothsaying should not be seen in a negative light. The concept acts as a useful rhetorical device that brings to light the difficult and conflicting position that CISOs occupy. Soothsayers or oracles were historically highly valued, being consulted for motives of politics and warfare, often acting as 'prophet-consultant' [2], [3]. In more modern times, 'futurists' have been employed to predict military threats, which include those related to cyber security. A futurist's predictions may be taken seriously, even when based on their own works of fiction [4]. But how is this relevant to modern business?

In my study of 18 UK-based, but predominantly multinational commercial businesses, I identified that CISOs were relied upon to provide protection for those organisations from opaque, fearful threats that were difficult to understand, even mystical in nature. The impacts from those threats were considerable, with these businesses fearing for their continued existence as a result. They desired both interpretation and prediction of those threats to gain a sense of comfort that they would remain viable.

Cyber security was positioned as an expert system, comprising technical aspects, e.g. software vulnerabilities that could not be taken at face-value; they needed to be deciphered in order for any associated risks to be related to the organisation. The CISOs themselves were positioned as being necessary, with an implication that, without their role (or perhaps without them specifically), their organisations may under- or over-react to a threat. Without a CISO, an organisation's leaders may look at d ata – i.e. signs – and make their own, inaccurate, interpretations. Such judgement based on signs is analogous to soothsaying practices of divination, an interpretive practice performed by specialists that was also alluded to by senior leaders in my study, who suggested that the capabilities of their CISOs went beyond knowledge, with an intangible, almost uncanny, sense for the subject.

As well as providing assuagement, and 'protection', CISOs also performed a semiotic function, acting as a totem. Both historically and in myth, soothsayers were deployed totemically in situations of warfare. This is particularly relevant to cyber security, given the many militaristic references that are common in cyber-security discourse. These organisations felt that they were under attack, but, crucially, their adversaries were ephemeral and pervasive and their methods arcane and mysterious. In such a situation, an advantage would be gained by going 'into battle' with someone on one's side that can advise on those aspects that are not well understood, and also demonstrate to anyone observing the warring party that it is defended against such threats.

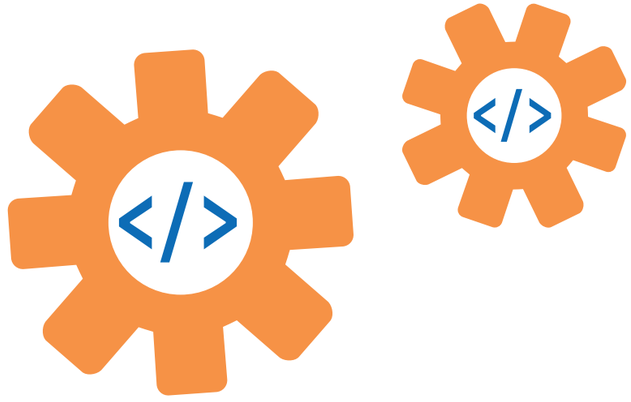
These narratives offer a number of benefits to CISOs and the cyber-security industry, but also to wider power structures, which I discuss in more detail elsewhere [5]. There is, therefore, a motivation to maintain such narratives, which may motivate 'cyber sophistry'. The CISO-as-soothsayer may have a self-interest in the realisation of their prophecies, which may motivate unscrupulous behaviour, and yet which could be a factor of the jeopardous position that CISOs are in, who, as with soothsayers, are often scapegoated.

The CISO-as-soothsayer concept has a number of implications. First, the role of the CISO becomes one of advising on the level of risk, at least at the most senior levels of the organisation. Rather than being a role of 'securing' – or indeed 'policing' – an organisation, it is a role more akin to weather forecasting. Second, managers and practitioners should be conscious of the potential for cyber-sophistry and the unhelpful outcomes that can result. Third, cyber-security education should either aim to demystify the subject, or, alternatively, to acknowledge the mysticism and thus reinforce the need for specialist interpretation. Adopting the latter approach may result in staff being instructed in the use of systems in a secure way, with the security aspects of this being implicit rather than explicit, and certain decisions on acceptability of risk being deferred to cyber-security specialists. This is, however, potentially problematic if it results in end users feeling less responsible for security and depending entirely on technological protections, becoming themselves powerless in the process. Fourth, regardless of whether cyber security is a dark art or not, perhaps systems should be designed on the basis that their security will need to be interpreted by a specialist. Often specialist parts for domestic goods have a separate 'information for installer' section. Employing this analogy, an 'information for CISO' section could be provided by system designers.

I argue that there is value in acknowledging the interpretive nature of cyber-security practice and reclaiming soothsaying as a beneficial advisory profession, rather than seeing the term in a negative light. The soothsayer is one of many identities that CISOs occupy, and my research continues to explore the multiple and conflicted nature of this position. By combining analytical lenses from a number of disciplines, including sociology, international relations and management theory, I hope to achieve a greater understanding of the purpose behind such a varied, misunderstood and important role.

[1] J. Da Silva and R. B. Jensen, "Cyber security is a dark art': The CISO as soothsayer," ACM Conference On Computer-Supported Cooperative Work And Social Computing (CSCW), Feb. 2022.
[2] N. M. Underberg, "Soothsayer (Diviner, Oracle, Etc.): Motif D1712," in Archetypes and Motifs in Folklore and Literature: A Handbook, Routledge, 2017, pp. 147–153.
[3] H. S. Daemmrich and I. Daemmrich, Themes & Motifs in Western Literature: A Handbook. Francke, 1987. [Online]. Available: https://books.google.co.uk/books?id=hIZZAAAAMAAJ
[4] D. Nissenbaum, "Author Warns U.S. Military to Focus on China," Wall Street Journal, Jun. 29, 2015. Accessed: Dec. 16, 2020. [Online]. Available: https://www.wsj.com/articles/author-warns-u-s-military-to-focus-on-china-1435539010
[5] J. Da Silva, "Cyber security and the Leviathan," Computers & Security, vol. 116, p. 102674, May 2022, doi: 10.1016/j.cose.2022.102674.

One CISO remarked that "it's implicit with our role, if something goes wrong . . . you're the guy [that gets fired]".



AUTOMATIC CLIENT UPDATE FOR EVOLVING LIBRARIES

Santanu Dash

> Lecturer, ISG

Software development relies on a community effort. Software developers frequently offload tasks to libraries maintained by third parties. These libraries evolve independently, supporting a diversity of clients, and there is thus a need to update clients to keep up with the libraries.

Updating clients for evolving libraries, however, can be challenging. Popular libraries are fast-moving and increase in size rapidly. A study of 11 versions of the Android Operating System showed that Android's interface grew ten-fold over a decade [3]. Due to the cognitive load of keeping up with large libraries and a lack of resources, developers tend to defer updating their code.

Library Evolution

Services offered by a library can be accessed through its interface, made up of a collection of methods commonly referred to as an Application Programming Interface (API). As libraries evolve, APIs are added or removed from its interface. Removal of APIs has an implication on the functionality of clients who use it, and so libraries follow a two-step process for API removal, commonly known as the Deprecate-Remove cycle.

In the first stage of the Deprecate-Remove cycle, an API is marked for removal but continues to exist in the library. At this stage, library developers leave notes about the removal schedule for the API in the documentation for the method. Often, they also recommend a replacement API that should be used. If client software is not updated to use replacements for the API, the client becomes obsolete once the API is retired.

The expectation is that developers will update clients to keep up with API changes. Unfortunately, despite clear directives in the documentation of libraries on how client software should be updated, developers tend to defer updating clients as they struggle to keep up with rapidly evolving libraries. A study of 1.2M Android apps showed that 85.6% used older versions of libraries and, alarmingly, 16K apps used libraries with known vulnerabilities [1].

Auto-updating Software

To build large software systems and maintain them, we need tooling that can help developers update their code to use newer versions of libraries. These tools need to understand update directives in software documentation and, subsequently, drive automatic program transformation aimed at updating client software. However, there are significant challenges that must be overcome before this can be achieved. We discuss some of them below.

Mixed-Text Analysis

Upgrade directives contain a mix of code and natural language. We need to analyse this mixed text to identify replacements for deprecated APIs. Recent advances in mixed-text processing make it possible to try to parse upgrade directives. These approaches combine formal grammar of programming languages with Natural Language Processing to distinguish code tokens from text [4]. While this is promising, merely distinguishing code from text is not enough to identify replacement APIs from upgrade directives. We need new forms of analysis to establish relationships between deprecated APIs and their replacements from the upgrade directives. A map from deprecated to replacement APIs can guide software transformation tools to rewrite clients to use replacement APIs.

Identifying Potentially Correct Transformations

Software transformation tools require a list of locations which should be edited or transformed. Through Mixed-Text Analysis, we know which APIs need to be changed and identifying edit locations in the code is straightforward. However, the set of potentially correct transformations may increase exponentially, especially if the type-signature of the replacement API is different to the deprecated one. If type-signatures of the deprecated and replacement API diverge, the client can be rewritten in many ways while preserving its properties or semantics. Therefore, the speed at which we identity and triage potentially correct transformations is crucial for the success of automatic software update.

