Information Security Group

Review 23/24

ROYAL HOLLOWAY UNIVERSITY OF LONDON

INDEX

INTRODUCTION
— Lizzie Coles Kemp

> Professor & Head of ISG Department

Welcome to the latest edition of the annual ISG Review. I have been contributing to this review since joining the ISG in 2008, but for the first time I am writing as Head of Department for the ISG. I first met the ISG in 1993 when I was working as a security software engineer. By that point I'd been working in information security for three years, and I was thrilled to learn that information security was an area of academic study as well as of practice. My relationship continued with the ISG; I enrolled as a student onto the MSc in Information Security on a part-time basis in 1997 and then joined the ISG as a member of staff in 2008. The ISG has always been a special place; it's a meeting point between information security practice, policy, and research and I am honoured to be its Head of Department.

I have, of course, very big shoes to fill. Chris Mitchell stepped in as an interim head of department two years ago and did a great job of leading the department out of COVID measures. Chris also spearheaded the development of our Coursera distance learning programme. I'd like to give my heartfelt thanks to Chris for his term of departmental leadership and for his support as I take over that service.

As the articles in this newsletter show, the last 12 months have seen the ISG continue to go from strength to strength. The Coursera Distance Learning Programme led by Fauzia Idrees has continued its great success; at the time of writing, we have some 1300 students enrolled on the programme and these students are located all over the world. Developing the Coursera programme has given us a chance to revisit our syllabus and the hard work that colleagues have put in to developing this programme will stand us in good stead when we review our campus syllabus later on this year.

This year has also seen success in obtaining research grants. For example, Jassim Happa and Konstantinos Mersinas were successful in attracting EU funding for their project ResilMesh and Rikke Jensen succeeded in attracting EPSRC funding for the project Social Foundations of Cryptography. In addition, several colleagues have been awarded consultancy and knowledge exchange funding. I am also delighted to say that the ISG has been re-accredited as a NCSC Academic Centre of Excellence in Cyber Security Research.

Our knowledge exchange and engagement work continues to be a vital part of our work. Darren Hurley-Smith is technical manager for Omnidrome, RHUL's state of the art drone and sensor research and innovation centre, and his efforts are key for the success of this important RHUL investment. Darren's work is a good example of how ISG staff develop knowledge exchange networks both across the institution and with external partners.

Sadly, this year we say goodbye to Santanu Dash and Guido Schmitz. I'd like to take this opportunity to thank Santanu and Guido for their contributions to the ISG and we wish them the very best in their future endeavours. We are in the process of recruiting new staff members and I look forward to introducing you to them in our next annual review.

I'd like to close by writing a few words on Fred Piper, a tribute to whom is included in this newsletter. I was deeply saddened to hear of Fred's death. It was Fred's vision and foresight that made it possible for people with many and varied backgrounds to study and research information security and in so doing he made the practice of information security all the better for it. Thank you, Fred!

IN MEMORIAM FRED PIPER: 1940–2024
— Chris Mitchell

> Professor, ISG

It is with great sadness that I have to tell you that Professor Fred Piper (simply Fred to everyone who knew him) died at home after a long illness on March 11th 2024. Fred made huge contributions to society generally, at home and abroad, but in this brief article I will mainly focus on his work at the University of London.

Fred studied for his BSc and PhD at Imperial College, before taking up a lectureship at Royal Holloway in the mid-1960s. He then moved on to Westfield College, University of London in the late 1960s. Westfield was where I first met him; I was a first year undergraduate in his algebra lectures starting in October 1972, by which time he was already a Reader in Mathematics. His wonderfully clear and inspiring lectures made an enduring impression on all of us. After gaining my first degree in 1975, I was fortunate enough to stay at Westfield to complete my PhD under his supervision. He was a wonderful supervisor as well as teacher, giving me just the right encouragement and push at the appropriate times. At Westfield, Fred joined the late Dan Hughes, and they together formed a formidable research partnership, enduring through the 1970s and beyond. They co-authored a milestone book Projective Planes, which became a standard graduate level textbook on the subject. As Fred recalled about Dan after his death in 2012, 'he will probably be best remembered for his inspirational lectures, his infectious enthusiasm for mathematics (and life in general) and his willingness to spend time with anyone who was interested, no matter whether they were established senior researchers or fresh faced PhD students. I have lost count of the number of well-established mathematics professors who admit to being influenced by Dan and who unashamedly admit that they owe some of their success to his influence. I am proud to be one of them.' I think that everything Fred wrote about Dan could equally be applied to Fred, in spades.

With the end of science teaching at Westfield, Fred moved back to Royal Holloway in the mid-1980s and developed a research group in Cryptography, working closely with the then newly appointed Peter Wild; Peter had been a PhD student at Westfield College in the late 1970s, and although supervised by Dan Hughes rather than Fred, nonetheless worked closely with him. Fred's interest in cryptography had been sparked by another former PhD student of his, Henry Beker, who in the late 1970s was appointed as Mathematician at Racal Datacom, a company making cryptographic equipment. Indeed, such was the level of interest that Fred and Henry jointly published a trailblazing book on cryptography, Cipher Systems, in 1982.

When Dieter Gollmann and I joined Royal Holloway in 1990, with our more Computer Science focussed interests complementing Fred and Peter's Mathematical interests, it seemed natural to develop and launch an MSc in Information Security, which we did in 1992. Fred was clearly the leading and inspirational figure in developing the degree as well as what became the Information Security Group. By the time the degree was launched, we had also been joined by two further key figures in the life of the ISG, Chez Ciechanowicz and Sean Murphy. Over the subsequent years Fred's own interests broadened to cover not only cryptography but also the broader, industry and commerce focussed, subject of information security, where he became a champion of early attempts to develop the security profession through his work with the IISP.

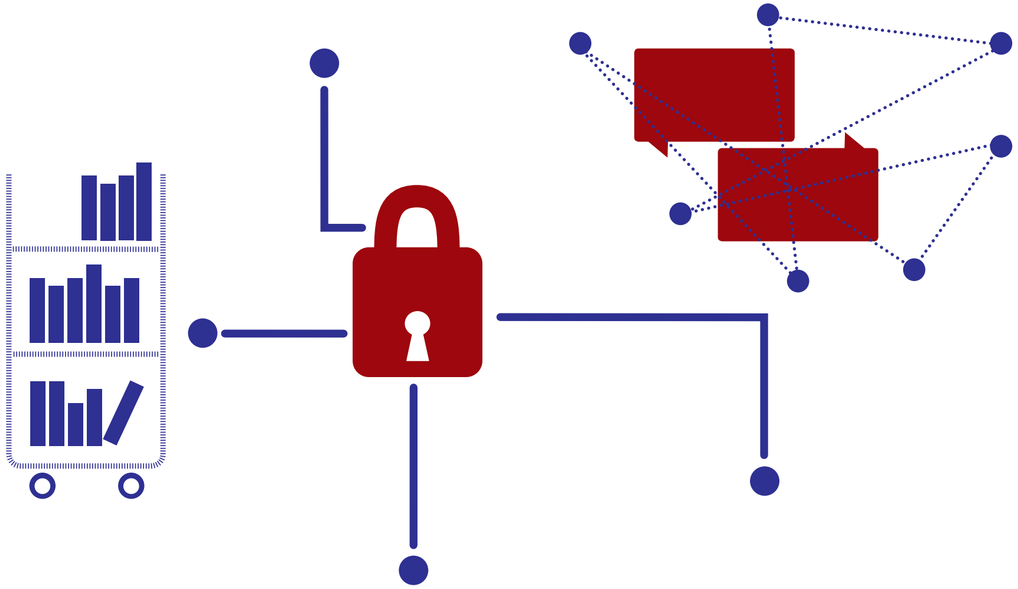
Of course, volumes could be written about Fred's influence on the development of the ISG at Royal Holloway over 30 years, as well as the practice of Information Security in the wider world. Suffice it to say that Fred was the key figure, not only for his long spell as ISG Director, but also subsequently when he was a hugely important source of wisdom and guidance to his successors in the role. Fred cared deeply about the ISG, which of course today is an academic department in its own right, and the ongoing success of the department is a testament to Fred's dedication and energy.

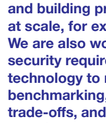
Fred looked after and cared deeply about his PhD children. From my own experience I can testify that he was always keen to stay in contact and continue to work with his ex-students. As I already mentioned, his continuing contacts with Henry Beker led to him to develop an interest in Cryptography which not only led to the book I already mentioned but can be seen as the root of the Information Security Group today. I have already mentioned Peter Wild and Henry Beker, but many other former research students of Fred have, through their ongoing relationship with Fred, gone on to develop careers in security. For example the late and sadly missed Mike Walker, Fred's second PhD student who started in the late 1960s, became a world-renowned expert on Cyber and Mobile Security and Cryptography within the telecommunications industry and academia, serving as Research and Development Director for Vodafone Group worldwide for ten years. Klaus Vedder, supervised by Fred in the late 1970s, became Group Senior Vice President at Giesecke and Devrient. Both Klaus and Mike became ETSI Fellows in 2018, recognising their contributions to mobile telecommunications.

Once Fred and Peter Wild were re-united at Royal Holloway in the mid-1980s, they jointly supervised a long line of PhD students who have gone on to become major players in the field of cryptography and security. Current and former ISG staff members who graduated from this school include Karl Brincat, Alex Dent, Keith Martin, Siaw-Lynn Ng, Kenny Paterson and Matt Robshaw, and key players in UK industry and academia include Steve Babbage, Simon Blake-Wilson, Andrew Bowler, Tony Bromfield, Glyn Carter, Matthew Dodd, Mel Dymond, Richard Horne, Mark Hoyle, Maura Paterson, Stephanie Perkins, Tim Stinchcombe, Jonathan Tuliani, Alison Vincent and Mike Ward. I could go on and on, and apologies for not mentioning the many other individuals who benefitted from Fred's supervision and friendship.

Fred was the subject of many awards. He received the IMA Gold Medal in 2002. He led the Royal Holloway Information Security Group when it was awarded the Queen's Anniversary Prize in 1998. He was invited to give the 2004 BCS/IEE Turing Lecture. He was awarded an honorary CISSP for 'leadership in Information Security' in 2002, the first European to be given such an honour. He was awarded an honorary CISM for 'globally recognised leadership' and 'contribution to the Information Security Profession' in 2003. He was named Network Professional of the Year in the 2005 Communications in Business Awards, and was added to the ISSA Hall of Fame in 2005. In 2008 he was elected to be a Fellow of (ISC)2, and in the same year he was the first person to be elected to the InfoSecurity Europe Hall of Fame. Also in 2008 he was elected to the International Advisory Board of IMPACT (the International Multilateral Programme Against Cyber Threats). In 2011 he was awarded an Honorary Fellowship by Royal Holloway, University of London. In 2021 the CIISec named an annual award after him (the Fred Piper Award). I suspect I have omitted many more honours and recognitions than I have mentioned here - Fred was held in the highest of esteem worldwide.

Above all else, I think Fred would be happiest with the knowledge that through his teaching, wise counsel and encouragement, he personally touched – and improved – the lives of so many people, although he would no doubt squirm to read this praise as he always sought to avoid the limelight. He will be very sorely missed by so many.





INTRODUCTION TO THE CRYPTOGRAPHY GROUP AND OUR 2023 – 24 HIGHLIGHTS
— Rachel Player

> Lecturer ISG, Director Cryptography Group

Overview
The Cryptography Group was formally founded in May 2021 by members of the Information Security and Mathematics Departments. However, cryptography research in the ISG goes back to at least 1987, making it one of the oldest academic groups working in cryptography. We are a team of ten permanent academics and many PhD researchers. We are passionate about the subject and involved in the international cryptographic community. Collectively, we are particularly interested in developing solutions in three important areas of cryptography: post-quantum cryptography, secure computation, and the design and analysis of secure protocols. We have additional expertise in information theoretic security and cryptanalysis of symmetric cryptosystems.