Establishing Correctness of the Transformation

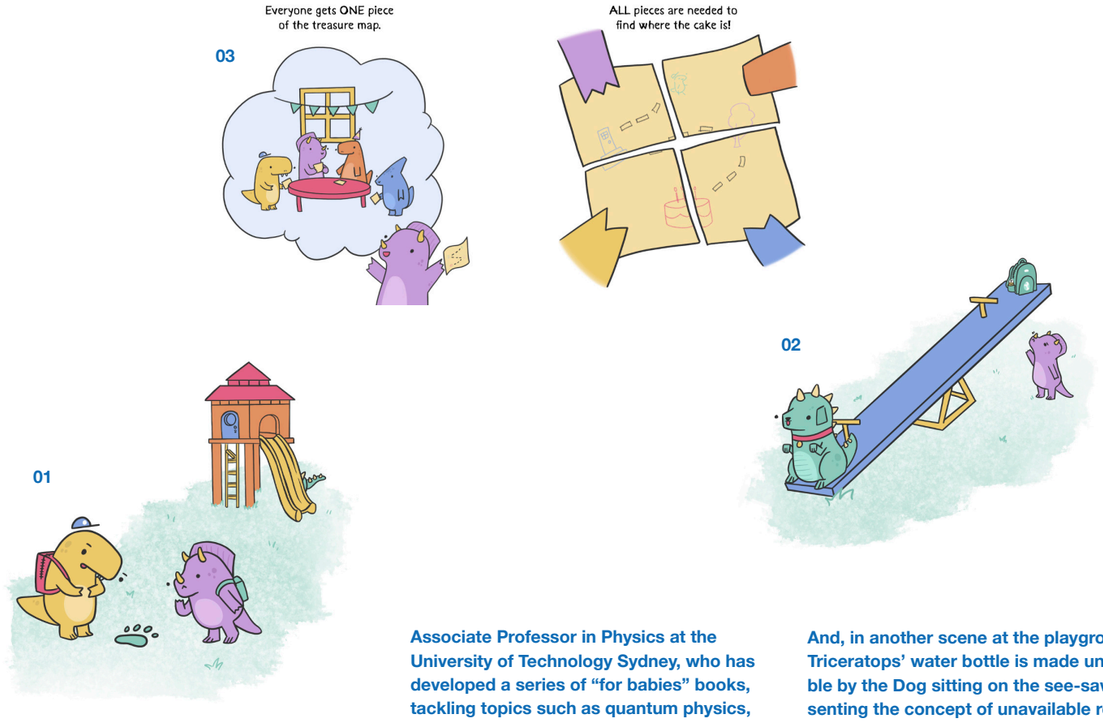
For automatic client update to become acceptable as a tool to developers, we need to minimise the number of incorrect transformations. To rule out incorrect transformations, we need a test for semantic equivalence to establish whether the software has the same properties (or to be precise, semantics) pre- and post-transformation. Semantic equivalence is hard and computationally expensive to establish. Therefore, recent advances in program transformation use the existing test suite as specifications and check whether the transformed program passes the original test suite [2]. Indeed, this equivalence check is dependent on the completeness of the test suite and, wherever possible, additional directed tests need to be written and used on both versions of the software to establish weak semantic equivalence.

Software Update Research at ISG

The long-term health of a software system depends on how often it is updated and whether it moves in lockstep with other independently-evolving pieces of software it relies on. We are starting to look at Software Sustainability as a research theme at the Information Security Group. I am leading this work as part of a recently announced 3-year EPSRC grant titled MUSE: Multi-Modal Software Evolution (EP/W015927/1), which will start in October 2022. We remain open to collaborations and would be delighted to share details about the project with interested parties.

References

[1] E. Derr, S. Bugiel, S. Fahl, Y. Acar and M. Backes. Keep me Updated: An Empirical Study of Third-Party Library Updatability on Android. In Proc ACM CCS, 2017.
[2] C. L. Goues, M. Pradel and A. Roychoudhury. Automated program repair. Communications of the ACM, 62(12), 2019.
[3] D. He, L. Li, L. Wang, H. Zheng, G. Li and J. Xue. Understanding and detecting evolution-induced compatibility issues in Android apps. In Proc ASE, 2018.
[4] P.-P. Pârţachi, S. K. Dash, C. Treude and E. T. Barr. POSIT: Simultaneously Tagging Natural and Programming Languages. In Proc ICSE, 2020.



LEARNING TOGETHER: CYBERSECURITY FOR TODDLERS

Dr. Elizabeth A. Quaglia

> Senior Lecturer, ISG

Inspired by my recent time on maternity leave, I was drawn to a call for proposal to develop resources around CyBOK v1.1 (https://www.cybok.org/), and I was successful in obtaining the funding to design two small books for toddlers, on the topic of cybersecurity and cryptography. My motivation was that, even though education happens at all stages in life, there is general consensus that early childhood education is key in laying the foundations for lifelong learning, and I wanted to try to explore this.

My goal was to develop material for short, illustrated books, whose imagery and simple text would convey in an intuitive way the basic principles and notions in cyber security in general, and cryptography in particular. The idea for this project takes inspiration from the successful children's books by Chris Ferrie (https://csferrie.com/), Associate Professor in Physics at the University of Technology Sydney, who has developed a series of "for babies" books, tackling topics such as quantum physics, quantum computing and Bayesian probability in an accessible and pleasantly visual way. We, that is the advisory team for this project (Dr. Jorge Blasco Alis and Dr. Jassim Happa) and I, believe cyber security lends itself very well to this type of approach, and that describing its fundamental concepts by illustration and simple words will be an effective way to gently introduce and raise awareness of this important topic.

The experience of developing the material for the books was challenging, but wonderful. I worked very closely with psychologist Dr. Valentina Zambon, who specialises in child and family therapy and in specific learning disorders. Valentina had a great impact on the style of writing, suggesting ways to make the text in the books more accessible and appropriate for toddlers, for instance by introducing lots of questions.

The two books (Learning Together: Cybersecurity for Toddlers and Learning Together: Cryptography for Toddlers) follow T-Rex, Triceratops and their friends in their day while at the playground and while preparing a surprise birthday party, as the Dog tries to do something they are not supposed to do (enter the playground, eat the cake, …).

The characters, colours and design are born from the creativity of designer Alex Thompson, who illustrated both books. As a taster, in the first image (01) we see the dinosaurs detecting the intrusion of the Dog in the playground by noticing pawprints in the mud.

And, in another scene at the playground (02), Triceratops' water bottle is made unreachable by the Dog sitting on the see-saw, representing the concept of unavailable resource.

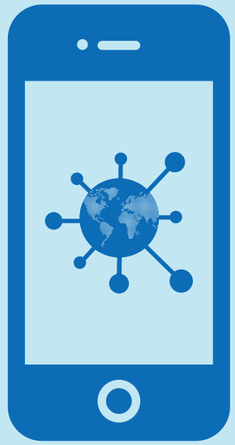
We also explore cryptographic concepts such as secret sharing through the imagery of a treasure map detailing the location of the treasure, which in our case is the birthday cake! (03)

The benefits of developing this project include reaching a new and diverse audience, namely toddlers as well as grown-ups in their care-sphere. Indeed, since toddlers will generally need the support of an adult during reading activities, our books are also intended for the wider audience of parents and family, carers and child care providers, who will be exposed to the books' contents as well.

To support the grown-ups in their learning journey, we equip the books with a glossary of technical terminology, which helps relate the scenarios in the books to technical concepts, and we provide links to additional resources from CyBOK (including webinars, podcasts and online courses).

Our hope is to provide an opportunity for children and adults to learn together about the advanced and very relevant topics of cyber security and cryptography.

The two books were presented at the Ashmolean Museum in Oxford in March 2022, during the CyBOK Showcase Event. If you wish to read these books, they will be available on the CyBOK website in pdf form. And if you would like to support the dissemination of the books, please reach out! In the meantime, enjoy the reading.



CDT UPDATE

Keith Martin

> Prof. ISG & Director of the CDT

The EPSRC Centre for Doctoral Training (CDT) in Cyber Security for the Everyday at Royal Holloway provides scholarships for around ten PhD students each year, supporting them for one year of intensive cyber security training and three years of research. The CDT aims to bring together researchers from a range of different backgrounds, supporting both single and multidisciplinary projects.

It's pertinent that our CDT is named Cyber Security for the Everyday since it's that very notion of 'everyday' that has changed so much since this iteration of the CDT commenced in September 2019. Just like everyone else, researchers are getting used to a hybrid world of home working, occasional office visits and meetings where some people are in a room and others are on a screen. I suspect elements of that are not going to go away anytime soon.

One aspect of research that has dramatically changed is travel. Our CDT has a generous travel allowance and prior to the pandemic our PhD researchers were very often on the move, attending workshops, conferences and visits all around the world. This can be an invigorating experience for those on a PhD research apprenticeship, with such events providing opportunities to build personal networks and reputation.

I have to confess that for a while prior to the pandemic I had been getting increasingly concerned about this wandering lifestyle. It struck me that so much academic travel was unnecessary. It had become a habit rather than a need. In an age where information is so digitally accessible, was it really necessary for an international research roadshow to be in place? Don't get me wrong - I do think it is good to travel and to meet people, but I think far too much of it was going on.

Well – that's certainly changed! The pandemic has shaken research travel culture to the core. It's never been easier and cheaper to attend an international conference in the new world of online delivery. In this sense, our PhD researchers have never had it so good. However, I also believe that they are missing out, particularly on international network building – it's hard to do that online. What I fervently hope is that a saner academic research culture will emerge, with more selective and valuable opportunities to travel, rather than the mass movements of the past.

With this in mind, I was particularly pleased to learn that three CDT researchers were among the winning entries in Royal Holloway's internal COP26 competition inviting students to submit a creative response to climate change and related issues of sustainability. Students were asked to consider climate change and the impact that it is having, and will have, both in terms of the global context and at a more local level. Oliver Bock-Brown, Cherry Jackson and Rebecca Hartley all submitted extremely thoughtful responses. It pleased me to see a new generation of researchers in training who may help to develop a more responsible research culture. But it also delighted me to see how the CDT, which is not focused on an area directly targeting climate change, supports researchers who are so creatively able to voice their opinions on issues beyond their core area of study. This is exactly the breadth and maturity that we hope for from our CDT researchers.

Another event which didn't happen in the manner of the past was what was previously termed our annual CDT Showcase. Before the pandemic, we held an outward-facing event where the CDT research was presented to external stakeholders. In November, partly due to pandemic restrictions and partly due to a need to reconnect with ourselves, we held an internal residential event at nearby Cumberland Lodge just for members of the CDT. It was a wonderful two days and a reminder of everything good that is happening – without the need for anyone to get on a plane!

One of the highlights of Cumberland Lodge was an impressive team presentation by the newest cohort of students on a group project they have performed involving a technical, ethical and privacy-related analysis of a novel Apple scheme to try to detect and mitigate the use of iCloud for storage and sharing of illicit child-related images. The nine students in this cohort have backgrounds that include Archaeology and Anthropology, Behavioural Science, Computer Science, History and Politics, and Mathematics. The quality of this presentation and the accompanying report are testament to the effective way in which the CDT brings together researchers from different backgrounds and allows them to grow their knowledge of cyber security in the first year, sharing their different perspectives and knowledge.

Of course, we do still want to share what we are doing with everyone. I thoroughly recommend checking our CDT Blog, which contains a range of short articles about what's been going on, internship reports, links to publications, as well as a chance to see Oliver, Cherry and Rebecca's winning entries in the COP26 Competition. We are always keen to discuss projects, internships, or opportunities to support our training year in different ways, so please do get in touch.

A NEW DIRECTION FOR MASTERS EDUCATION IN THE ISG

Peter Komisarczuk

> Professor ISG

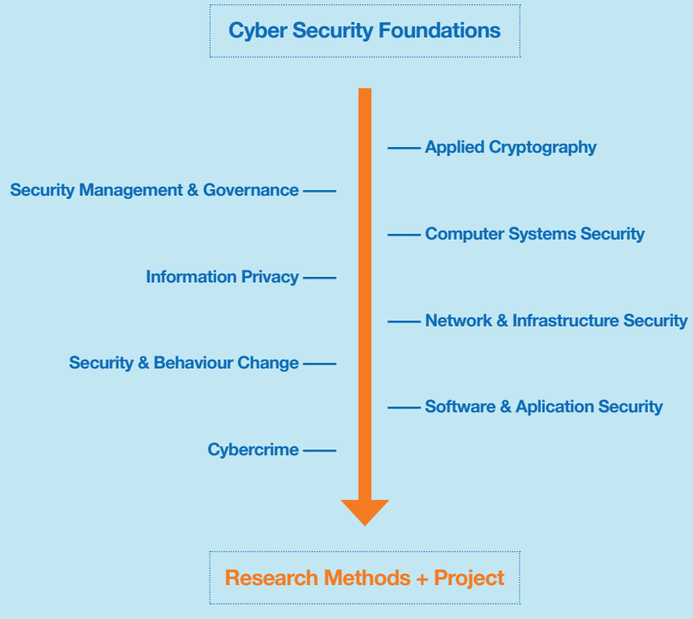
2022 sees the first major change to the shape of our masters degree offerings for many years. In October our first cohort of distance learning students will begin our new Masters in Cyber Security delivered through a partnership with the University of London Worldwide (UoLW) and with Coursera. Our current distance learning degree, which is offered through UoLW, will be phased out over a period of five years and where possible current students will be encouraged to move to the new programme.

The new degree opportunity allowed us to change the structure and flavour of the distance learning degree, and to engage more widely with the Cyber Security Body of Knowledge (www.cybok.org). Through the collaboration with our partners UoLW and Coursera, we are engaging with developments in the globalisation of education and taking advantage of the latest features in mass delivery education platforms.

This has allowed us to restructure the degree in terms of modules and content to meet some of the changes we are seeing in the student demographic and employer's needs. The restructure allows us to offer PGCert, PGDip and MSc programme variants, two entry points in the year, and new MOOCs, all at a new competitive price point including differential pricing. The degree is currently in development and will be rolling out from October 2022 – we look forward to the Programme Director and administrator joining the team in the early summer. The new degree has a single foundations module and 8 other taught modules plus a research methods module which leads into the project. The nine taught modules are each worth 15 credits (rather than the current 20-credit structure) and the individual project is in two parts: it starts with the research methods module in which the student selects a project topic, creates a project plan and undertakes a preliminary literature search, before finishing their project in a 30 credit finale.

The new delivery platform for the degree is the global online e-learning infrastructure provided by Coursera, which is the market leader and has a focus on professional training. Coursera delivery provides a full suite of multimedia opportunities and third-party tools. We are rising to the challenge of creating new videos and content, including some hand-on lab work, delivered through Coursera Labs which allows coursework and projects to be delivered through the browser as well as through other Learning Tool Interoperability (LTI) options.

For more information see the course details on UoLW and Coursera.



THE ISG SMART CARD AND IOT SECURITY CENTRE (SCC)

Konstantinos Markantonakis, Darren Hurley-Smith, Carlton Shepherd

> Director, ISG, SCC
> Lecturer, ISG, SCC
> Senior Research Fellow, ISG, SCC

The Smart Card and IoT Security Centre is spearheading the ISG's effort in commercialisation, impact and student engagement activities. In 2021, we celebrated several achievements resulting from our challenge-led research activities. Our first project, Seclea, led by Dr Raja Naeem Akram (now Senior Lecturer at the University of Aberdeen) is now a fully-fledged company with several employees. Seclea, which offers a new platform to de-risk the adoption of artificial intelligence algorithms, has received substantial funding from private investors, including Europe's largest venture capital fund and Innovate UK. The second project, PrineSec, a year three project of Innovate UK's competitive CyberASAP programme, generates real-time analysis of an organisation's security and privacy compliance using causality chains and is now being applied to IoT security analysis. Our most recent endeavour, Tensorcrypt, led by Dr Carlton Shepherd, enables organisations to securely share and analyse sensitive datasets using confidential computing. Tensorcrypt was also a CyberASAP project (2021/22), winning grant funding of over £73,000 from Innovate UK. A patent application has been filed and a proof-of-concept was successfully developed, which provided employment to three talented Royal Holloway undergraduates. The whole journey is a great example of success stories being built from academic excellence and entrepreneurship.

The SCC would like to thank Prof Keith Mayes, the founding director of the Smart Card Centre, for all his support for, and contribution to, the SCC. He has been an inspiring leader and valuable colleague. I never forget when we first joined the ISG back in 2002 and we shared an office in the Orchard building having nothing more than two desks our chairs and our laptops. Through hard work and dedication, the Smart Card Centre strengthened its activities, which are still in full operation 20 years later. We would like to wish him all the very best for his retirement and his transition to a Royal Holloway Emeritus Professor. We also look forward collaborating with him in the Digital Catalyst and Omnidrome activities. Thank you, Keith!

Over the last 12 months the SCC has published several papers on drones/unmanned aerial vehicles (UAVs) and mobile systems security. Vihangi Vagal, a former MSc Information Security student (now at Deloitte), completed her masters project with the SCC on UAV geofencing techniques in complex dynamic scenarios. The work was presented at the 40th IEEE/AIAA Digital Avionics Systems Conference (DASC)---one of the leading events in the area---winning a best paper award to boot [1]. Congratulations, Vihangi!

Dr Carlton Shepherd led the publication of the first comprehensive analysis of physical fault injection and side-channel attacks on mobile devices [2]. This was a collaborative effort within the EU Horizon 2020 EXFILES consortium, which unites law enforcement agencies, universities, and the private sector towards developing new mobile forensics methods. The research critically examines existing approaches that often contain unrealistic practical assumptions and offers several recommendations for future research. Furthermore, Carlton led research on new side-channel attacks on mobile devices, exposing design-level operating system vulnerabilities within the Android sensor stack that affect all Android devices worldwide. The results were responsibly disclosed to Google, who are deploying a fix in a forthcoming major Android release. A paper is under review at a leading security venue.

Carlton and Konstantinos have agreed with Springer to author the first book on trusted execution environments (TEEs). Such technologies have exploded in popularity for securing applications, e.g. biometrics and digital rights management (DRM) systems, using hardware-assisted separation. The book, due to be published in 2023, will explore the security properties and lineage of various TEEs, from multi-application smart cards to modern systems such as ARM TrustZone and Intel SGX, and future technologies.

Benjamin Semal, our PhD student, recently passed his PhD viva subject to minor corrections. His thesis examines the threats posed by microarchitectural covert channels in multi-tenant computing environments. Benjamin proposed a new framework for evaluating and scoring new threats and developed two new covert channel methods using CPU memory controllers. The first method enables privileged adversaries to leak information between two processes within a single native environment [4]. The second extends this to cross-VM scenarios for unprivileged adversaries [5]. The attacks resulted in responsible disclosure engagements with Intel, AMD, and Amazon Web Services (AWS).

The focus on challenge-led research has driven the acquisition of new equipment to drive multi-disciplinary research between the ISG, Computer Science, Life Sciences, and Geography departments. The existing fleet of affordable, consumer-grade drones is currently being used for research into sensor fraud, digital forensics, and exploring resilient channel security for swarms of unmanned vehicles. Industry-grade surveying platforms, such as the Matrice 300 RTK, will enable novel research into pressing security challenges around identifying, reporting, and safeguarding endangered and new species of flora and fauna. Extending these resources is a comprehensive suite of mobile prototyping and RISC-V development platforms for supporting educational efforts and proof-of-concept attacks and mitigation methods within next-generation cloud infrastructures.

The SCC continues to pursue Horizon and EPSRC grants. ZELDA is a Horizon proposal focusing on the development of novel, trustless network architectures to facilitate decision making using data from heterogeneous mobile and IoT devices. It aims to address significant privacy issues and auditing challenges regarding the transport and processing of information, focusing on privacy-preservation and data minimization. CHAINFRAIN is an EPSRC open-call proposal, focusing on road freight and theft prevention in that domain. A key challenge that will be addressed is the transport and processing of confidential vehicular and cargo data across European borders.
We hope that this short overview of our recent activities will excite interest. Please do contact us at scc@rhul.ac.uk if you feel there are areas that we could explore further together.