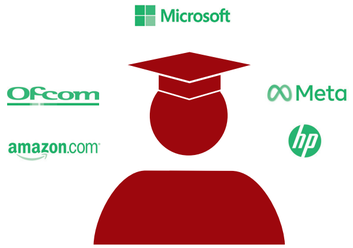
Research
Some of the key research questions that we are working on now include improving efficiency of homomorphic encryption and secure multi-party computation protocols, and building privacy-preserving applications at scale, for example, for machine learning. We are also working on approaches to map security requirements of communications technology to mathematical properties, for benchmarking, understanding parameter trade-offs, and development of practical security measures. We are also analysing the security of protocols in secure messaging and e-voting, as well as constructing protocols with stronger security or anonymity guarantees.

Teaching
Our research expertise informs the teaching of cryptography, which we deliver across a range of modules. We have dedicated modules on cryptography at the BSc and MSc levels on campus and for Distance Learning via Coursera, for which we have developed books to support our teaching. Alongside this, we incorporate material on cryptography in other modules, including an introduction to information security module for second-year BSc students. Advanced cryptographic concepts such as homomorphic encryption and secure multi-party computation are also touched on in our Coursera module on information privacy. We supervise a range of BSc, MSci, and MSc projects on topics across cryptography. We are also considering a new module in Advanced Cryptography for the MSc programme. We supervise a number of PhD researchers in cryptography, creating a supportive research environment through the CryptoChats and FHE reading groups.

Knowledge exchange
We are not just focussed on research and teaching, but we are also active in a range of knowledge exchange initiatives. We organise events such as the London-ish Lattice Crypto & Coding Meetings that feature a range of national and international researchers in cryptography as speakers. We also give invited talks on our research at various venues, including in other disciplines. We have been active for many years in various standardisation organisations (including BSI, ISO/IEC, and ETSI), informing the development of new cryptographic standards, and we are hosting an ISO/IEC SC 27/WG 2 meeting in April 2024. We provide consulting services to a range of organisations. We are active in outreach including the development of a booklet for toddlers on the topic and designing a mini course on “cyber security for change makers” with a part on cryptography for 6th form students, with the aim of increasing diversity in the sector. Cryptography researchers have also taken the lead in diversity initiatives such as supporting the Wisdom group locally and through organising the Crossfyre event, which supports early-career women working in cryptography.

Highlights

- We continued to publish our research at top-tier venues in cryptography and security including Asiacrypt 2023, CSF 2023, IEEE S&P 2023 and 2024, and Eurocrypt 2024.
- Members of the group were invited panellists or speakers at a variety of events including HISC 2023, WAC6, and UK Crypto Day.
- We served on the programme committees of top-tier venues, including ACM CCS 2023 and USENIX Security 2023.
- We welcomed some of our external research collaborators to visit Royal Holloway (for example, from NXP, Belgium; Aarhus University, Denmark; and INSA CVL, France), and participated in research visits to other institutions (for example, to University of Bristol).
- We organised and hosted the 5th edition of the London Crypto Day in June 2023 at RHUL.
- We hosted the 19th IMA International Conference on Cryptography and Coding at RHUL in December 2023, and the programme chair was Elizabeth A. Quaglia.
- We are due to host the spring meeting of ISO/IEC SC 27/WG 2 (whose focus is the development of cryptography standards) at RHUL in April 2024.
- We launched the Crypto Chats reading group for members to stay updated about current results in the field and to present their own work.
- Several researchers obtained their PhD in cryptography in 2023. Congratulations to Dr Marcel Armour, Dr Luke Stewart, Dr Jeroen Pijnenburg, Dr Lenka Mareková, Dr Simon-Philipp Merz, Dr Jodie Knapp, Dr Liam Medley, and Dr Angelique Loe.



CENTRE FOR DOCTORAL TRAINING UPDATE
— Keith Martin

> Director & Professor, ISG

September 2023 saw the fifth, and final, cohort of new PhD students commence their studies in the EPSRC Centre for Doctoral Training in Cyber Security for the Everyday. If we view the current CDT as an extension of the original, then this was the eleventh cohort to join Royal Holloway. This means that the CDT, overall, has overseen around 110 PhD projects – around half of which have now completed. That’s quite a statistic!

The achievements of the CDT are possibly best evaluated not through academic papers, research talks or internship experiences (although these are all important!) but through the destinations of CDT graduates. Here are just a few of the latest job titles: Senior Researcher at Microsoft Research, User Experience Researcher at Meta, Cyber and Hybrid Policy Officer at NATO, Principal - Privacy, Security and Academic Partnerships at Ofcom, Applied Scientist at Amazon Web Services, Senior Security Researcher at HP, Senior Cryptography Engineer at Proton, Founder and CEO at RevEng.ai, Lecturer in Cryptography, King’s College London, Consultant, Crisis & Security Strategy at AnotherDay, Cofounder & CTO at Oso, Cyber Security Researcher at WithSecure, and Chancellor’s Fellow, University of Edinburgh. And this list goes on… This is a proud legacy of highly-qualified people whose careers are progressing not solely because of their CDT experience, but at least partially through the foundations and broad perspectives on cyber security that the CDT has helped to foster. Congratulations to everyone who has graduated and we look forward immensely to discovering where the other half of our (current) students end up pursuing their careers.

Speaking of current students, the 2023 cohort are well into their first year of training and are doing very well. As with previous cohorts, the first task we assigned them was to self-organise and deliver a group project on a topical cyber security subject. This year the cohort were assigned the task of investigating what privacy and security challenges and opportunities are presented by generative AI. Their excellent report and presentation focused not just on technical aspects but also societal and social perspectives. This year (as for every year!) the cohort have diverse academic backgrounds, so their project looked at crime, politics, education, intellectual property, creative industries, healthcare and environmental issues. In conducting this project they not only learned about generative AI but, just as importantly, about themselves, since the main aim of this group task is to begin to appreciate how people with different backgrounds approach and reason about cyber security. If the success of this project is anything to go by, there are another dozen fascinating PhD projects on the way.

I’d like to take this chance to remind everyone that the CDT is always seeking external partnerships to support our work. The most obvious touchpoint is through the support of internships, which is a component of the CDT programme that enables students to experience cyber security through the eyes of partner organizations. These are typically around three months in duration, so please get in touch if you feel this opportunity might be of interest.

Operationally, the most significant news concerning the CDT is the departure of our CDT Manager Claire Hudson. After over a decade of supporting the CDT, Claire is moving on to a new role. It is almost unimaginable to consider the CDT without Claire at the helm of proceedings. Claire has been instrumental in supporting the students, running our events, putting together the first-year programme, and generally helping everyone involved with the CDT to navigate the bureaucracy behind every CDT journey. On behalf of the students, staff and all our external partners, I would like to give an enormous thanks to Claire for the energy, enthusiasm and expertise that she brought to the role.

TIGHTROPE: A CYBER SECURITY COURSE FOR CHANGE MAKERS
— Liz Quaglia
— Joe Reddington

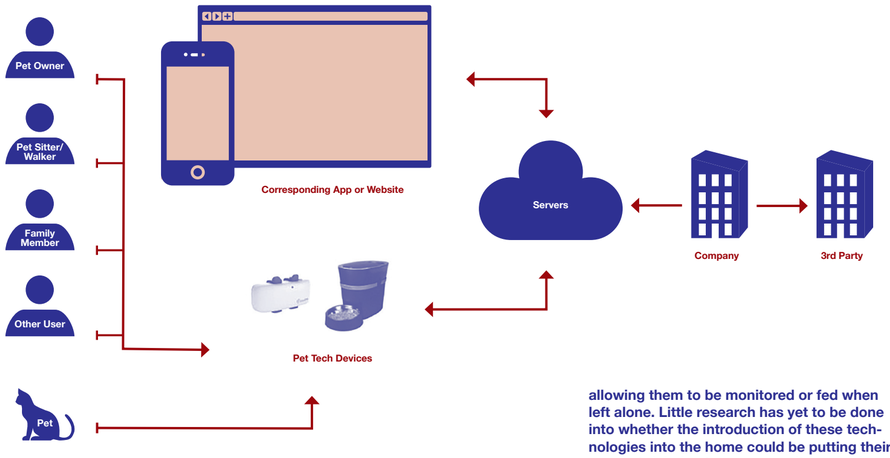
> Reader, ISG
> Lecturer, ISG

In 2023 over 600,000 young people in the UK finished secondary education, the majority of them with only the most basic concepts of cyber security. Even at A-level, a time when young people are starting to express themselves, explore relationships, and navigate their own personal privacy, the education sector is entirely lacking. Worse, when advice or guidance is given, it typically comes in the form of “share nothing, put nothing on social media, protect your privacy at all costs”, which is too restrictive and draconian to be accepted by young people finding their place in the world. Overall, the cybersecurity sector has an opportunity to enhance its support for individuals by refining the targeting and timing of resource delivery.

Meanwhile young adults are socially engaged and strongly motivated to make a difference. The democracy of the smartphone means that competing and conflicting views about what constitutes a threat and who should be protected emerge in ever younger parts of society. Online abuse, doxing, and other threats are more salient and damaging. Young people that are interested in changing the world are exactly those that would benefit from more cyber security knowledge and training but are also exactly the ones that don’t identify with the cultural stereotype. The cyber security sector has been slow to recognise that the market for cyber security training is moving away from programmers and nerds and towards campaigners and activists. Our target population aren’t interested in ‘Cyber security careers’ but they are interested in ‘Digital safety in social change’.

Last year we designed a unique type of cyber security course to help correct these two issues by creating a six-session “Security for Changemakers” aimed at A-level students that provides important cyber-security education through the lens of young people who are trying to change the world: they learn risk assessments from examining charities; they learn about jigsaw attacks from case studies of activists being targeted; and they learn about encryption by examining examples of corruption. That is, they were given a full cyber-security toolkit, without ever touching a keyboard or thinking in ‘classic terms’. The covered topics include digital security, physical safety, and legal considerations, all in the context of advocating for positive change. In general students pick an issue they were passionate about (or used an example from one of our ‘change cards’) and are led through a series of exercises to explore the effects of various security issues.

Figure 1: The pet technology ecosystem; showing how users interact with these systems. Other users may include vets, insurance companies, health clinics, etc. Arrows represent the flow of data.



COLLABORATIVE SYSTEM SECURITY RESEARCH AT THE ISG

— Maryam Mehrnezhad
— Scott Harper
— Stephen Cook
— James Clarke

> Dr & Senior Lecturer, ISG
> PhD student, Newcastle University
> PhD student, ISG, RHUL
> PhD student, University of Surrey

System security research is a broad area of cyber and information security and privacy. Such research can focus on hardware infrastructure, software products such as apps and websites, misinformation on social media and dark web platforms, systemic bias and discrimination in AI and ML, user tracking across platforms, as well as human dimensions and trust in systems and the legal aspects of these systems.

Here at the ISG, we work on a range of system security research topics collaboratively within the department and beyond. This article showcases examples of such projects performed by PhD students.

APP VULNERABILITIES IN ANIMAL TECHNOLOGIES:

Scott Harper is a final-year PhD student, based at Newcastle University, UK. His work focuses on animal technologies, a range of digital products that can aid in the care of a pet, providing health-related information, or allowing them to be monitored or fed when left alone. Little research has yet to be done into whether the introduction of these technologies into the home could be putting their users at risk due to poor security and privacy practices. To this end, we performed a range of experiments to determine whether the users and their data are at risk [1].

We began by analysing the login procedures of mobile apps interacting with these technologies, looking at 40 popular pet and farm Android apps. Using a combination of static, dynamic, and network traffic analysis tools, we identified serious security vulnerabilities in these apps, that would openly expose a user's login details. After communicating these vulnerabilities to the responsible companies, two of these apps later removed these vulnerabilities, no longer exposing user details. We also identified various poor privacy practices, with many of the apps violating GDPR by not getting user consent before communicating with tracking services.