References
1. V. Vagal, K. Markantonakis and C. Shepherd, "A New Approach to Complex Dynamic Geofencing for Unmanned Aerial Vehicles," 40th IEEE/AIAA DASC, 2021.
2. C. Shepherd, K. Markantonakis, N. van Heijningen, D. Aboulkassimi, C. Gaine, T. Heckmann and D. Naccache, "Physical Fault Injection and Side-Channel Attacks on Mobile Devices: A Comprehensive Analysis," Computers & Security, 2021.
3. C. Shepherd, B. Semal and K. Markantonakis, "A Side-channel Analysis of Sensor Multiplexing for Covert Channels and Application Fingerprinting on Mobile Devices," arXiv preprint arXiv:2110.06363, 2022. https://arxiv.org/pdf/2110.06363.pdf
4. B. Semal and K. Markantonakis, K. Mayes, J Kalbantner, "One Covert Channel to Rule Them All: A Practical Approach to Data Exfiltration in the Cloud," 19th IEEE TrustCom, 2020. https://doi.org/10.1109/TrustCom50675.2020.00053
5. B. Semal and K. Markantonakis, R, Akram, J Kalbantner, "A Study on Microarchitectural Covert Channel Vulnerabilities in Infrastructure-as-a-Service," 2nd Cloud S&P Workshop, 2020. https://doi.org/10.1007/978-3-030-61638-0_20

INTERDISCIPLINARY EXPLORATION WITH THE CRITICAL SECURITY READING GROUP

Lizzie Coles-Kemp, Nick Robinson & Ian Slesinger

> Prof. ISG
> Postdoctoral Research Assistant, ISG
> Postdoctoral Research Assistant, ISG

The Critical Security Reading Group (CSRG) is a bi-weekly online reading group based within the ISG, and is organised by three members of the ISG: Lizzie Coles-Kemp, Nick Robinson and Ian Slesinger. The main purpose of the group is to provide a forum for exploring a variety of themes related to the intersection between digital security, society and politics – taking an interdisciplinary approach that also stays relevant to current events, societal trends and emerging academic literature. Given the interdisciplinary nature of our discussions, our group is open to anyone who is interested in the broad area of digital security, and current participants include faculty within the ISG and in the wider RHUL community, academics in related fields from other universities, and practitioners in the private and third sectors.

Recent themes have included work on digital responsibility, data and trust/surveillance, decolonising security, anticipatory security futures, geopolitical and cyber risk, and research that intersects with issues of gender, race and accessibility. In 2020, in conjunction with the Research Institute for Sociotechnical Cyber Security, the CSRG led a national discussion about what digital responsibility is and how it is related to the security of digital technologies and services. Outside of academic research, the group has also turned its hand to critiquing security in a national security context, with one recent session focussing on the UK government's latest National Cyber Strategy 2022. We've also been incredibly fortunate to be joined by several guest authors, who have given up their time to openly discuss their research, with recent guests including Myriam Dunn Cavelty (ETH Zurich), Clare Stevens (University of Portsmouth), Daniel Woods (University of Innsbruck), Becky Kazansky (University of Amsterdam) and Julia Slupska (University of Oxford).

How did the CSRG come about? Lizzie has been working with marginalised and underserved groups for the last 14 years and from the start of her work it was clear that the security technologies that are used in essential everyday services (such as banking, welfare, housing, and employment) are not necessarily deployed to protect the users of the service, and sometimes more to protect the service from the users. For those in insecure settings, particularly those experiencing economic hardship, adversarial security controls exacerbate insecurity and can result in increased resistance to the controls designed to protect the system. This led Lizzie to formulate the following overarching research and teaching question "Under what social, economic and political conditions are security technologies able to achieve the designated security goal?" To answer such a question requires a critical evaluation of what the security goal is, who benefits from the realisation of the security goal, and what assumptions are being made about the economic, social and political conditions shaping the implementation of security technology. Together with ISG colleague Rikke Bjerg Jensen, Lizzie created a reading group to explore these questions and so the CSRG came into being.

How does the CSRG work? For each session, we ask participants to read the designated paper and to come along to the group with one or two thoughts on the paper – maybe something they enjoyed, something they disliked, or maybe something they didn't understand and would like to discuss further. After sharing these thoughts with the wider group, the baton is passed on to a colleague to share their own insights, before finally culminating in a large group discussion on the paper and the wider issues it promotes. Above all else, the CSRG is friendly, supportive and non-confrontational, allowing participants to discuss an array of ideas and issues in an open and relaxed environment.

Why do people take part? The group provides a space in which people can challenge assumptions and belief about the power of security technologies and their ability to protect. At its core the group asks the fundamental question "Under what economic, social, and political conditions do security technologies protect people?" We critically examine which people are protected and why, as well as considering which people are left vulnerable and the harms that arise as a result.

When the pandemic started, CSRG members asked that we move the reading group online and run it throughout the year. Moving the reading group online enabled the CSRG to widen its participation, invite authors of papers to join the conversation, and to maintain a consistent and steady presence throughout the academic year. With the CSRG now entering its 3rd year, we are keen to expand our audience and broaden the scope of our discussion. If you have any ideas on where our next conversation should head, or if you want to join us for our next session, please don't hesitate to reach out and join our mailing list!

For enquiries, please email Lizzie at Lizzie.Coles-Kemp@rhul.ac.uk

30

ISG MSC UPDATE

Jorge Blasco Alis

> Senior Lecturer, ISG
> Programme Director MSc

This year marks the 30-year anniversary of our MSc in Information Security. Since its inception the ISG has always aimed at offering a degree that meets the needs of the real world and prepares our students to succeed in their future careers. We have proven this commitment in several ways. Last year, both our campus and distance learning MSc degrees renewed their NCSC certifications, recognising that they 'provide well-defined and appropriate content' that is 'delivered to an appropriate standard'. This year, we went further and successfully applied to be recognised as one of the Academic Centres in Excellence in Cyber Security Education with a Gold Award. This award recognises our efforts in developing and influencing cyber security education as well as our engagement with industry, government and other educators.

Since the start of the pandemic in March 2020, we have adapted the way we teach so that we could quickly react to the evolution of the pandemic. This year we have offered a variety of ways to access our teaching, ranging from face-to-face sessions, live online streaming or our well-known block mode delivery on campus. We hope that lives can go back to normal as soon as possible but we are confident that we are prepared to deliver our high-quality teaching in a world where change is constant.

I would like to use some of my words here to thank again my colleagues and students. During the past two years our academic and administrative staff have gone to extraordinary lengths to keep our community together. Our students have answered that call demonstrating why our MSc alumni are honest and trustworthy professionals.

As usual, I would like to finish this yearly update on a positive note. Each year, the department awards the best project of the year with a special prize. This year, with two cohorts we were very happy to award them two of our students. The prizes went to Chris Underwood and Ivan Beres. Congratulations!

INSIGHTS ON SECURITY CULTURE – AN EMPIRICAL STUDY WITHIN UK UNIVERSITIES

Konstantinos Mersinas

> **Senior Lecturer, ISG**

Security culture can be defined as the totality of human aspects, including behaviours, attitudes, beliefs, knowledge and shared values, which contribute to the protection of information in an organisation (Da Veiga and Eloff, 2010; Alhogail and Mirza, 2014). Security culture is a subset of organisational culture, and although it has been extensively studied in the industry, studies within academia are less frequent. In a project funded by the National Cyber Security Centre (NCSC), we conducted 19 interviews with professional services / administrative staff, students, academics and senior management members across three Higher Education Institutions in the UK (Durojaiye, Mersinas, Watling, 2021). Our goal was to examine security culture in higher education institutions (HEIs), whether such a culture is promoted by universities, and identify the complexities of establishing a security culture within HEIs.

University users' findings

A subset of the study's key findings is presented here. First, we observe that HEIs have various cyber security related structures in place, but these are not clearly visible to users. All subjects reported that they know someone to contact in case of a security incident. Most interviewees identified the IT helpdesk as the most appropriate point of contact. However, we found that individuals overall identify too many entities, roles and points of contact for reporting incidents. This finding might imply that devolution of IT and security services within universities does exist, but might have evolved circumstantially without centralised planning. In addition, senior management reported that cyber risk is not assessed separately from other risks; there is an understanding of what needs to be done for enhancing cyber risk governance, but strategies to achieve this goal were not observed.

Second, information exchange and communication on security-related issues between individuals and the university's 'cyber security entity' is basically unilateral, i.e., from users to the security entity. Communicated security messages are vital in nudging cyber behaviour change (Renaud and Dupuis, 2019); and members of senior management reported that their goal is that users comply with policies and adopt recommended security behaviours. However, feedback from the HEIs' side was largely absent. The importance of communication for users was also indicated in an additional survey. A principal component analysis on survey data revealed a one-item factor which accounts for 9.87% of the total variance; the item is described as 'improvements in cyber security communication from the university' (eigenvalue = 1.48).

In security culture research, attention is usually focused on security consciousness and awareness, and on user skills and confidence. It is worth mentioning that the former term is a traditional view on security, but might be misleading. Awareness, although to an extent measurable, does not necessarily imply security hygiene. It is the actual behaviour of individuals which determines the level of exposure to threats. The latter term, skills and confidence, can be approached by the so-called self-efficacy factor, a variable often used in behaviour change models (Witte, 1998). In our study, we identified factors that influence the levels of confidence. Namely, we found that perceptions of security levels depend on roles. A repeatedly emerging pattern in our content analysis is that members of staff who are involved more closely with specific processes (e.g. with exam papers) were more confident that security of the process is adequate (in this case mainly confidentiality).