Following on from this study, we wanted to gain a better understanding of the users' perspectives and experiences. We conducted a user study of 593 participants across three countries (UK, USA, and Germany), looking at the types of data they believe are collected, incidents that have occurred, as well as capturing their concerns and the security precautions taken. We found that, despite many of the participants showing concern over some form of incident occurring, they were far less likely to take precautions to protect themselves when using these technologies, compared to their general online security precautions.

We additionally reviewed top-ranking animal welfare legislation, finding no real mention of these technologies. Given that animals and their data are the focus of these devices, this likely leaves the real users of these technologies (human users) at risk. We are continuing our research in this space by collaborating with colleagues across other disciplines and other related stakeholders such as vets and farm managers.

BLE ATTACKS ON FEMALE-ORIENTED TECHNOLOGIES:

Stephen Cook is a first-year PhD student at the ISG at RHUL. He was previously a Research Assistant on the EPSRC PETRAS CyFer project. He performed a range of attacks on FemTech IoT devices. The rise of IoT devices containing environmental sensors, storage and communication technologies, has led to the creation of personalised healthcare devices which have revolutionised how an individual manages their health. The benefits provided by this new category of IoT devices, which we call Medical IoT FemTech, come at the cost of the collection of personal and intimate data including heart rate, reproductive and sexual health data, psychological health, location, etc.

These devices work alongside apps installed on a user's phone allowing them to monitor and adjust their experience. This personal data is often highly sensitive, meaning that ensuring its privacy and security is of paramount importance. Unfortunately, this data is often shared with other entities before the users have necessarily agreed to do so or without their knowledge. We have shown that these apps often contain trackers; pieces of software that gather analytical data regarding how the user is using the app.

The majority of these smart and connected IoT devices use Bluetooth Low Energy (BLE) to communicate with the mobile app. We specifically studied the BLE implementations in around 30 IoT FemTech devices and found them to be lacking proper authentication in establishing communications allowing for spoofing attacks. Some of these devices and apps do not employ proper encryption methods to secure the data during transit, meaning an attacker could intercept this personal information [2]. In addition to these system studies, we have conducted user studies highlighting the concerns of the users of such systems.

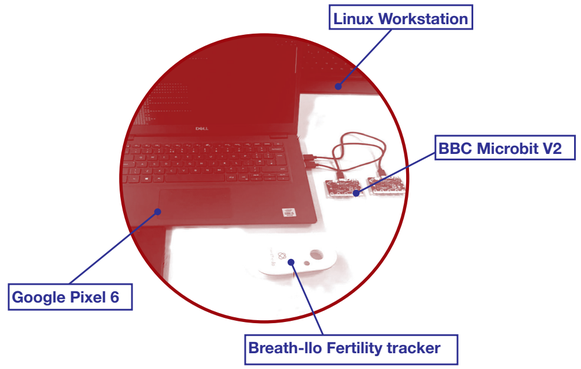


Figure 2: BTLE traffic analysis configuration using BBC Microbits V2 and an IoT fertility tracker as an example

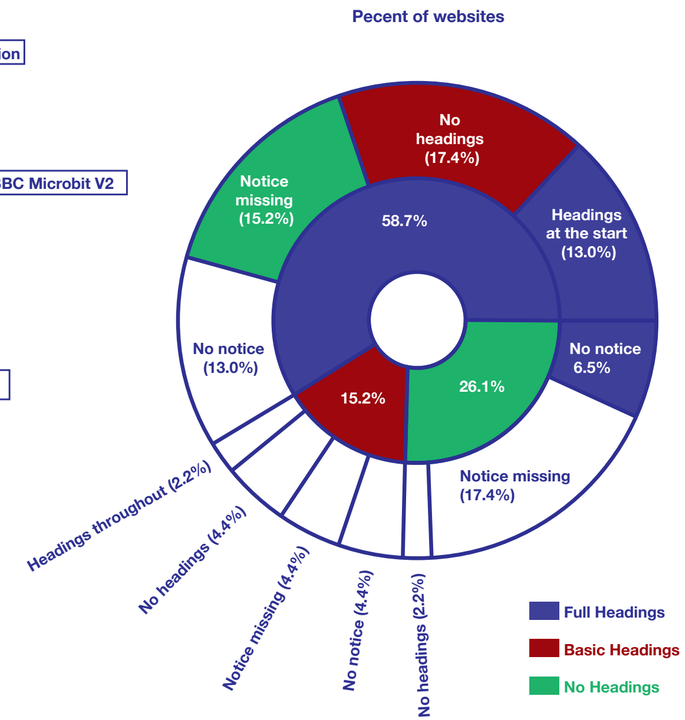


Figure 3: WebbIE accessibility testing; inner circle: the whole site, outer circle: the cookie notice.

We have also reviewed the related regulations showing that there is a gap in the current regulations and practices regarding the protection of such sensitive data. We are working with a number of academic and industrial partners, sharing our research results and contributing toward better security and privacy features and experience in such systems.

EVALUATION OF COOKIE NOTICES FOR USERS WITH VISUAL IMPAIRMENTS:

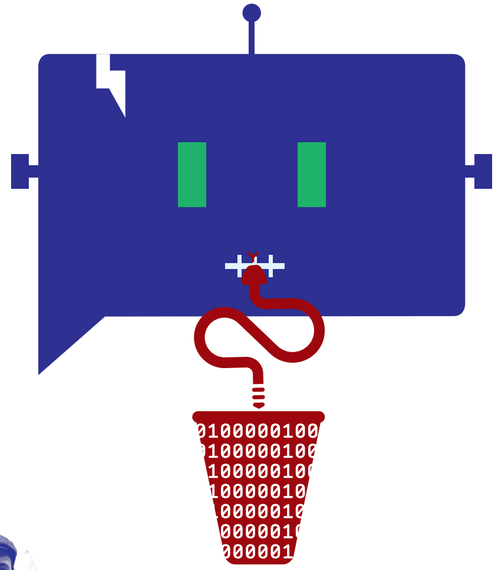
James Clarke is a second-year PhD student at the University of Surrey, working on the security and privacy of accessible technologies for people with visual impairments. Visual impairment is a broad term to describe any vision loss, ranging from partial vision loss to complete blindness. In the UK, there are more than 2 million people who have visual impairments, with around 60% of them being women. People with visual impairments have a variety of tools, called assistive technologies, which can help them use computers and access the Internet, such as screen readers.

Our work investigated how various assistive technologies interact with website cookie notices [3]. Cookie notices provide a method for users to decide which cookies are stored on their devices, impacting their privacy online. Through a series of system and user studies, we observed the current practices of cookie notices and users' opinions towards cookie notices. We found that several cookie notices were inaccessible to users of assistive technology and that users generally had a negative perception of cookie notices. We also discovered that many websites omitted the necessary headings in their cookie notices, as illustrated in the figure. Based on this, we gave recommendations to improve the current cookie notice landscape.

In our current work, we are looking at the security practices of the assistive technologies themselves. While the work is still in its early stages, we have found several issues, which we have brought to the attention of assistive technology manufacturers with the aim of improving the security and privacy of these tools. We continue to work on such an important topic in a collaborative way with multiple stakeholders. We hope to enable users with visual impairments to use modern technologies and improve the quality of their lives without any risk and fear.

References

[1] Harper, Mehrnezhad, and Leach, "Security and Privacy of Pet Technologies: Actual Risks vs User Perception.", Frontiers in the Internet of Things 2: 1281464, 2024
[2] Cook, Merhnezad, Toreini, "Bluetooth Vulnerabilities in General and Intimate Health IoT Devices and Apps: the Case of Female-oriented Technologies." 2024
[3] Clarke, Mehrnezhad, and Toreini. " Invisible, Unreadable, and Inaudible Cookie Notices: An Evaluation of Cookie Notices for Users with Visual Impairments."



PROTECTION AGAINST AI SYSTEM MISBEHAVIOUR AND MISUSE

— Jassim Happa

> Lecturer, ISG

Over the last 18 months we have seen an exponential growth in uses of AI, particularly those based on Large Language Models (LLMs). While AI systems, including those that use LLMs, have become excellent at predicting text for search engines and chatbots, they also come with a variety of problems. Firstly, they cannot separate fact from fiction. This is often observed as an effect referred to as hallucination. Facts or problem-solving solutions are never guaranteed to be correct. Secondly, they can only predict information based on what they have observed – meaning that whatever they generate is a function of probability and data they have processed. Thirdly, they cannot reason. However, more recent innovations in this space suggest that reasoning engines are currently being developed and will likely be built on top of LLMs that function as knowledge bases, so AI systems will be able to derive mathematical proofs and demonstrate rudimentary forms of creative and critical thinking – while also fact-checking their findings.

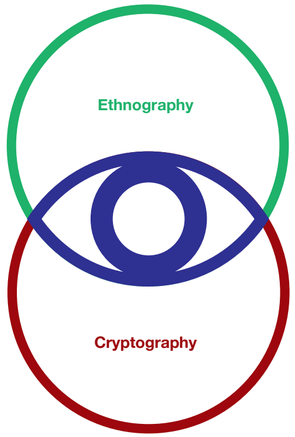
We have seen a plethora of novel applications leveraging LLMs to deliver new capabilities, including amongst many others: accessibility (e.g. the Rabbit R1); first-pass disease diagnosis; medical product development, including drug discovery and testing; generating media (e.g. images, video and audio); and language translation. This leaves researchers with many concerns about the future of AI - including about the possibility of superintelligence or AIs going rogue. For the foreseeable future AI systems will still need oversight, to ensure they behave within acceptable boundaries and do not manifest as safety or security concerns. We will also need the methods and tools to appropriately respond to AI system behaviour when things do go wrong.

The dramatic growth of AI systems has created major challenges in security and incident response such as:

- *AI-system threats.* AI systems can misbehave -- i.e., threats and undesirable behaviour can come from the AI system itself because of design flaws or intrinsic limitations of the underlying implementation, algorithm, method, or bias of the developer and/or data used in training. AI systems can also be misused -- i.e., threats can come from malicious actors manipulating AI systems, e.g. through data poisoning or prompt engineering, even if the AI system appears to behave as intended. Examples of potential threats include:
  - *Attacks and vulnerability discovery.* Attackers can exploit AI system vulnerabilities to manipulate the AI system's behaviour, or use AI to discover new vulnerabilities (either about itself o r of other systems).
  - *Safety.* In safety-critical systems and safety-related scenarios, it is vital to be able to make split-second decisions that can be independently verified as appropriate behaviour.
  - *Alignment.* Alignment in AI refers to ensuring that AI systems behaviour and use is consistent with human values, goals, and intentions. Key challenges that need addressing include: value specification (i.e. what are "our" values in the first place?), preventing reward hacking, generalisation (i.e. scaling the alignment for all circumstances), robustness, preventing value drift (or indeed, drifting with us if our values do drift), and including ethical diversity.
  - *Corrigibility.* An AI system should cooperate with corrective intervention, even when it possesses default incentives to resist. It should also deny attempts at intervention by malicious actors to prevent misuse.
  - *Data Privacy.* AI systems often require access to large amounts of sensitive data to learn and improve. Ensuring privacy and preventing unauthorised access to personal data or sensitive data remains a significant challenge.
  - *Intellectual Property.* Training data in AI systems is often based on creative content generated by real people who own the associated IP. The lack of protection of intellectual property has given rise to art being generated "in the style of" another artist, or even inappropriately copying content outright.
- *Interoperability.* No shared vocabulary for AI-system incident response exists. As AI systems become more complex and widespread, ensuring "security at scale" becomes a challenge. Having a common vocabulary could facilitate and improve capability and capacity for responding to AI-system incidents.
- *Context* is difficult to capture and update. Context may include the circumstances in which the AI system is operating or the intent behind the use of a particular AI system capability. We need dynamic solutions that can adapt to such real-world situations. Threats may exist despite not appearing in the testing of AI-systems. These may not be covered by existing, more static guard rails (protection measures).
- *Ad hoc* empirical and experimental evidence. Currently, most testing efforts assume white box access to AI systems, and benchmarks are often defined by developers. Most AI systems are proprietary – leaving less room for a community-driven, best-practice and standards effort. Generating more scientific evidence can also inform future regulatory and policy discussions.
- *Explainability, Interpretability and Accountability*. Many AI models operate as black boxes, making it challenging to understand how they arrive at their decisions. The lack of explainability can lead to mistrust, and can make it difficult to identify and mitigate potential biases or errors in the system.
- *Slow establishment and development of AI-system threat detection best practices.* Security and safety testing is often specific to the AI-system in question as AI-systems are often tested internally in companies. This siloing of experiences limits the sharing of lessons learned.

Today most efforts directed towards the security of AI focus on building secure and safe AI from the ground up, or on make existing systems more secure. Addressing these security-related challenges requires a combination of technical measures, robust testing, and collaboration between AI developers, security experts, and policymakers. Currently, AI-system practices such as guard railing, utility functions, conformance testing, and model checking (among others) are bespoke and specific to the AI-system in question. There is a need for foundational research necessary towards improved standards in benchmarking, testing, and monitoring AI-systems for the protection of organisations and individuals. In the coming years, I expect – and certainly hope – to see solutions that move towards real-time monitoring of AI system behaviour. How exactly these solutions will be designed and implemented is yet to be determined.

In conclusion, the abundance of data and advances in computing capacity have allowed the development of powerful AI-systems. This has given rise to new security concerns arising from the possibility of AI misbehaviour and misuse. Today, most efforts on security of AI focus on building (secure and safe) AI from the ground up. We need to conduct foundational research towards an AI-system incident detection and response solution that can protect assets (including people) from AI system threats – particularly focusing on safety scenarios.



SOCIAL FOUNDATIONS OF CRYPTOGRAPHY

— Rikke Bjerg Jensen

> Reader, ISG

In the 2019-20 edition of this newsletter, I wrote a piece titled "What is Information Security?" together with my then ISG colleague Martin Albrecht. There, we set out our ambition to bring ethnography and cryptography into conversation through research with and within protest settings. At the time, we had only done a small pilot study with Anti-Extradition Law Amendment Bill (Anti-ELAB) protesters in Hong Kong. Yet, this work showed us that the security notions of the participants in these protests differed from those in the cryptographic literature.

The obvious connection between cryptography and ethnography (at least to us) is social relations. That is, while the immediate objects of cryptography are not social relations, it presumes and models them. Ethnography, on the other hand, studies social relations within their distinct social contexts.

Now the Engineering and Physical Sciences Research Council (EPSRC) has decided to fund our three-year research project on the Social Foundations of Cryptography, which we kicked off in January 2024. [1] The project is a collaboration between cryptographers Martin Albrecht (King's College London) and Ben Dowling (Sheffield University), and ethnographers Andrea Medrado (University of Westminster) and me. We will also soon be expanding our team with two postdocs and two PhD researchers.

So, I thought I would use this year's newsletter to say a little bit about this project and what excites me about it – from the perspective of ethnography. Fundamental to our project is that we are asking ethnography and cryptography to inform and transform each other. This moves beyond the typical interaction between the social and computer sciences (at least in the area of information security that I work in) that focuses on their 'applied' sub-fields. Here, technological solutions are often 'only' examined at the application stage, while fundamental design decisions are frequently left largely unchallenged. The premise of our project, however, is that by allowing social science to interrogate established assumptions and norms in computer science, we can unlock innovation in the latter. We therefore ask ethnography to pose, and expose, foundational questions about cryptography itself, not simply about its applications.

The core research aim of our project is to ground cryptographic security notions in findings produced through extended ethnographic fieldwork within a diversity of protest and activist settings. Concretely, we will be conducting extensive ethnographic fieldwork with participants in protests across multiple, international sites to establish how security is perceived, experienced, augmented and resisted among the groups under study. We will use what we learn from the ethnographic work to ask whether the security technologies that protesters and activists rely upon for their protection do indeed protect them, cryptographically speaking, as well as meet their needs and desires. We will also use what we learn from this work to critically evaluate the core assumptions relied upon in the mainstream cryptographic literature.

Now, why bother doing actual ethnography when there is a long history of information-security research that has relied on social science methods such as interviews and questionnaires to work out what people think about security and how they practice it; or when 'rapid ethnography', where the ethnography is limited to short-term participant observation most often in organisational settings, has successfully established itself in some branches of technology research? Indeed, such approaches would be much less time-consuming and, in many ways, more straightforward to put into action. However, for our project, they also fall short.

First, asking people about (their) security is distinctly different to experiencing and observing, through immersion in their lived environment and context, how they practice security and situate it within their daily social relations and interactions over extended periods of time. In other words, an ethnographic approach does not explore information security in isolation, but grounds it in its social reality. As Herbert told us decades ago, ethnography allows us to examine that which the groups under study take for granted and thereby revealing "the knowledge and meaning structures that provide the blueprint for action". [2] Put differently, ethnography allows us to learn that which people do not consciously reflect upon themselves. For this, 'rapid' approaches do not suffice.

The exploratory nature of ethnography, grounded in fieldwork with and within the groups it aims to understand, is a key enabler in unlocking information security needs and practices as they transpire in people's everyday lives. So I would argue at least. For the Social Foundations of Cryptography project, ethnography enables extended explorations of, for example, what security looks and feels like for the groups under study; how security is experienced and voiced and how it is negotiated and shared between protesters; how security technology is used within activist groups and for what purposes as well as what security expectations are held within such groups and how they manifest in daily activities. Ethnography further allows us to explore and understand the contextual structures and dynamics that govern and influence information-security practices, facilitating a more comprehensive analysis of such practices as well as the security-related concerns and needs of the groups under study. This helps ground security notions in the actual (observed) experiences of people, over extended periods of time, rather than in how people articulate security practices, concerns and desires through, say, interviews, when prompted.

[1] https://social-foundations-of-cryptography.gitlab.io/about
[2] Steve Herbert. For ethnography. Progress in Human Geography, 24(4):550–568, 2000.

CYFER ART-SCIENCE EXHIBITION: A CREATIVE KNOWLEDGE COMMUNICATION RESPONSE TO THE SCIENCE OF CYBERSECURITY AND PRIVACY OF FEMALE-ORIENTED TECHNOLOGIES
— Maryam Mehrnezhad

> Dr & Senior Lecturer, ISG

Female-oriented technologies (FemTech) promise to enable women to take control of their bodies and lives, helping them overcome the many existing challenges in medical care and research. The market is growing fast (predicted to be over $75 billion by 2025). This industry offers a wide range of solutions, including mobile apps, IoT devices and online services covering menstruation, menopause, fertility, pregnancy, nursing, sexual wellness, reproductive health care, etc. The class of technologies is broad, ranging from stand-alone mobile menstruation apps to illness-tracking wearables and IVF services on the blockchain. Despite their growth, their potential risks and harms to citizens remain an understudied phenomenon.

In 2021, I was awarded the CyFer grant by EPSRC PETRAS (National Centre of Excellence for IoT Systems Cybersecurity). I have been working with a fantastic team exploring cyber-security, privacy, bias and trust in FemTech. We have published over ten papers including system studies [1], user studies [2], fairness auditing in ML algorithms [3], and regulations [4].

Our work in CyFer is not limited to writing and publishing academic papers. In 2022, we invited artists, designers and creative technologists and commissioned five teams competitively from an open call. The core members of the team included Joe Bourne (PETRAS), Dr Teresa Almeida (Umea Sweden), Dr Ehsan Toreini (Surrey, UK) and myself. We worked with these artists, designers, technologists, members of the CyFer project, EPSRC PETRAS team, members of EPSRC NCSC RISCS, the RHUL Cultural team, and the Gender Institute and delivered this exhibition in 2023. We estimate that around 4000 people have visited this exhibition during its three months at RHUL (Egham campus). These top-notch art pieces also made an appearance at Mozilla MozFest in March 2023, and a number of them went to the V&A Museum in London in Sep 2023. Some of these works have also featured internationally, e.g., in Urban Screens, Sydney, Australia and a podcast channel based in the Netherlands.

These works include:

//

Moon Tapestry (Althea Rao, University of Washington, USA)

Moon Tapestry is possibly the world's most idiosyncratic and inefficient menstrual cycle tracker NOT powered by Artificial Intelligence. Its small-but-mighty memory will proudly remember only 28-days of your basal body temperature, which you will measure and input every day.

//

The Menstrual Data Co-op (Elena Falamo, freelance designer, between London, Berlin, and Italy)

The Menstrual Data Co–op is a (for now) fictional data cooperative: a group of individuals who jointly own their menstrual and fertility data and through equitable processes control its share and use.

//

User 59899 (Nadia Campo Woytuk (KTH Royal Institute of Technology, Germany) and Nicolas Harrand (RISE Research Institute of Sweden)

User 59899 is an exploration of what it means to make different layers of intimate data physical, all of which has been collected by Menstruation Apps. This includes the data we know we are sharing, to more obscure data. Three striking wall hangings explore the permanence of this disembodied data and the power individuals have over its creation and destruction.

//

Secret Keeper (Sian Fan, interdisciplinary artist, between Essex and London)

These are retro-futuristic-pseudo-spiritual video sculptures inspired by anime, 90s electronics and optimistic futures, which explore the tension between the vulnerability of scientifically defined trust and the resolution of spiritual belief.

//

The Quipu Kit (Vasiliki Tsaknaki and Lara Reime, IT University of Copenhagen, Denmark)

The Quipu kit invites participants to engage with their experiences of privacy and trust in relation to menstruation and fertility tracking applications through the tangible and material processes of knotting data.

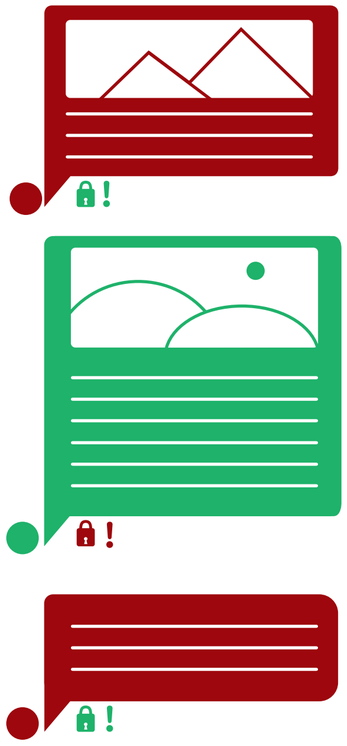
//

We received inspiring and appreciative feedback, including the following examples illustrating the general public understanding of the importance of this research topic: "shocking to see how much data is collected from such simple harmless-looking apps", "insightful, thought-provoking, thinking about my own intimate data", "…will look into the privacy policies [of period-tracking apps]", and "this niche exhibition is fascinating and deserves to go to the United Nations Museum for global impact."