The last finding can indicate that when people are involved with security processes and mechanisms, they place increased trust in these processes and their efficiency. But why is this the case? One possible explanation is transparency. For members of staff who deal with these mechanisms and processes in their daily activities, these are transparent and provide a sense of trustworthiness. Such employees are mostly administrative staff. The opposite phenomenon is observed amongst academics and students who – in general – are not involved with the underlying mechanisms and the set-up of such processes. The latter groups reported that they do not trust security mechanisms, nor are confident about security being adequate. The same groups of individuals stated that they feel they are expected to trust these mechanisms and processes, but they are not able to do so. Thus, there seems to be a relationship between perceived inadequate security levels and ignorance about security mechanisms and processes. Beyond transparency and knowledge, another possible psychological explanation could be uncertainty avoidance. Events associated with known probabilities are systematically perceived by individuals as favourable, or overestimated depending on the context, even if they are measurably sub-optimal. In contrast, people tend to consider choices as unfavourable if they involve uncertainty (Ellsberg, 1961); process ignorance reinforces uncertainty. We can also examine the angle of security ownership in explaining the role-dependence of security perceptions. For example, some employees handle personal and sensitive data, e.g. students' academic or wellbeing records. Research indicates that involvement in security processes does influence security culture in organisations, especially if this involvement implies responsibility and ownership (Alnatheer et al., 2012).

Building on insights

Building on the study's findings, a number of recommendations arise. First, it is up to university management to decide whether and how cyber risk is not assessed with regards to their risk priorities. But, it should be noted that senior management tend to prioritise different security services (e.g. availability) to other members of staff (e.g. confidentiality and integrity).

University management need to focus on cyber security strategies to achieve the 'how' for cyber risk governance. Importantly, there is a lack of feedback from the university side to users, who communicate with the university in a unilateral fashion (as in the case of reporting incidents). The design and dissemination of security and risk messages to users is also important. Our survey findings indicate students feeling significantly more comfortable engaging in risky cyber behaviours, compared to other user groups. Therefore these messages might need to be customised for target groups.

Finally, if security processes were to involve more members of staff, the outcome would be dual as security consciousness increases and people are more confident about security. Although, this does not necessarily mean adequate security levels, security responsibility and ownership could be the basis for cultivating a security culture within the university.

References

[1] Da Veiga, A. and Eloff, J.H. (2010), "A framework and assessment instrument for information security culture", Computers & Security, Vol. 29, No. 2, pp196-207.
[2] Alhogail, A. and Mirza, A. (2014), "Information security culture: A definition and a literature review", Computer Applications and Information Systems, pp. 1-7.
[3] Durojaiye, T., Mersinas, K., & Watling, D. (2021). What Influences People's View of Cyber Security Culture in Higher Education Institutions? An Empirical Study. The Sixth International Conference on Cyber-Technologies and Cyber-Systems, Barcelona, Spain.
[4] Witte, K., 1998. Fear as a motivator, fear as inhibitor: Using the EPPM to explain fear appeal successes and failures. The Handbook of Communication and Emotion.
[5] Renaud, K., & Dupuis, M. (2019). Cyber security fear appeals: unexpectedly complicated. In Proceedings of the New Security Paradigms Workshop (pp. 42-56).
[6] Ellsberg, D. (1961) "Risk, Ambiguity and the Savage Axioms", Quarterly Journal of Economics, 75 (1961), 643-669.
[7] Alnatheer, M., Chan, T. and Nelson, K. (2012), Understanding and Measuring Information Security Culture, Pacific Asia Conference on Information Systems, pp. 144.

STAFF PROFILE SAQIB A. KAKVI

How did you become interested in Computer Science?

Computers have permeated every aspect of my life, and growing up around them sparked my interest in computer science at a young age. My father, who worked in IT, was genuinely enthusiastic about mentoring me, which fuelled my passion. He aroused my curiosity and taught me to think critically and out of the box. Then, through compelling storytelling, practical demonstration and profound observation, he devised new solutions and coached me through the process. I have fond and unforgettable memories of spending hours playing with the Commodore 64 with my father as a kid. I felt a true sense of belonging with computers and it further developed over time.

Even at school, I would frequently spend my holidays in the computer labs, assisting the IT staff with routine maintenance. So, when I read the books "Window 95 for Dummies" and "Internet for Dummies" and realised I already knew everything, it was a watershed moment. This further ignited my desire to pursue a career in informatics and computers.

How did you become interested in Information Security?

My father was also my first contact with information security. He had (and still has) a small red folder with descriptions of all the known viruses at the time. It was a stack of 20 A5 sheets containing all available information on a single virus. Reading about attack pathways, mitigation measures, and recovery strategies piqued my interest. These thoughts stayed in my head, and I was eventually determined that not only would I study Computer Science, but I would also study security. I'm not sure when it started, but I've always visualised a future in information security. This decision was reinforced in the final year of my undergraduate studies, where I took an elective module in Information Security. This module is where I first learnt about modern cryptography, and the subject instantly captivated me.

Tell us about your research

"You have one foot in the past, and one foot in the future," one of my colleagues once said of my research. Even though he said it jokingly, it perfectly sums up my study. My research career began with the goal of proving, or rather, improving the security of older digital signature techniques that are still in use today. Recently, I've been concentrating on standardised signatures and attempting to demonstrate that they are secure and that my proofs are optimal. This section of my research deals with the "past." On the other hand, in terms of the "future," I'm working on new cryptographic techniques that use emerging technologies. For example, I'm now working on Witness Encryption and its sequel Smart Encryption, which are (relatively) new primitives.

In both cases, I enjoy going off on tangents and working on seemingly unrelated primitives that help me achieve my primary goals in unexpected ways.

Your research secures schemes from the past, so was everything insecure until now?

"No, everything was secure," is the quick answer (at least in most situations). There was great thought given to the design and development of these schemes when they were suggested, and while there have been some setbacks, most of them are still standing. Therefore, we were confident that they were secure because they had stood the test of time. Of course, my proofs indicate that the schemes (or at least some variants) have always been secure, so our trust was not misplaced, but we now know for sure that they are secure.

On the other hand, you are looking to the future – could you elaborate on that?

We live in a dynamic world where transformation and disruption are inevitable. The digital world is evolving at breakneck speed. This means that, as Information Security practitioners, we can either foresee the future or spend time playing catch-up. While it is notoriously difficult to foretell the future, we can nevertheless forecast what will happen. I'm specifically interested in the developing technology of Smart Contracts to see what security issues can arise and how we can utilise them to create intriguing new cryptographic primitives, such as the "Smart Encryption" project I'm working on now.

How did you cope with the impact of the pandemic on university life?

I was working at a university in Germany when the pandemic profoundly disrupted our world. The transition to online-only instruction was an exciting yet challenging experience for all of us. We pooled our resources to create high-quality courses that our students truly appreciated. It opened the door to future possibilities, created opportunities and enabled us to try out new assessment methods. Our group had just relocated; to make things more interesting; we decided to split and work in two groups. The move to an online-only model filled the gaps and made us feel like we were all in the same place. Over Zoom, we even managed to throw a Christmas party! Having said that, I am looking forward to transitioning to in-person teaching and chatting with colleagues over a cup of coffee in the office.

WISDOM 2021-2022 ROUND-UP

Rachel Player &
Elizabeth Quaglia

> Lecturer, ISG
> Senior Lecturer, ISG

It's now been almost six years since the WISDOM group was founded in 2016 by former PhD students Dr Sheila Cobourne and Dr Thyla van der Merwe. WISDOM was born out of the recognised need to increase diversity in the fields of Mathematics and Information Security, and to support the women already working in these fields. WISDOM began as an initiative within the Department of Mathematics and the ISG. This year, the group has expanded to welcome members from across the EPMS School. WISDOM's efforts are coordinated by a committee of PhD students, with support from ISG staff members. The committee representatives work together to organise events, outreach efforts, and socials. The mailing list counts over 100 members, who are invited to attend events and volunteer in outreach efforts. (New WISDOM members are always welcome!)

In the early days, the WISDOM group worked hard to establish itself as a network to support and raise the profile of women working in Information Security and Mathematics at Royal Holloway. One step towards achieving this was by hosting now-traditional events such as the welcome event at the start of the first term, and the Winter Networking Event. This year, the October 2021 welcome event was very well attended, and it was great to meet new faces from across the School.

We were glad to organise another edition of Winter Networking Event in December 2021, where we heard from two speakers about their career experiences to date. In particular, Dr Elena Issoglio, from Universita degli Studi di Torino, Italy, walked us through her academic journey, and gave us a taste of her research interest in stochastic differential equations. We also had a talk from Nat M, from NCSC, who shared her experience as a mathematician in various roles, now part of a sociotechnical security group that applies a multidisciplinary approach to delivering security that works in the real world.
The speakers joined online, but we were glad to be able to see members in person to watch the talks together. After the talks, the discussions continued over coffee.

This year, we have also been glad to continue newer traditions, such as the Halloween bake off. Members brought along their spooky bakes to a lunchtime social and the entries were judged both for their taste and for their fit to the theme! This was a great opportunity for members to meet informally and try some delicious treats. We very much look forward to future WISDOM bake off socials!

Over the last couple of years, the Wisdom committee has been ably led by co-presidents Erin Hales and Tabitha Ogilvie. Both Tabby and Erin have put in significant effort to spearhead initiatives, events, and socials. They are now stepping down from their roles, and on behalf of all members, we would like to thank them for their enormous efforts in driving the group forward. Anyone who is interested in taking a more senior role in Wisdom and continuing their excellent work is invited to get in touch.

If you'd like to know more about WISDOM, follow us on social media where we share all the details of our upcoming events. We also maintain a blog where contributors share their thoughts and personal experiences on topics such as diversity and inclusion. We welcome guest contributions, so please get in touch via wisdom@rhul.ac.uk if you have something to share.

Follow WISDOM on social media:
@WisdomRhul
https://www.facebook.com/wisdomrhul/
https://www.linkedin.com/groups/12047422/

WRITING FOR PUBLICATION: AN OPPORTUNITY FOR POSTGRADUATE STUDENTS

Siaw-Lynn Ng

> Senior Lecturer, ISG

The ISG has a long tradition in cyber security research, and is one of the largest academic cyber security research groups in the world. Along with academics and research assistants, there is a large group of postgraduate research students, working on topics ranging from cryptography to cyber economics. In addition, the ISG 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 3000 graduates from more than 100 countries.