Given the very positive reaction it received, this exhibition is now permanently archived (360 tour) on the RHUL website allowing the world to visit it: https://royalhollowayartarchives.viewin360.co/share/collection/7Jnt3?logo=0&info=0&fs=1&vr=1&sd=1&initload=0&thumbs=1tour

For details of these artworks please visit: https://petras-iot.org/update/artistic-exhibition-by-the-petras-cyfer-project-meet-the-artists-and-designers/ and https://sites.google.com/view/maryammjd/cyfer-project

References
[1] Mehrnezhad, Shipp, Almeida, Toreini. "Vision: Too Little too Late? Do the Risks of FemTech already Outweigh the Benefits?." Proceedings of the 2022 European Symposium on Usable Security. ACM, 2022.
[2] Mehrnezhad, and Almeida. "" My sex-related data is more sensitive than my financial data and I want the same level of security and privacy": User Risk Perceptions and Protective Actions in Female-oriented Technologies." The European Symposium on Usable Security, ACM, 2023
[3] Toreini, Mehrnezhad, and van Moorsel. "Fairness as a Service (FaaS): verifiable and privacy-preserving fairness auditing of machine learning systems." International Journal of Information Security (2023): 1-17.
[4] Mehrnezhad, van der Merwe, Catt, Mind the FemTech Gap: Regulation Failings and Exploitative Systems, Journal of Frontiers in IoT, 2024, earlier version at: Privacy Engineering in Practice (PEP), Symposium on Usable Privacy and Security Workshop, 2023



THE STANDARDISATION OF SECURE GROUP MESSAGING
— Yiannis Tselekounis

> Lecturer, ISG

End-to-end encrypted secure messaging (SM) is a widely used class of cryptographic protocols that allow groups of clients to communicate securely over untrusted network and server infrastructure. They provide the strongest possible security guarantees by preventing potential eavesdroppers – including telecommunication and Internet providers, malicious actors, and even the provider of the communication service – from being able to access, or even modify, the transmitted messages. The design of SM protocols is a challenging task as they are used for settings in which messages are exchanged asynchronously and sessions exist for long periods of time (e.g., for years). Consequently, participants can be offline at times, and their state is more likely to be exposed at some point during the lifetime of a session. SM protocols are therefore expected to satisfy so-called forward secrecy (FS) and post-compromise security (PCS). The former means that even when a participant's private key material is compromised, past messages (delivered before the compromise) remain secure. Conversely, PCS means that, once the compromise ends, the participants will eventually recover full security as a side-effect of continued normal protocol usage.

The rigorous design and analysis o" two-party SM protocols has received considerable attention in recent years. This is in no small part due to the advent of the double ratchet paradigm, introduced by Marlinspike and Perrin [1]. Forming the cryptographic core of a slew of popular messaging applications, including Signal, who first introduced it, as well as WhatsApp, Facebook Messenger, Skype, Google Allo, and Wire, double ratchet protocols are now regularly used by over a billion people worldwide. However, double ratchet protocols are inherently designed for the case where only two users communicate with each other; in order to employ them for groups with more than two users, there is little or no alternative to running double ratchets between all pairs of users, resulting in protocols in which the communication complexity of updating key material (an operation crucial to providing PCS) grows linearly in the group size, and this is undesirable for large groups.

In order to address the lack of satisfactory SGM protocols, the Internet Engineering Task Force (IETF) has launched the message-layer security (MLS) working group, which aims to standardise an eponymous SGM protocol. Following in the footsteps of the double ratchet, the MLS protocol promises to be widely deployed and heavily used. Indeed, the working group already includes messaging companies, including Cisco, Facebook, Google, Wickr, Wire, and Twitter, whose combined messaging user base includes everything from government agencies, political organisations, and NGOs to companies both large and small—not to mention a major chunk of the world's consumer population. Although MLS provides a rigorous protocol specification, it provides no formal security guarantees of the proposed protocol, and potential security flaws will have devastating consequences to the privacy of users.

In a series of papers [2, 3, 4, 5], we initiated the study of continuous group key agreement (CGKA) as a core primitive for secure group messaging, and we have tackled the challenging task of analysing the security of, and presenting improvements to, the IETF proposal for a secure group messaging (SGM) standard; this is vital given it will almost certainly be used by billions of users worldwide. The main challenge behind this problem stems from the fact that SGM protocols are highly complex, supporting large groups of thousands of users, and support a variety of operations, such as addition and removal of users and updating user states, where the latter can be corrupted at any time during protocol execution. Analysing security in this setting requires highly non-trivial cryptographic techniques and tools.

Two papers from 2020 [2, 3], are the first that formally study the security of the IETF proposal and define CGKA as its core component, including identifying several weaknesses and proposing fixes. At a high level, CGKA enables a dynamic group of users to periodically update group secrets, which are then used by the higher level messaging protocol to securely exchange messages. Our fixes resulted in a CGKA protocol that achieves optimal security. In [4], we modularised and generalised the core SGM design to present a practical, full protocol for SGM. Our results are based on a collection of new techniques, primitives and results, with applications beyond SGM. Finally, in [5], we paved the way to practical and scalable over unreliable networks by introducing the notion of fork-resilient CGKA, that allows clients to process significantly more types of out-of-order network traffic. Briefly, a network fork occurs when clients in a group have diverging views of the group's event history, e.g., due to network links going down for a period of time. Once connectivity is restored, the fork resolution method must provide a way for clients to reconcile their divergent views in order to agree on a new group state from which to proceed.

Improving the security of messaging protocols and applications is an important and exciting research area! If you are interested do please get in touch!

References
[1] M. Marlinspike and T. Perrin, "The double ratchet algorithm," 2016. https://whispersystems.org/docs/specifications/doubleratchet/doubleratchet.pdf.
[2] J. Alwen, S. Coretti, Y. Dodis, and Y. Tselekounis, "Security analysis and improvements for the ietf mls standard for group messaging," in IACR CRYPTO 2020.
[3] J. Alwen, S. Coretti, Y. Dodis, and Y. Tselekounis, "Security analysis and improvements for the ietf mls standard for group messaging," in Real World Crypto, 2020.
[4] J. Alwen, S. Coretti, Y. Dodis, and Y. Tselekounis, "Modular design of secure group messaging protocols and the security of mls," in ACM SIGSAC CCS 2021.
[5] J. Alwen, M. Mularczyk, and Y. Tselekounis, "Fork-resilient continuous group key agreement," in Advances in Cryptology – CRYPTO 2023.

SEDARC: SOUTH EAST DOCTORAL TRAINING ARC

— Andrew Dwyer
— Rikke Bjerg Jensen

> Lecturer, ISG
> Reader, ISG

In 2023, Royal Holloway was awarded a Doctoral Training Partnership (DTP) from the Economic and Social Research Council (ESRC), which will offer 39 PhD studentships for social-science led research each year for the next five years. The South East Doctoral Training Arc – or SEDarc – is led by Royal Holloway, but brings together six academic institutions. The other consortium members are the University of Kent, Kingston University, University of Reading, University of Surrey and the University of Sussex.

This award is demonstrative of Royal Holloway's commitment to training the next generation of researchers, not least at a time when PhD funding is increasingly hard to secure. For the ISG, it is especially exciting since we are one of seven Royal Holloway departments eligible for social science-led funding through SEDarc. This is a recognition of the excellence of socially-driven research in the ISG for over a decade; a development that started long before either of us joined the department. SEDarc is structured around five cross-disciplinary themes that run across the social sciences. [1] Two of these themes are especially relevant – and exciting – to those of us researching the social foundations and societal implications of information security: Secure, Effective and Trusted Organisations; and Transformative Technologies for Society. While the former is grounded in, for example, geopolitical currents and institutional structures and dynamics, the latter brings to the fore the socio-economic foundations of cyber security and the societal implications of transformative technologies.

Such themes also speak to our own heritage in PhD training. For more than a decade, the ISG has hosted consecutive Centres for Doctoral Training (CDT) focused on cyber security. Here, we have recruited more than 100 PhD researchers from across the social and technical sciences to conduct research at the intersections of their respective fields. These PhD researchers are now engaged in cutting-edge thinking and practice across academia, industry, and governments internationally. More information and detail about the consortium's unique doctoral programme (focusing on quantitative research training, generating research impact, and non-academic careers) as well as the application process are set out on the SEDarc website, [2] which also highlights its vision:

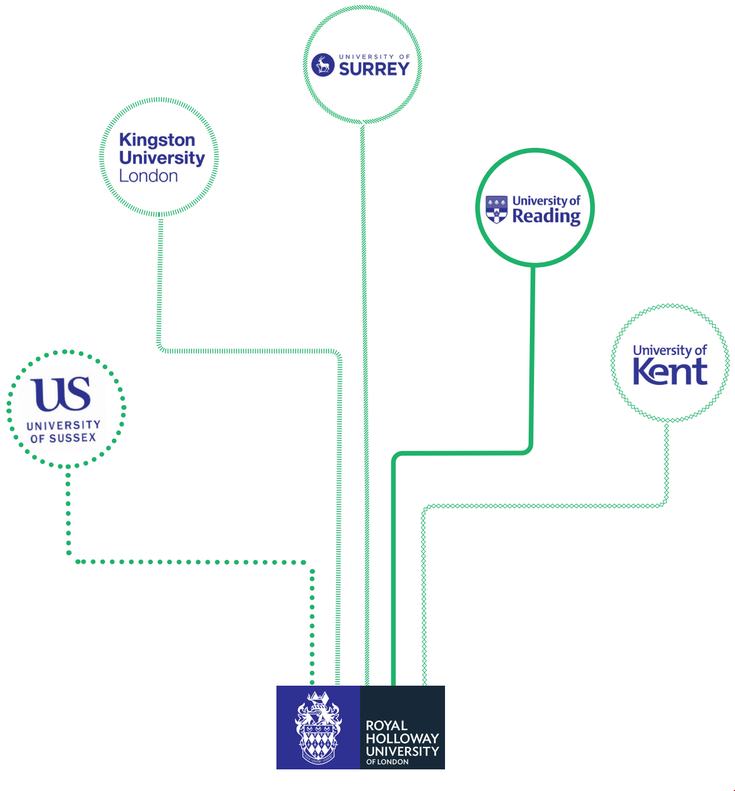
" to develop world-class social science researchers from all backgrounds who thrive in challenge-led, collaborative, and interdisciplinary contexts. It offers a transformative approach to PhD studies that combines a cutting-edge doctoral training, job placements outside academia, and an individual research project based in one of five interdisciplinary, challenge-led pathways."

We're excited to welcome the first cohort of SEDarc PhDs in September 2024. Through SEDarc, the ISG will continue to support emerging researchers engaged in novel socially-driven research across information security. If you, or someone you know, would be interested in finding out more, please do get in touch with our SEDarc DTP lead, Andrew Dwyer.

References

[1] https://www.royalholloway.ac.uk/media/27246/sedarc-themes.docx

[2] https://www.royalholloway.ac.uk/studying-here/fees-and-funding/research-degrees/sources-of-funding/sedarc/



ONLINE HATE AGAINST WOMEN AND GIRLS ON 4CHAN

— Adrian Bermudez-Villalva

> Research Fellow, ISG

Online hate speech, particularly against women and girls, is a widespread problem affecting various online spaces, including social media and other platforms such as 4chan. 4chan, known for its anonymity and minimal moderation, was launched in 2003. Previous research shows that this platform has been a breeding ground for misogynistic and hateful content [1]. This environment not only perpetuates gender-based discrimination but also poses significant cybersecurity threats, including cyberstalking, doxing, and coordinated harassment campaigns. Addressing this issue requires a multifaceted approach that encompasses technological, legal, and educational strategies. 4chan is structured as an imageboard where users can post anonymously, a feature that encourages individuals to share content without accountability. This anonymity, while a cornerstone of the platform's culture, facilitates a space where hate speech can thrive, often targeting women. The content ranges from sexist remarks to explicit threats of violence, creating an unsafe environment that extends beyond the digital realm.

The cybersecurity threats associated with this hate speech are substantial. Victims of online hate and harassment may experience unauthorised distribution of personal information, cyberstalking, and even physical threats. These actions can lead to psychological trauma, damage to one's reputation, and a significant impact on personal and professional life.
AGENCY is a £3.5 million project awarded by the UKRI EPSRC. It is a multidisciplinary collaborative project involving Birmingham, Newcastle, Durham, KCL, Surrey, and RHUL. As a part of this project, Dr Adrian Bermudez-Villalva (Research Fellow, ISG), Dr Maryam Mehrnezhad (also from the ISG), and Dr Ehsan Toreini (University of Surrey) are exploring the issue of online hate against women and girls on the "politically incorrect" (/pol/) board on 4chan. The /pol/ board stands out for its focus on political discussions. It has gained notoriety for hosting controversial and polarising conversations, often marked by the presence of hate speech, discrimination, and misogyny against various groups, including women and girls [2].

We are analysing posts from the /pol/ board to measure the prevalence of online hate against women and girls. To achieve this, we are using the 4chan API to systematically collect data, developing a comprehensive dataset comprising posts submitted by users on this specific board. This dataset serves as the foundation for our investigation, enabling us to employ advanced Natural Language Processing (NLP) techniques to detect, quantify, and understand instances of hate speech within this online community.
The application of NLP techniques involves an analysis that not only identifies explicit instances of hate but also uncovers the subtler, nuanced expressions of animosity or bias based on gender. Through the application of topic modelling, we are delving deeper into the dataset to discover hidden semantic patterns. This technique allows us to automatically identify topics prevalent within our text corpus, with a special focus on those related to women. We are also conducting a semantic analysis to explore the specific themes, contexts, and levels of toxicity present in these discussions. Such an analysis not only has the potential to reveal the prevalence of hate speech but also helps us understand the nuanced ways in which it manifests on the /pol/ board.

Our research involves a rigorous quantitative analysis to measure the extent of online hate against women and girls on 4chan. By quantifying instances of hate speech, we aim to provide empirical evidence that sheds light on the scale of the problem. This comprehensive approach, combining the collection of data using the 4chan API, the use of NLP techniques for detection and analysis, and quantitative methods to measure prevalence, will offer valuable insights into the dynamics of gender-based online hate on the /pol/ board. Through this research, we hope to contribute to the broader understanding of online hate speech and inform strategies for its mitigation.

One approach to mitigating online hate involves re-evaluating the moderation policies and the extent of user anonymity on online spaces such as social media or forums. Implementing more stringent moderation tools powered by artificial intelligence (AI) on these platforms can help identify and remove hate speech more efficiently. While this may raise concerns about censorship, creating a balance that protects users from harm while preserving freedom of expression is crucial. Furthermore, imposing certain limitations on anonymity, such as requiring user verification for posting, could deter individuals from engaging in hate speech. While this might not be possible on 4chan due to its nature, our research can shed light on how online hate spreads in the wild.

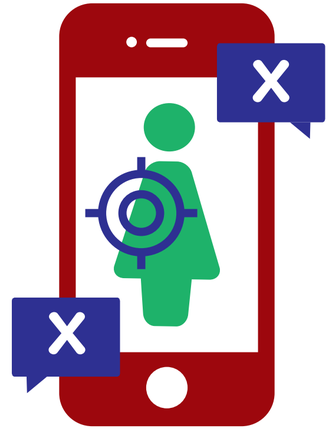
At the same time, strengthening legal frameworks at both national and international levels is essential for combating online hate. Laws that specifically address cyber harassment and doxing need to be enforced rigorously, with platforms like 4chan held accountable for failing to address hate speech adequately. Collaboration between law enforcement and cybersecurity experts is vital to trace and prosecute individuals who engage in illegal activities online. Further, addressing the root causes of online hate requires community engagement and education. Online spaces could implement initiatives to foster a culture of respect and empathy among users. Educational campaigns that highlight the impact of hate speech on individuals and communities can contribute to a shift in attitudes. Additionally, providing support and resources for victims of online hate is crucial for their recovery and empowerment.

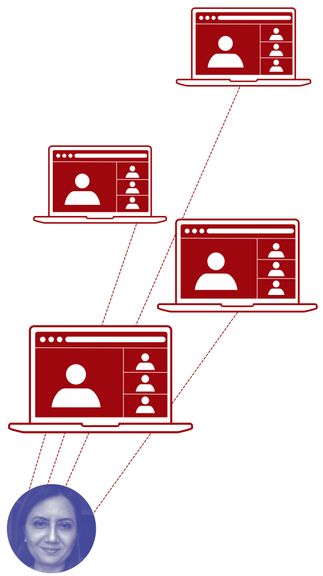
The issue of online hate against women and girls on 4chan is a complex problem that intersects with cybersecurity, legal, and social domains. Tackling this issue requires a comprehensive strategy that includes enhancing moderation, implementing technological solutions, enforcing legal frameworks, and promoting community engagement and education. By addressing the cybersecurity aspects of online hate, we can take significant steps towards creating a safer and more inclusive digital environment for all users, particularly for women and girls who are disproportionately targeted.

References

[1] Frenda, S., Ghanem, B., Montes-y-Gómez, M., & Rosso, P. (2019). Online hate speech against women: Automatic identification of misogyny and sexism on Twitter. Journal of Intelligent & Fuzzy Systems, 36(5), 4743-4752.

[2] Papasavva, A., Zannettou, S., De Cristofaro, E., Stringhini, G., & Blackburn, J. (2020, May). Raiders of the lost kek: 3.5 years of augmented 4chan posts from the politically incorrect board. In Proceedings of the International AAAI Conference on Web and Social Media (Vol. 14, pp. 885-894).





DISTANCE LEARNING MSC IN CYBER SECURITY – AN UPDATE

— Fauzia Idrees Abro

> MSc Course Director & Senior Lecturer, ISG

//

Introduction

In October 2022, the ISG launched the Distance Learning (DL) Cyber Security MSc Programme in partnership with the University of London (UoL). The programme benefits from UoL's global reach, an innovative online learning platform designed by Coursera, and Royal Holloway's academic leadership.
The Cyber Security programme currently awards three qualifications:

- Master of Science (MSc) in Cyber Security;
- Postgraduate Diploma (PGDip) in Cyber Security;
- Postgraduate Certificate (PGCert) in Cyber Security.

The MSc in Cyber Security is a two-year programme and has two intakes a year – in October and April. The programme has been developed with the help of industry experts to align with current market demands and meet the expectations of students preparing for employment after completing the programme. Some of our module leaders are also industry experts. There is a good balance of theoretical knowledge and practical skills, which are essential for the cybersecurity job market. It covers both technical and non-technical aspects of cybersecurity, such as legal and regulatory considerations, human factors, and configuring networks and applications to safeguard the cyberspace.

There are four study sessions per year, each lasting 10 weeks, starting in October, January, April and July. The MSc involves ten compulsory taught modules and a research project.

The taught modules are as follows:

1. Cyber security foundations;
2. Applied cryptography;
3. Network and infrastructure security;
4. Computer systems security;
5. Security management and governance;
6. Cybercrime;
7. Software and application security;
8. Research methods for cyber security;
9. Information privacy;
10. Security and behaviour change.

Each module consists of online video lectures, interactive activities, peer review assessments, live webinars, quizzes, and a final summative assessment. Additionally, students have the option to interact with each other and the academic staff through group discussion forums and live webinars on Coursera. They can also engage in discussions through an informal Stack channel exclusively for students, which is not accessible to academic staff. In parallel with the ten MSc modules, we are also delivering six Massive Online Open Courses (MOOCs) along with a 'specialisation' in Cyber Security. These courses are currently running on Coursera and are available to take free of charge. The six MOOCs are:

i. MOOC1: An introduction to Cyber Security;
ii. MOOC2: Introduction to Applied Cryptography;
iii. MOOC3: Introduction to Computer Security;
iv. MOOC4: Introduction to Network Security;
v. MOOC5: Security Management and Governance; and
vi. MOOC6: Cybercrime.

The specialisation requires students to take MOOCs 3-6.

//

Current Status

During our first intake in October 2022, we launched the first two modules: CYM010 Cyber Security Foundations and CYM040 Applied Cryptography. Following this, in January 2023, we expanded our offerings with two additional modules: CYM050 Network & Infrastructure Security and CYM060 Computer Systems Security. Our second intake in April 2023 saw the introduction of CYM020 Cyber Security Management and Governance, alongside a revised version of CYM010. Subsequently, in July last year, we released CYM030, marking our commitment to ongoing module development. For our third intake in October 2023, we again re-issued CYM010 and CYM040, along with the introduction of CYM100 Research Methods. In January this year, we revised CYM050 and CYM060 and released them alongside a new module: CYM070 Software and Application Security.

Looking ahead to our fourth intake in April 2024, we're excited to unveil two of the final three modules: CYM090 Information Privacy and CYM500 Project, alongside CYM010 and CYM020. The very final module CYM080 Security Behaviours will be released as scheduled in July 2024, marking the completion of the module development phase, in line with the agreed plan between UoL and RHUL. Throughout this journey, we've continually refined our modules to meet the evolving demands of the rapidly growing cyber security market.

The programme has attracted many applications in all three intakes, and recruitment has significantly exceeded projections; the number of registered students less than two years after launch is double that anticipated. Our first ever MOOC, Introduction to Cyber Security, launched in June last year, has attracted around 16,000 learners from around the globe and has been rated as the most popular new open course on Coursera's platform.

//

Comparative Analysis

Compared to our previous distance learning programme, the MSc Cyber Security programme offers increased flexibility in terms of registration with two intakes and four study sessions per year (rather than a single yearly study session). These multiple sessions also allow for the opportunity for students to resit assessments within the same year, rather than having to wait until the assessment period of the following year. As previously, all assessments are fully online, with no requirement to travel to campuses or exam centres.

Also introduced on this programme is the option for applicants who do not meet the standard entrance requirements to register via a 'performance-based admission' route through which they initially only register on two modules; once they have been passed students can then progress onto the full MSc degree. Alternatively, if applicants do not wish to sign up for the full MSc degree programme, there are also PG Certificate, PG Diploma and Individual Module options available.

As with our previous distance learning programme, students can pay for the degree up-front, or pay yearly on a 'pay as you go' basis. However, an additional new feature of this programme is a reduced fee option for students in designated 'Band A' countries: https://www.london.ac.uk/sites/default/files/leaflets/country-bands.pdf

An interesting feature resulting from our partnership with Coursera is the provision of MOOCs in addition to the regular modules that comprise the degree programme. The six Cyber Security MOOCs allow potential students to sample aspects of full modules for free or, for a small fee, to receive an online certificate per MOOC upon completion of an assessment activity. What makes this programme unique is the integration of hands-on activities on the state-of-the-art Cyber Range platform. The platform is integrated with software tools and resources required to launch different cyber scenarios. Cyber Range scenarios immerse students in realistic situations simulating cyber-attacks, providing them with hands-on experience in responding to threats as they would encounter in real life. By replicating authentic cyber threats and challenges, Cyber Range offers students a practical environment to develop critical skills in identifying, mitigating, and recovering from cyber-attacks. Cyber Range also provides students with an opportunity to work collaboratively as a team to defend cyberspace in this borderless world.

//

Conclusions

Currently, Royal Holloway runs four distance learning programmes, among which the MSc Cyber Security garners the highest number of applications per intake. To our knowledge, the programme is the first DL MSc in Cybersecurity to use Cyber Range, providing students with a realistic experience of cyber-attacks. With our dedicated specialist staff and demand that exceeds expectations, the programme has incredible potential. Recently, the programme received commendation for the UoL Roger Mills Prize for innovation in learning and teaching. The Prize panel noted: 'An exciting application that clearly demonstrates innovative use of technology and the strength of the partnership between Royal Holloway, University of London and the University of Lonon teams. The panel were impressed by the use of hands-on labs and simulations, and the clear focus on skills for the workforce that together lead to an engaging student experience. The opportunities for collaboration in the cyber threat activities are exciting and aim to support the diversity of the student population well.'