Besides writing for publications in peer-reviewed journals and conferences, we provide an opportunity to communicate new ideas and insights more informally to other security professionals. This also allows graduate and postgraduate students to improve their technical and communication skills, to establish them as an expert in their fields of study, and to influence the development of those fields. These articles are written mainly for security professionals, and give general introductions to topics of interest, or provide analysis of current issues in cyber security, without assuming that readers have an extensive mathematical or computer science background.

The main publication venue for these articles is the Computer Weekly ISG MSc Information Security thesis series. This is a series of informative leading-edge articles distilled from outstanding MSc projects which present research in areas of information security of interest to information security managers and professionals. These MSc projects are re-written in collaboration with the individual ISG project supervisors as accessible short articles for a general professional readership and published online at www.computerweekly.com.

A short description of this year's articles follows; the full articles can be found from links in https://royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/computer-weekly-search-security-awards/.

• There is a growing trend for personal investors to use new and emerging technologies to manage their finances, and investment platforms are the technology of choice. In "Protecting personal investors on UK investment platforms from cyber threats", Gerard Phillips (supervised by Geraint Price) describes a new threat model focusing on the risks to personal investors in the UK who use UK investment platforms to manage their pensions and savings. This offers new insights allowing anticipation and defence against future attacks.

• As a large proportion of the web servers on the internet run Linux or other UNIX-based operating systems, it is important to understand how well-protected they are from malicious software. To this end Giuseppe Raffa (supervised by Daniele Sgandurra) describes the evaluation of the effectiveness of some anti-virus programs for Linux desktops using local installations as well as an online malware scanning service in the article "Testing anti-virus in Linux: How effective are the solutions available for desktop computers?".

• On another aspect of information security, in "The Computer Misuse Act and the characteristics of convicted hackers", James Crawford (supervised by Rikke Bjerg Jensen) analyses the characteristics of 132 of the individuals convicted under the Computer Misuse Act between 2008 and 2018 and considers whether they conform to the stereotypes of gifted and highly skilled hackers.

Note that 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/

SOCIAL SCIENCE AND HARDWARE-BASED COMPUTER SECURITY

Ian Slesinger, Lizzie Coles-Kemp & Niki Panteli

> Postdoctoral Research Assistant, ISG
> Prof. ISG
> Prof. Digital Business

The Discribe Hub+ has been established to research the social, economic and political dimensions of a Digital Secure by Design (DSbD) approach to hardware security that starts at the chip level at the base of the stack. The Hub is part of a broader UKRI initiative tied to the Industrial Challenge Research Fund (ICRF) that links academic expertise and industry resources with UK government support. The goal of DSbD is to bring to fruition a commercially viable Instruction Set Architecture based on the Capability Hardware Enhanced RISC Instructions (CHERI) model developed by computer science researchers at Cambridge University and SRI International. The DSbD challenge has been created around Arm's Morello programme, which has been established to produce a hardware CPU demonstrator board to be shared with academic researchers, SMEs and industry partners for testing and experimental development.

Specifically, the ISG in collaboration with the School of Business and Management is leading a work package of Discribe Hub+ tasked with evaluating the standardisation, regulatory and policy implications of potential future commercial implementations of the CHERI technology. To do so we are applying qualitative social science methodology derived from the interdisciplinary field of Science and Technology Studies (STS). An STS approach enables us to examine the political, social and economic conditions that shape the DSbD proposition. CHERI's technologist proponents are making a bold technical proposition of fine-grained memory protection and memory compartmentalisation that will obviate nearly 70% of security vulnerabilities. How, to what extent and by whom can this pitch be translated into a commercially viable, ubiquitous and user-friendly product across a range of sectors and use-case scenarios? Answering this question requires investigating a wide range of social scientific phenomena. These include: examining the political economy of the relationship between the state and big players in the technology industry; geopolitical questions on the strategic role and purview of the state with regard to cybersecurity; questions of organisational structures and socio-technical networks in relation to businesses, government, and the supply chain and innovation cycle in technology manufacturing; the relationship between standards, regulation and trust in new technology; the relationship between policy interventions, regulation, ethics and how responsibility is located and attributed in the security eco-system; and finally profound philosophical questions of what would a DSbD chip actually be securing, what does 'security' mean here, and who or what are the agents and objects of security.

Evaluating the implications of how a given technology works helps us to understand possible barriers to adoption. Using STS we can apply a different set of tools from technical experts to interrogate how that technology's design or use might evolve or change in relation to the social and material environment in which it exists. This opens up creative possibilities for technological innovation at the initial stages of design and a more robust consideration of the conditions in which a technology must operate effectively through its lifecycle. It can also help explain the reasons why a particular innovative technology might face inertia in adoption and usability challenges that could derail its successful adoption.

In the case of DSbD this involves ascertaining how the interactions between designers and users in the Morello project establish the security value of the CHERI-enabled chip. This security value will determine the technology's path to market. The security value will likely be shaped by the emergent chip's usability and its potential to change the security paradigm relative to the disruption caused by the present paradigm of patching security vulnerabilities through frequent software updates at the OS and program levels of the stack. This requires us as researchers to understand and measure the extent of the social, political and economic costs of the present reliance on software patching, and to understand what the societal benefits of implementing CHERI technology would be. We must also evaluate the potential challenges and barriers to the adoption of CHERI technology across organisations, market sectors and the wider society, including those pertaining to regulation and technical standards. Additionally, we must investigate and explain the processes and mechanisms through which shared security understandings and values are created around CHERI. One way we are approaching this is by producing case studies of past innovation processes for security technologies in which socio-technical narratives played a significant role, including the adoption of Trusted Platform Modules and the X.509 standard for public key certificates.

If you would like to engage further with the ISG's work on Discribe Hub+ please contact Ian at ian.slesinger@rhul.ac.uk. More information about the wider DSbD challenge is available at https://www.dsbd.tech, while the Discribe Hub + website https://www.discribehub.org.

https://msrc-blog.microsoft.com/2022/01/20/an_armful_of_cheris/

MACHINE LEARNING RISK MANAGEMENT AND REGULATORY COMPLIANCE

Raja Naeem Akram
Konstantinos Markantonakis

> CEO & Co-Founder Seclea
> Professor & Director of the ISG SCC

Machine learning is transforming the world, from healthcare services, manufacturing, financial services, and scientific discovery to cybersecurity. The major driving force for machine learning adoption is the increase in productivity. According to some estimates, by 2030, all aspects of technology, from cyber to physical, will have some component based on machine learning algorithms.

Machine learning, or Artificial Intelligence (AI), has significant benefits for the commercial sector and society. However, this relentless pursuit of building AI solutions for every problem, along with organisations trying to gain a competitive edge, should be counterbalanced with caution. AI has its benefits, but they come with significant risks. In their 2019 annual reports filed with Securities and Exchange Commission, Google and Microsoft have added warnings to their "risk factors" for investors relating to potential legal and ethical problems from their AI projects. The risks posed by AI include traceability, bias, privacy, transparency, security, and accountability, as described below:

• Traceability: Tracking the actions taken by humans or machines during the lifecycle of an AI application;

• Bias: Discrimination arising from the choice of training data, design decisions and training evolution;

• Privacy: Data sourcing and use of data by the AI algorithm might violate data privacy requirements;

• Transparency: Explanation of the behaviour and decisions of advanced AI algorithms;

• Security: Ensuring AI is safe and protected at all lifecycle stages;

• Accountability: Ability to audit an AI algorithm and its decisions to identify the root cause of an issue.

Regulatory authorities and standardisation bodies have proposed regulations, standards, and guidelines for developing and adopting AI solutions that have four things in common: fairness, traceability, transparency, and accountability. Most of the regulations and policies have taken a risk-based approach. If your AI application poses risks to individuals and society, it must abide by the relevant rules and standards.

According to the proposed EU's Artificial Intelligence Act (AIA) [1], any applications that pose high risk must ensure that they are compliant with AIA. Failure to do so has a higher penalty than GDPR non-compliance – with fines rising to €30 million, or 6% of global revenue. AIA defined high-risk applications as "… AI systems that are creating an adverse impact on people's safety or their fundamental rights are considered high-risk. To ensure trust and consistent high level of safety and fundamental rights protection, a range of mandatory requirements (including a conformity assessment) would apply to all high-risks systems."

Cybersecurity controls, especially automatic incident detection and response, intrusion detection and response, and firewalls, are listed in the AIA. A simple rule of thumb to identify whether your cybersecurity application falls under the high-risk definition of AIA is to determine what information it uses and who gets affected by its decisions. If the data used during training or deployment relates to humans, or AI decisions might affect humans or their ability to perform a task then your application is most probably a high-risk AI application. Even if your application cannot be clearly defined as a high-risk or low-risk application, the recommendation of EU-AIA is to aim for compliance, thereby safeguarding your AI investment and minimising any potential future compliance issues.

To de-risk AI development and adoption, it is necessary to start by defining, managing and monitoring a robust Governance, Risk Management and Compliance (GRC) strategy. Organisations are typically well-experienced in GRC practices for their business and IT functions. However, treating AI as just another IT element is not recommended. AI requires contributions and oversight from diverse segments of an organisation and people with varied backgrounds and experiences. For example, AI has contributed to an increase in the demand for ethical expertise to ensure AI is developed and used ethically. Similarly, from a technology perspective, AI development and operations are different to standard software development, and so AI GRC requires a different strategy and tools.