THE INTERNATIONAL CYBERSECURITY CENTER OF EXCELLENCE A GLOBAL COMMUNITY

— Konstantinos Mersinas

> Senior Lecturer, ISG

The International Cyber Security Center of Excellence (INCS-CoE) – see https://incs-coe.org/ – serves as an umbrella organisation to foster research, policy, and education in cyber security, through synergies between government, industry, and academia. The Centre has grown and expanded to become a truly global community of security experts. From the initial three founding countries and six Founding Universities: Royal Holloway (UK), Imperial College London (UK), Keio University (Japan), Kyushu University (Japan), UMBC (USA) and Northeastern University (USA), the Centre now consists of 13 universities from the UK, US, Japan, France, Israel, and Australia. We recently welcomed Virginia Tech (US) as the most recent member institution. I have the honour of being the Royal Holloway board member, having succeeded Prof Keith Mayes, the former ISG Director.

An established annual activity of INCS-CoE is the Country-to-Country Capture-The-Flag (C2C CTF) event. The 2023 competition was hosted at Keio University, Tokyo, with 78 students participating from 43 universities, forming 16 teams and representing 20 nationalities, participating in the final round in person in Japan. The event was funded by nine corporate sponsors. Similar levels of participation are expected in the 2024 competition, which will be hosted by Edith Cowan University in Australia. Royal Holloway students have been a part of the top-performing teams during past competitions, and all levels of studies are represented, from bachelors to PhD. C2C CTF activities at RHUL are led by Dr Darren Hurley-Smith, with Dr Jassim Happa serving as a member of the organising committee.

The Centre promotes research activities via quarterly seminars and the collaborative creation of white papers on critical security topics, such as cyber security issues in transportation, the growing role of AI, and cybercrime and ransomware. Researchers from all member institutions are invited to join the activities. In 2024, we are continuing our efforts by utilising cross-country funding opportunities to foster collaborations and joint research projects amongst member institutions.

A NEW STRUCTURE FOR THE MSC IN INFORMATION SECURITY

— Saqib Kakvi

> Lecturer, ISG

The academic year 2023/24 saw a significant change in the structure of our flagship MSc in Information Security. As part of a university-wide initiative, all modules were redesigned to have a credit value equal to a multiple of 15, rather than the previous multiple of 20. We saw this as an opportunity to change the shape of the MSc based not only on our own insights, but also feedback from the students.

One of the key driving factors in the redesign was a transition to a single set of core modules for the course. Previously, students had to choose between either Core A, containing modules with more technical content, and Core B which was more focused on the business and operational aspects of security. The reasoning behind this structure was to cater to the diverse backgrounds of our students and to meet the needs of students with differing career goals in information security. Over time the cyber security landscape has significantly changed, and the distinction between technical and management aspects of information security has blurred and the need to understand both aspects have increased.

To address this, we examined the core modules and identified overlaps and potential synergies within our modules to define a new set of mandatory modules. The first change was to complement the security management module with new material on research methods, to enable our students to have the right tools for their projects from the very start. This forms our first mandatory module "Security Management and Methods".

We also examined the other modules in Core A and Core B, and the module leaders spent many hours not only identifying the overlaps and intersections of material, but also what they felt were the fundamental aspects of security.
The result was a modification of the previous Security Technologies module which was combined with the Introduction to Cryptography module to give us our second mandatory module "Cryptography and Security Mechanisms". The remaining technical aspects from the Core A modules were then combined to make a new optional module "Fundamentals of Computer Security", and the second Core B module "Secure Business Architecture" also became an optional module. The result of this is that students can now study all of what was covered by both Core A and Core B if they so choose.

In a similar vein to the mandatory modules, we realised that our students would benefit from a broader perspective and knowledge of information security. We therefore decided to change our optional module requirements to have the students take four modules of 15 credits each as opposed to the previous two modules of 20 credits each. We believe that this will allow students to explore more aspects of information security and increase their employability and understanding of the subject as a whole.

These structural modifications are not the only changes. We are also introducing new optional modules to cover emerging areas of information security. The first of these modules "Usable Privacy and Security" ran this year and we are very pleased with the results. We have detailed plans to roll out further new modules in the coming years, and we are always updating and refreshing our modules to keep abreast with developments in the field.

THE ISG SMART CARD & IOT SECURITY CENTRE (SCC) 2024

— Konstantinos Markantonakis
— Darren Hurley-Smith
— Carlton Shepherd

> Professor, ISG & Director, SCC
> Dr & Lecturer, ISG, SCC
> Lecturer, Newcastle University

The Smart Card and IoT Security Centre is continuing its dedicated effort within the ISG to promote research excellence, commercialisation and impact, and student engagement activities. We continue to focus our research efforts on high profile challenge-led research with real world significance. Some highlights of our existing research efforts on the security interactions of hardware and software are presented below.

Besides solely executing programs and storing intermediate data, today's processors contain a wide variety of useful features for monitoring system features. Hardware performance counters (HPCs) are one such feature, enabling developers to take fine-grained measurements of programs under execution. On Intel CPUs there are dozens of such counters, covering how many cache hits occur, branches were taken, instructions were executed, and so on.

In our research [1], we took a comprehensive look at how HPCs could be used to uncover information about programs that developers intend to keep hidden. Specifically, we explore how they could be used to learn what functions are being performed in compiled libraries, e.g. dynamic link libraries (DLLs), and trusted execution environments (TEEs). We found that many such functions can be identified with high accuracy (86.22–99.83%) under a range of assumptions. In July 2023, our findings were published in IEEE Transactions on Computers [1], the premier journal on computer architecture.

In parallel with the above, we have also been examining how mobile devices collect sensor data and provide them to applications. In particular, are these procedures secure? This question is behind our recent research work. We found that Google and the Android Open Source Project (AOSP) made some key security oversights, after painstakingly analysing the Android documentation on low-level sensor multiplexing (not the best bedtime reading). In particular, we found that applications could request sensors to return data at a certain sampling rate. When some applications requested faster rates than others, the fastest rate was returned to all applications in a deterministic fashion. Using this knowledge, we constructed two attacks: (1) developing a new covert channel enabling unprivileged Android applications to send data that bypasses existing security controls, e.g. the permissions system; and (2) fingerprinting applications that use sensor data, such as mobile games and fitness applications. Our findings affect all known Android devices globally. Our findings affect all known Android devices globally and they were reported to and acknowledged by Google and the AOSP for which a bug bounty was offered (we declined; the bounty was given to charity). The work was recently published in IEEE Transactions on Dependable and Secure Computing (TDSC) [2].

Amir Rafi, one of the PhD students and a member of the SCC lab, recently published a paper on the security analysis of Digital Rights Management (DRM) solutions, which was presented at the IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). The current DRM landscape includes a range of proprietary solutions, causing a fragmentation in the industry; content providers are thereby compelled to implement multiple DRM systems to support multiple platforms. Today's mobile platforms are shipped with proprietary DRM systems integrated into the application or operating system itself, such as Android (Widevine), iOS (FairPlay), and Microsoft Windows (PlayReady). Android and iOS have a global OS market share of 72.11% and 27.22% respectively for mobiles; 47.54% and 52.38% respectively for tablets; and Windows OS is used on 76.31% of desktops [3]. Widevine for instance, is available on 5 billion devices worldwide. Amir's paper presents the first domain-specific security evaluation of mobile-based DRM systems, including Google Widevine, Apple FairPlay, and Microsoft PlayReady. The paper derives a taxonomy of security features for underpinning the security of an end-to-end DRM system (comprising client and server) and also defines the evaluation criteria required to conduct this security analysis. Based on a comprehensive analysis of public domain material, this work identifies probable attack vectors and presents a comparative security analysis of Widevine, FairPlay and PlayReady DRM systems. The security analysis discovered several vulnerabilities in these DRM systems; mitigations for these vulnerabilities were discussed in the paper, which also suggests future directions for research.

The SCC continues to pursue competitive funding opportunities. We have submitted a Horizon proposal focusing on automotive security (that is currently under review), leveraging our Trusted Execution Environment (TEE) expertise and our excellent hardware resources, including the PIXKIT car development kit. The proposal aims to address significant privacy issues and auditing challenges in the automotive industry.

Our accumulated expertise on Trusted Execution Environments has enabled us to complete a monograph that is currently in the final stages of review by Springer, to be published by June 2024. The book explores 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.

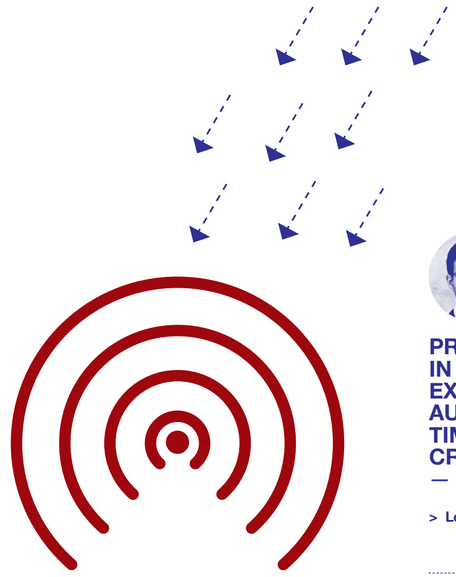
Following the spinout success of our "Seclea" project we are in the process of exploring commercialisation and funding opportunities for our "TensorCrypt" project, which was also a finalist in the Innovate UK CyberASAP programme. Our effort is supported by a proof-of-concept that was successfully engineered and provided employment for three RHUL undergraduates. TensorCrypt contributes to the Authentication, Authorisation & Accountability, Risk Management & Governance and Hardware Security CyBOK technical areas. Building on our experience in identifying and protecting intellectual property (IP), our effort is further supported by an awarded patent "A method and System for Securely Sharing data" International Application Number PCT/GB2022/053042, authored by two of us.

This academic year, the SCC is again providing first-hand experience of research and development at the highest level, by enabling undergraduate students to work with experienced researchers on real world problems related to cybersecurity and privacy. We advertised a range of challenge led research and commercialisation opportunities to first year UG CS and EE students, and we are really privileged that we will be collaborating with more than 10 students, in a number of key group and individual projects.

We hope that this short overview of our recent activities will excite your interest. Please contact us at k.markantonakis@rhul.ac.uk if you feel there are areas we could explore further together.

References

[1] Shepherd, C., Semal, B., & Markantonakis, K. (2022). Investigating Black-Box Function Recognition Using Hardware Performance Counters. IEEE Transactions on Computers, 1-14. https://doi.org/10.1109/TC.2022.3226302
[2] Shepherd, C., Kalbantner, J., Semal, B., & Markantonakis, K. (2023). A Side-channel Analysis of Sensor Multiplexing for Covert Channels and Application Fingerprinting on Mobile Devices. IEEE Transactions on Dependable and Secure Computing, 1-12. https://doi.org/10.1109/TDSC.2023.3323732
[3] Rafi, A., Shepherd, C., & Markantonakis, K. (2023). A First Look at Digital Rights Management Systems for Secure Mobile Content Delivery. 549-558. Paper presented at 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Exeter, United Kingdom. Advance online publication. https://doi.org/10.1109/TrustCom60117.2023.00087



PRIVACY VULNERABILITIES IN APPLE AIRDROP EXPLOITED BY CHINESE AUTHORITIES – FINALLY TIME TO DEPLOY PROPER CRYPTOGRAPHY?

— Christian Weinert

> Lecturer, ISG

AirDrop is a proprietary feature of Apple devices that allows users to conveniently share files with nearby iPhones, iPads, or MacBooks. It is based on a proprietary wireless direct link protocol and notably does not require an Internet connection for data transfers. Once an AirDrop transfer is completed, there is presumably no way to tell where the file was coming from. This has made the feature attractive for political activists in China to distribute government-critical content. However, as it turns out, AirDrop transfers are not as anonymous as they may seem, and, therefore, this poses severe privacy risks.

Recent news reports in January 2024 revealed that Chinese authorities have found a way to determine the phone numbers and email addresses of senders of "inappropriate information" distributed via AirDrop. For this, Chinese forensic experts claim to have analysed log files on the receivers' devices and applied techniques to "crack" cryptographic measures that are supposed to protect the senders' contact details.