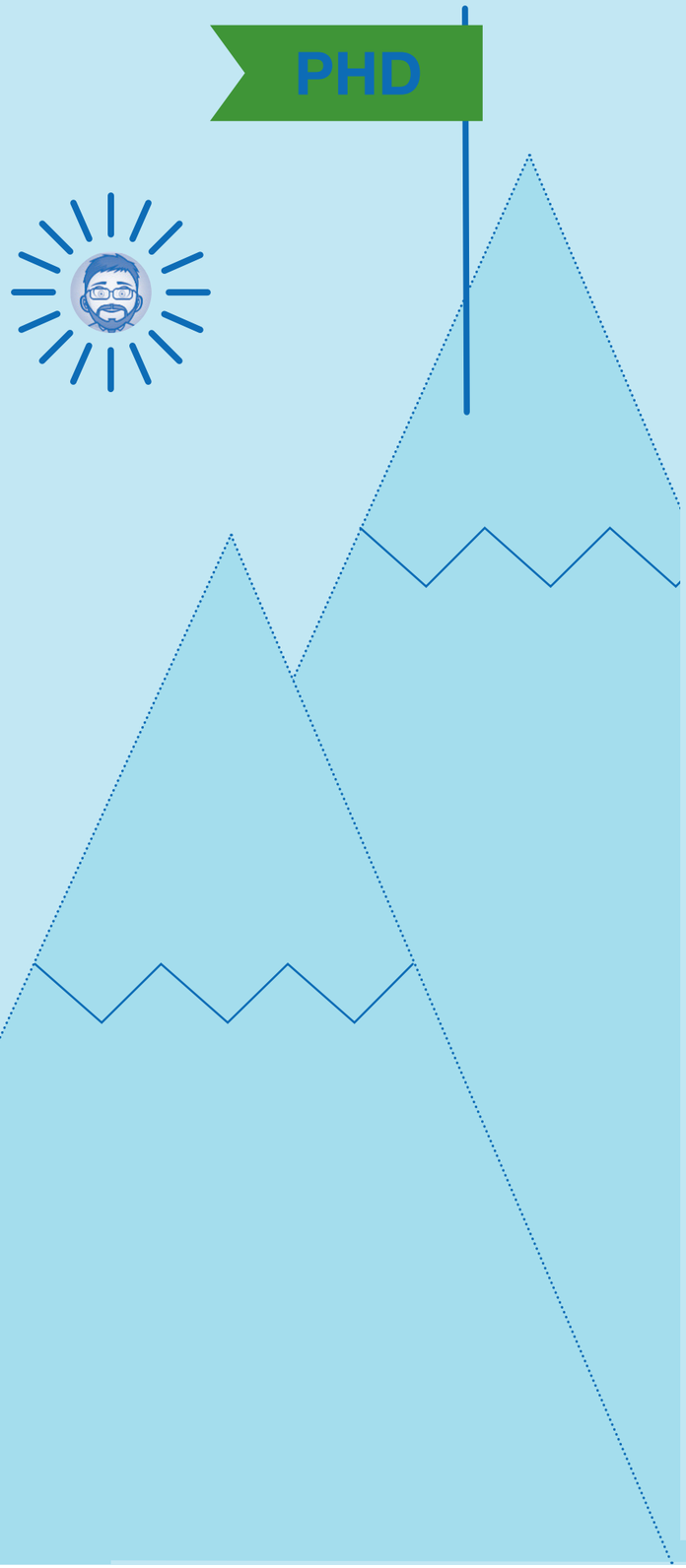
From the strategy perspective, organisations can define and manage responsible AI practices to ensure that fair, transparent and explainable AI solutions are used. From a technology perspective, organisations need a toolset that ensures all activities arising during an AI algorithm's lifecycle are analysed, managed and verified to ensure that they follow responsible AI guidelines and any relevant regulatory requirements.

Seclea (seclea.com), an ISG-RHUL spinout, provides an explainable and responsible AI platform to develop and use AI applications with fairness, traceability, transparency, and accountability. Organisations can manage their risk and regulatory compliance with the Seclea Platform and provide relevant information to all AI stakeholders. This enables all parties to jointly work towards building a better solution that benefits the organisation involved and the wider society.

Seclea's Platform integrates with the AI development and deployment pipeline, whether on-cloud or on-premise, with little friction. It allows data science and ML engineers to design, code, train, and evaluate the best AI solutions for a problem. Seclea works in the background, analysing the development activities and their potential impacts on fairness, explainability, risk profile and regulatory compliance. AI stakeholders, including data scientists, project managers, ethics leads, risk managers and auditors, can use the Seclea Platform to oversee an AI project. The ultimate goal is to enable a collective oversight and efficient management of AI risks.

1 https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

SECLEA
BUILDING TRUST IN AI



MY PHD EXPERIENCE
Craig Jarvis

> PHD Student

Shortly before Christmas, 2021, I successfully defended my PhD thesis. This is the story of how I got there, and why it so often looked as though I wouldn't.

Blackhat & Vitriol
My temple throbbed, punishing me for the previous night's excesses as intrusive music imposed itself upon my eardrums. The keynote speaker, Rick Falkvinge of the Swedish Pirate Party, took the stage amidst a flourish of strobe lighting that could disorient even those without a hangover. My friends and I were in Amsterdam at Blackhat, an event the media disapprovingly branded 'The Largest Hacker Gathering in Europe'.

Towards the end of his keynote, Falkvinge displayed a picture of Aaron Swartz. A few months earlier, Swartz attempted to download the entire contents of JSTOR, one of the world's largest paywall-protected academic databases. Swartz intended to liberate the cornucopia of knowledge. He believed the world's knowledge should be available to all online, not bound behind paywalls that only the elite could scale. But he was caught in the act. On facing what many considered disproportionate criminal punishment, Swartz committed suicide. Falkvinge proclaimed the community assembled before him to be amongst the world's most powerful collectives. If the governments of the world would not reform, we, the hacker community, Falkvinge preached, must tear down the Internet, our beloved yet disfigured digital creation. His presentation received rapturous applause. My hangover receded in the wake of the palpable vitriol aimed at the world's governments. Such tension could not be the outcome of a single incident. From where did it originate? Over the next few years, I watched as digital policy stalled, and the policies that did progress were poorly written – it was clear Information Security experts had been little consulted. I wondered what the long-term societal implications would be if the information security community and policy makers were, if not in open conflict, then permanently estranged.

The First of Five PhD Supervisors
A few years later I met Professor Thomas Rid. I told Rid that the genesis and history of the government-hacker tension would be a great research project, hoping he would perhaps adopt the subject for his next book. Instead, and with much trepidation, I enrolled at King's College as his PhD student to explore the issue. Only a year later, Rid departed to the US. The research project's scope was now a little more focused: I was exploring the crypto wars, the policy contestation around citizens access to cryptography technologies, and whether government should have exceptional access methods (backdoors). The crypto wars seemed to be at the heart of the government-hacker tension, but it was still an amorphous project that, in hindsight, I can see lacked the focus to make it a viable PhD.

Despite best efforts, my next supervisor and I could not make the research project work, and the following spring I left King's. My research was orphaned.

The Greek Mafia and the ISG
I kept working on the research, and sought a new supervisor, but nobody was keen to take on the ambitious project that spanned a host of disciplines: InfoSec academics felt the project to political; history scholars felt it too technical. I was all but resigned to the project's failure. Several months later, an old colleague of Greek origins mentioned that the 'Greek Mafia' may be able to help. This was his term for a network of fellow ex-pats garrisoned around the UK. The ISG's Dr Konstantinos Mersinas was in the mafia and referred me to Professor Keith Martin. Keith was enthused by the research project, and believed it would require co-primary supervisors given the interdisciplinary nature.

First Visit to the ISG
I couldn't quite believe it. Keith had found not one, but two other potential co-supervisors, one from Royal Holloway's Department of History, another from the Department of Geography. Together we sat gathered in his office whilst Keith's dog plodded around the room politely introducing himself to the strangers. As my elation that people were interested in my research subsided, I became worried: How was I possibly going to keep experts from two, or even three disparate fields satisfied? Were there even enough hours in the day to do all that reading? I was still working full-time as a Security CTO – had I bitten off more than I could chew?

But it quickly became clear that Royal Holloway, and ISG specifically, could be a home for the academically weird interdisciplinary thesis I wanted to write. A few meetings later, we'd decided that this research should formally live in the discipline of History – Dr Emmett Sullivan joined Keith as my co-supervisor. All of a sudden, the thesis seemed viable again.

Living the Fail Fast Philosophy
I was soon invited to speak at an ISG research seminar. Easy, I reasoned – public speaking is part of my bread-and-butter as a consultancy executive. Whilst I'm far from a natural academic, presenting I can do. But it was never going to be that simple. I'd expected questions on my topic. For almost four years now I'd been studying the Crypto Wars. Of course there would be curve balls, but I wasn't worried – I knew my topic. But I didn't expect a grilling on my methodology. Why would people possibly care about what I perceived be the most boring part of any thesis? Turns out, they did. In spectacular fashion, and in full view of the ISG community, my research methods were annihilated. But, after a few shots of bourbon to balm my wounded ego, I reasoned that it was good to identify the problems early – had they not been remedied before the upgrade it would have been much worse.

A Disruptive Pandemic
It wasn't long before more troubles arrived – Emmett was taking early retirement due to Covid. Having now lost three supervisors in four years, I considered abandoning the PhD – the gods were clearly not blessing my research. Inevitable the next history supervisor would want to re-scope the thesis, as their predecessors all had before them – having gone through that process twice already, I knew it would be immensely painful. I was demoralised. On joining Royal Holloway I'd already decided this was the project's last chance. If I were to lose a third supervisor, I would concede defeat. Pursuing research that seemed destined for failure, alongside a demanding full-time job, was just too punishing. I agreed to meet whomever Emmett's replacement would be out of courtesy, but confided to Keith that I would almost certainly be bringing down the curtain on this project that had haunted me for almost half a decade.

Supervisor Number Five
Dr Dawn-Marie Gibson was kind but candid; Whilst she could see a potential thesis buried somewhere in my work, it was shrouded. The research project seemed superglued to the starting blocks. Failure had become the defining feature of my PhD.

Dawn-Marie asked me to articulate the gaps in the crypto wars history, and to focus on one of them for the seemingly seven-hundredth thesis proposal. A few months earlier, I had released a book on the history of the crypto wars, a result of my many misdirected years of PhD research. The result of all that pain, was that by now I knew the history as well as anyone. It was an easy exercise, and only a few months later the project was re-scoped, with much of my earlier work re-purposed towards the new proposal. The PhD again felt possible, though I only gave the project a 1 in 4 chance of success.

The Digital Cold Shoulder
Filling the knowledge gap that I had identified, of why the controversial key-escrow programme (a Clinton-era initiative to add government encryption and decryption capabilities into consumer technologies) had been abandoned, would require interviews. I was locked down in London. Remote interviews were needed.

Trying to interview anyone associated with topics of national security is a nightmare. I reached out to scores of potential subjects and was constantly met with some polite refusals, but mostly just deafening silences. Slowly, a few agreed to interviews. Surprisingly, those who did say yes also introduced me to others they thought may be able to help – this snowballing approach worked much better than my cold calling. Several consented before withdrawing, leading me to ponder whether there was a conspiracy afoot, but I suspect most were just hesitant to speak about a topic that ran in close proximity to classified data.

The Interviews: Spies, Professors and Lawyers
The subjects were all professional, many having a seemingly sincere desire to recognise the intricacies of the subject under evaluation. The former-NSA members thoughtfully reflected on their approach. The digital rights lawyers were surprisingly understanding of the challenges that the Clinton administration were trying to manage – that of all manner of digitally-mediated ills. The academics were particularly keen to reinforce that this argument continues today, albeit in somewhat different parlance, such as client-side filtering. It was also the first time I'd used automated transcription, a practice I would highly recommend.

The Viva
Professors Richard Aldrich (external) and Klaus Dodds examined my thesis. They told me at the start of the defence that I was passing, which reduced my heart rate by about 50%. Despite this, the next hours were tough, if enjoyable. I was thrilled that the examiners were so engaged with the subject matter – they'd even read my oft-meandering footnotes! Aldrich and Dodds saw myriad angles that I had not considered, reinforcing to me that whilst at the conclusion of my PhD journey, it was only the end of the beginning of my learning curve as a researcher. I was elated when no changes were requested to the thesis. The examiners commended ISG and Royal Holloway for being an institution that could foster such interdisciplinary research across the rarely combined fields of history, geopolitics, policy and information security. I will forever be grateful to Keith, Dawn-Marie, Emmett, the ISG, and Royal Holloway for nurturing my research project to success.

The Future
With the trauma of the PhD receding, I'm now writing up an article version of the thesis, hopefully taking up some opportunities to guest lecture, and focusing on my next research topic: Cyber terrorism.

STAFF PROFILE: DR CHRISTIAN WEINERT

> Lecturer, ISG

//

How did you become interested in Computer Science?

As probably for many others, it all started with excessively playing video games in my younger days: first on an Amiga A1200, then on a worn-out Windows 2000 machine that neighbours passed on to me, and eventually on a custom-built gaming PC. However, besides being a consumer, I also started wondering how such games are actually created. Hence, I joined my school's computer club along with other enthusiasts and later signed up for elective computer science classes. When I first learned about the programming language Delphi and realised that I could program a computer to do almost anything I could imagine, this was a mind-blowing experience. Shortly after, I started playing pranks on friends with self-developed malware ;)

//

How did you become interested in Information Security?

My first real contact with information security was a course called "Introduction to Cryptography" at TU Darmstadt, which was excellently taught by Johannes Buchmann, who was mainly responsible for establishing many of the security-related research centres in Darmstadt. Thereafter, I signed up for more security-related courses and decided to do my Bachelor as well as my Master thesis in Prof. Buchmann's lab, both on the topic of secure long-term archiving. I also started working as a student research assistant and thereby got to know the daily life in research early on, and got the chance to get my first "behind the scenes" insights into teaching.

//

Tell us about your research!

I mainly work on privacy-preserving cryptographic protocols in the area of secure multi-party computation. By optimising such interactive protocols for specific real-world applications, I helped to provide efficient privacy-preserving solutions for example for analyses of genomic data, speech processing, and machine learning inference.

A special focus of my research is on so-called private set intersection protocols, where two or more parties want to compute the intersection of confidential input sets in such a way that nothing but the intersection result is revealed. This simple functionality is instrumental for a wide range of real-world applications; for example, the contact discovery processes that are implemented in various mobile messaging applications can be modelled as a set intersection problem. In the process of investigating such practical applications of set intersection, we also discovered several privacy vulnerabilities that potentially affect billions of users worldwide.

While further optimising the performance of interactive cryptographic protocols is one important area of future work, it is also necessary to think about how to apply such protocols to more complex use cases and how to automate their application-specific optimization so that non-expert software developers can come up with secure, efficient, and deployable solutions.

//

You mentioned several privacy vulnerabilities that you discovered in globally used systems. How did you proceed when finding such a vulnerability and can you give some examples?

In each case where we discovered such vulnerabilities, we followed the responsible disclosure processes proposed by the affected companies such as Facebook (now Meta). In about half of the cases, the companies then developed appropriate fixes that were deployed in a somewhat reasonable timeframe. However, there are also prominent examples where companies decided to acknowledge our findings but not to act. For example, in a project called "PrivateDrop", we discovered that whenever an iPhone or iPad user opens the sharing pane, every WiFi-enabled device in close proximity can capture hash values of the user's own contact information during the authentication handshake of Apple's AirDrop protocol. Since such hash values of low-entropy data are extremely vulnerable to brute-force attacks, mobile phone numbers and email addresses can easily be recovered by malicious actors – a problem that is still not fixed and affects more than a billion Apple users.

//

What are the joy and challenges of being a lecturer?

I like the exciting mix of conducting independent research, pursuing professional service activities for the global research community, participating in multiple teaching activities, and acting on the various administrative tasks that usually come up throughout a typical working day. Flexibility in terms of when and where to work is also a big plus. That being said, overlapping deadlines often result in a chaotic schedule and allocating time between the different activities is a real struggle.

//

How did you cope with the impact of the pandemic on university life?

Back at my former institution in Germany, our small research group was challenged with rapidly transitioning a large-scale undergraduate course with almost 1000 registered students to a new digital teaching format that replaces everything from in-person lectures to tutoring sessions and examinations. This worked out quite well; however, it was a massive effort, especially since we had to come up with many custom solutions. Here at RHUL, with the universally provided and well-integrated communication infrastructure, scheduling meetings works with an ease and results in great interactions. I'm also looking forward to the upcoming summer term and students coming back to campus – it was way too quiet so far

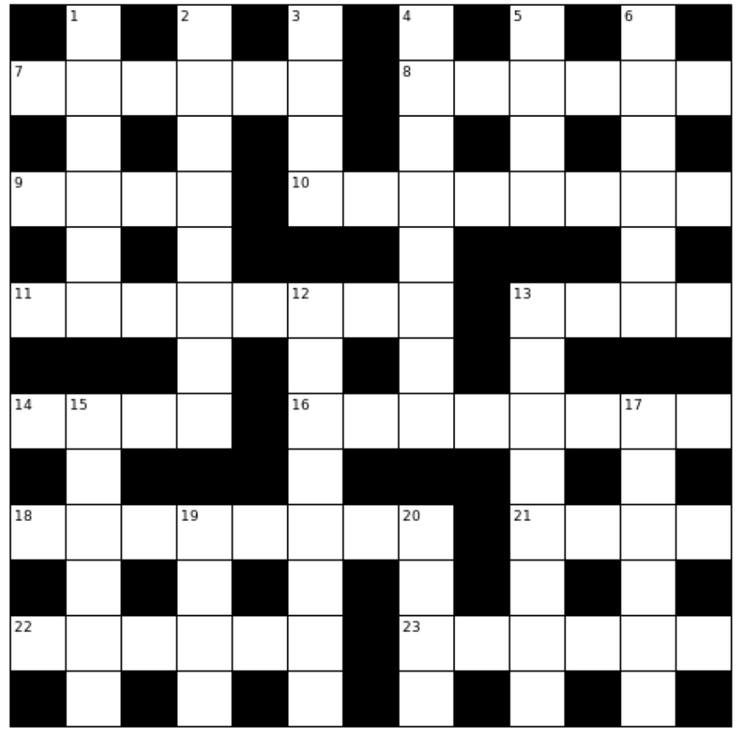
//

You recently relocated from Germany to the UK. How is your experience so far?

Apart from hefty visa application fees and several bureaucratic "chicken-and-egg" problems when trying to set up life in the UK, the experience so far is great! I love the beautiful RHUL campus and the surrounding nature. Also, it is great to have so many supportive colleagues within the ISG and the school office!

//

SHIFT WORK
By Serpent



Each answer must be encrypted with a shift cipher before entry in the grid: answers in the same row are encrypted using the same shift, as are answers in the same column.

The shift used to encrypt the rows and columns (in row then column order) is determined by the letters in a two-word key phrase (6,6); the letter C, for example, means A should be encrypted as C, B as D, etc. Four entries appear en clair.

Across

//

7 Knife used for stabbing (6)
8 Carnivore closely related to dogs (6)
9 Form of precipitation (4)
10 Wind instrument (8)
11 Sensible kind of number (8)
13 Softest substance on the Mohs scale (4)
14 Lepidopterist's favourite Shakespearean character (4)
16 Weapons, especially heavy artillery (8)
18 Aquatic mammal such as a dolphin (8)
21 Item of cutlery (4)
22 Greek letter used to denote wavelength (6)
23 Signal used to guide shipping or warn of danger (6)

//

Down

//

1 Pungent allium (6)
2 Destructive individual who might rout base? (8)
3 Noble gas (4)
4 Uncharged elementary particle with negligible rest mass (8)
5 Inexpensive restaurant (4)
6 More than enough (6)
12 Hard shell (8)
13 Brass instrument (8)
15 Fire _____ velocity (6)
17 Hot-headed mythical beast? (6)
19 Japanese drink/English author (4)
20 Club sport? (4)

//

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