This is not a big surprise for the research community. Already in 2019, a team from TU Darmstadt had found severe privacy vulnerabilities in the AirDrop protocol and reported them to Apple in a responsible disclosure procedure. I was part of that team and, clearly, the Chinese forensic experts exploited precisely the vulnerabilities that we reported to Apple. In fact, they even apply the same "cracking" strategy that we feared could be used.

The underlying issue is Apple's insecure use of cryptographic hash functions to obfuscate contact identifiers while the devices are running a mutual authentication protocol to try to figure out if they know each other. Cryptographic hash functions are supposed to produce irreversible, random-looking outputs. However, it is widely known among security researchers and practitioners that hashing is insufficient to protect personal information: with today's computing power, attackers can easily test all possible inputs to determine, for example, which phone number results in a given hash value.

Instead of a naïve brute-force attack as described above, the "cracking" method used by the Chinese laboratory relies on so-called rainbow tables. Rainbow tables are a well-known technique to achieve a time/memory trade-off for hash reversal: by pre-computing and storing relevant parts of hash chains, hash reversal can be significantly accelerated. Research done in a collaboration between Royal Holloway, TU Darmstadt, and the University of Würzburg has shown that for the special case of phone number hash reversal, the amortized attack run-time can be as little as 52ms (even without using a GPU for additional acceleration) – essentially allowing the results to be obtained in real time.

While the retention of hashed contact identifiers related to recent AirDrop transfers in log files is a new discovery by the Chinese forensic experts, it is trivial to reproduce. Apple's "sysdiagnose" feature allows anyone with access to an unlocked Apple device to trigger a procedure that will bundle a wide range of diagnostic information in an archive format that can easily be transferred to another device (ironically also via AirDrop itself) for later analysis.

Notably, the log files store only partial instead of full SHA-256 hash values (40 bit per hash to be precise). Applying hash reversal attacks on such partial hashes can result in finding a few collisions, meaning multiple phone numbers or email addresses that produce the same partial hash value.

Analysing device logs, unfortunately, is not the only way this design flaw can be exploited. Whenever an iPhone user opens the sharing pane on their device, anyone with a nearby Wi-Fi-enabled device can grab their hashed contact identifiers and then apply brute-force or other hash-reversal methods. This "sender leakage" happens because the sender will include their hashed contact identifiers in an initial discover message sent to all potential receivers.

A second, closely related vulnerability (dubbed "receiver leakage") occurs as potential receivers respond with all their hashed contact identifiers upon recognizing any of the sender's contact information from the initial discover message. Therefore, a malicious sender can covertly learn additional contact information (e.g., the private mobile phone number of the receiver) if the two parties already have some contact relationship, for example, if they have previously exchanged their business email addresses.

We not only identified, reported, and demonstrated these vulnerabilities, but also proposed a secure solution called PrivateDrop. It uses an alternative, provably secure cryptographic protocol for private set intersection to determine if two users know each other. As a result, even if the protocol messages are intercepted or retained in a device log, they would be of no use for forensic experts.

In a nutshell, the proposed PrivateDrop protocol produces encryptions of the contact identifiers of both parties under a random secret key; these encryptions can then be checked for equality. Instead of the assumed pre-image resistance of hash functions (which does not apply for low-entropy inputs), the security of PrivateDrop mainly relies on a variant of the well-known decisional Diffie-Hellman (DDH) assumption and ultimately on the assumed hardness of computing the discrete logarithm in cyclic groups – which is a fairly standard assumption in cryptography.

Whether Apple eventually decides to adopt a solution like PrivateDrop in future updates remains to be seen. We have implemented and benchmarked a PrivateDrop prototype, showing that it's a viable solution and would not cause noticeable performance delays. We hope that Apple takes the recent events as an opportunity to finally react and fix this long-standing issue by deploying proper cryptography.

WISDOM 2023-2024 ROUND-UP
— Rachel Player

> Lecturer ISG, Director Cryptography Group

It's now been almost eight 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. Since 2021-22, the group has expanded to welcome members from across EPMS, the school containing the Information Security and Mathematics Departments. Wisdom 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. This year, we have had several successful events and been glad to see a huge outreach effort come to fruition.

An important change this year is in the way we communicate with members. With the lists.rhul.ac.uk mailing lists having been retired, members can now enrol on our Moodle page to receive updates (the link is below, or the page can be found by searching "Wisdom" while logged into Moodle). This means it is now possible for anyone to register or deregister from receiving updates by themselves, which should be much more convenient!

We kicked off in October 2023 with a welcome event that enabled us to reconnect after the summer break and welcome new members to the group. This event was held jointly with the PGR café, which takes place weekly in the Bedford Building, and is an opportunity for staff and postgraduate researchers to chat over tea and sweet treats.

Next, we teamed up with the EPMS Reading Group and the Library to celebrate The Big Read initiative. This year, The Big Read was centred on Prof Hannah Fry's book "Hello World", and the event provided a great opportunity for us to reflect on the impact of AI, algorithms, and data.

Also in the autumn term, we held our traditional Halloween Bake Off event. This year, it was organised jointly with the Halloween social, where we enjoyed a spooky quiz and other food and drink, before sampling all the bakes! There were some exceptional entries this year, and I am already looking forward to the next edition.

A major effort over the past few years has been Wisdom's partnership with The Brilliant Club, initiated by previous Wisdom co-president Dr Catherine Keele. The Brilliant Club works with schools across the country to support less advantaged students to access university. Wisdom committee members Erin Hales and Emma Smith have created a new course for delivery through the Brilliant Club Scholars Programme. After months developing the course, in Autumn 2023, Erin trialled the delivery of the course in a school in Birmingham. Feedback from this trial version of the course will be used to finalise the course before it is rolled out to schools across the UK in Spring 2024. This was a huge effort for the Wisdom team, so congratulations to all involved, and our thanks to The Brilliant Club.

In February, Wisdom held a lunchtime pizza social. Members old and new were able to catch up after the winter break while enjoying pizza and soft drinks. In the photo I can be seen to be very pleased to be surrounded by so much pizza! (Photo credit: Sophie Hawkes. Photo description: Rachel stands behind a table with several pizza boxes, glasses, and soft drinks. Behind her the whiteboard reads 'Wisdom Pizza Social' with a drawing of a slice of pepperoni pizza.)

Looking ahead, in March 2024, we will be partnering with Women in STEM Society and the Lyell Geoscience Society to celebrate International Women's Day. The event will feature a panel discussion with speakers from across the STEM disciplines, followed by refreshments and networking. We are looking forward to working with other groups on campus with similar aims as ours, and hope that this can be the first of other joint events.

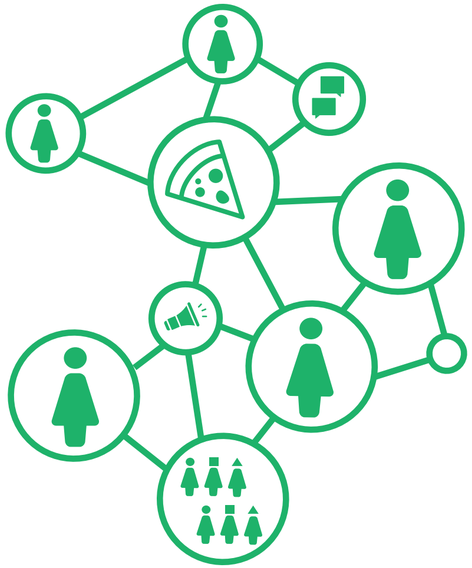
Some current Wisdom committee members will soon be completing their PhDs, and we wish them all the best for their future endeavours! Unfortunately, of the remaining committee, there is not currently the capacity to continue such an active programme of events and initiatives. We are therefore surveying members to determine the most impactful activities to focus on in the coming months. We are also very keen to hear from anyone who would like to join the committee!

If you'd like to know more about Wisdom, please enrol on our Moodle page, or follow us on social media where we share all the details of our upcoming events.

Get in touch with Wisdom:
wisdom@rhul.ac.uk

Enrol on the Wisdom Moodle page to receive updates:
https://moodle.royalholloway.ac.uk/course/view.php?id=23174

Follow Wisdom on social media:
https://twitter.com/WisdomRHUL
https://www.linkedin.com/groups/12047422/



THE ALL PARTY PARLIAMENTARY GROUP ON CYBER SECURITY
— Andrew Henderson

> Consultant, ISG

An All-Party Parliamentary Group (APPG) is an informal UK parliamentary group that is run according to rules laid down by Parliament. It is open to MPs and Peers from all political parties who attend its meetings. The purpose of the APPG on Cyber Security is to raise awareness in Parliament of issues relating to Cyber Security by providing a forum for briefings, debate and discussion. The group addresses developments in Cyber Security systems and techniques affecting consumers, businesses (including small business) and the role of cyber security in the smooth working of Defence, the UK economy and society as well as the Critical National Infrastructure. The group activity is applicable to, security, identity, regulation and fraud, and it provided information that promotes inclusion and understanding for non-specialists.

The ISG began sponsoring the APPG in 2016. The main purpose of this was to help raise awareness of the importance of cyber security as a topic with Parliamentarians. The APPG has looked at a wide range of topics over the years, highlighting many policy issues to relevant Ministers. As an example, when the Government published the National Cyber Security Strategy and Integrated Review in 2022, it sent an advanced copy to the APPG Chair. Subsequently we were able to hold a meeting to discuss the Review and comment on it. Our meetings have covered industry sectors such as IoT, Financial Services, and Maritime services, and we have also held two meetings with representatives of the US Government. One outcome of the APPG has been to help the ISG forge closer ties with the University of Maryland.

The current APPG chair, James Morris, was elected as the MP for Halesowen and Rowley Regis in 2010. He served on the Communities and Local Government Committee between 2010 and 2014. In his Parliamentary career he was Parliamentary Private Secretary to Esther McVey, but resigned his position in January 2015 in order to vote for a change in the law that would require planning permission to demolish or change the use of local pubs. He was Vice-Chair of the Conservative Party between January 2018 and November 2019. In February 2020, he was appointed a Lord Commissioner of the Treasury (Government Whip), and in September 2021 he was appointed Vice-Chamberlain of the Household, a senior Government Whip.

James Morris has very kindly contributed the following piece for the 2024 ISG newsletter.

Dear Readers,

I am very pleased once again to be penning a few words for the ISG as I took on the responsibility once again as the Chair of the APPG in early 2023. Back in 2019 I stated that I was determined to help make the UK one of the safest and most secure countries in which to live and work. Nothing has changed in terms of my ambition and I am glad to record my thanks to the ISG for its support of the APPG.

The help given by Professor Konstantinos Markantonakis and Andrew Henderson representing the ISG as secretariat has been invaluable. The APPG Parliamentary membership has grown with the addition of colleagues from the former APPG on Business Resilience and MPs from across the different parties, also representing every one of the four areas of the UK. This makes us one of the largest in Parliament in terms of membership. We are also creating positive impact in a wider context by forming a strong link between Academia, Parliament and Industry.

We got off to a busy start for 2023 with a notable APPG meeting in January that was a joint one with the APPG on Business Resilience. This looked at the insurance of cyber security risk and highlighted the difficulties that the market faces and potential remedies. In May we planned to have a meeting with the White House (via Zoom) who have set up their own Cyber Security office. Whilst we have had to re-arrange that to this year, the aim is to run regular meetings between the White House and Parliament to improve cyber security relations and understanding through the APPG. This will help to increase opportunities for collaboration at an international level. In June we looked at how to get more girls involved in STEM subjects, particularly Cyber Security.
We heard from a number of youngsters. The outcome of that meeting was a much better understanding for Parliamentarians about the challenges facing our education system and the importance of catching interest whilst still at Secondary school stage.
In November we returned to the topic of Maritime Cyber Security which included an excellent presentation from the ISG's Dr Konstantinos Mersinas. The outcome of a meeting, where obvious problems are highlighted, is usually a letter to the relevant Minister.

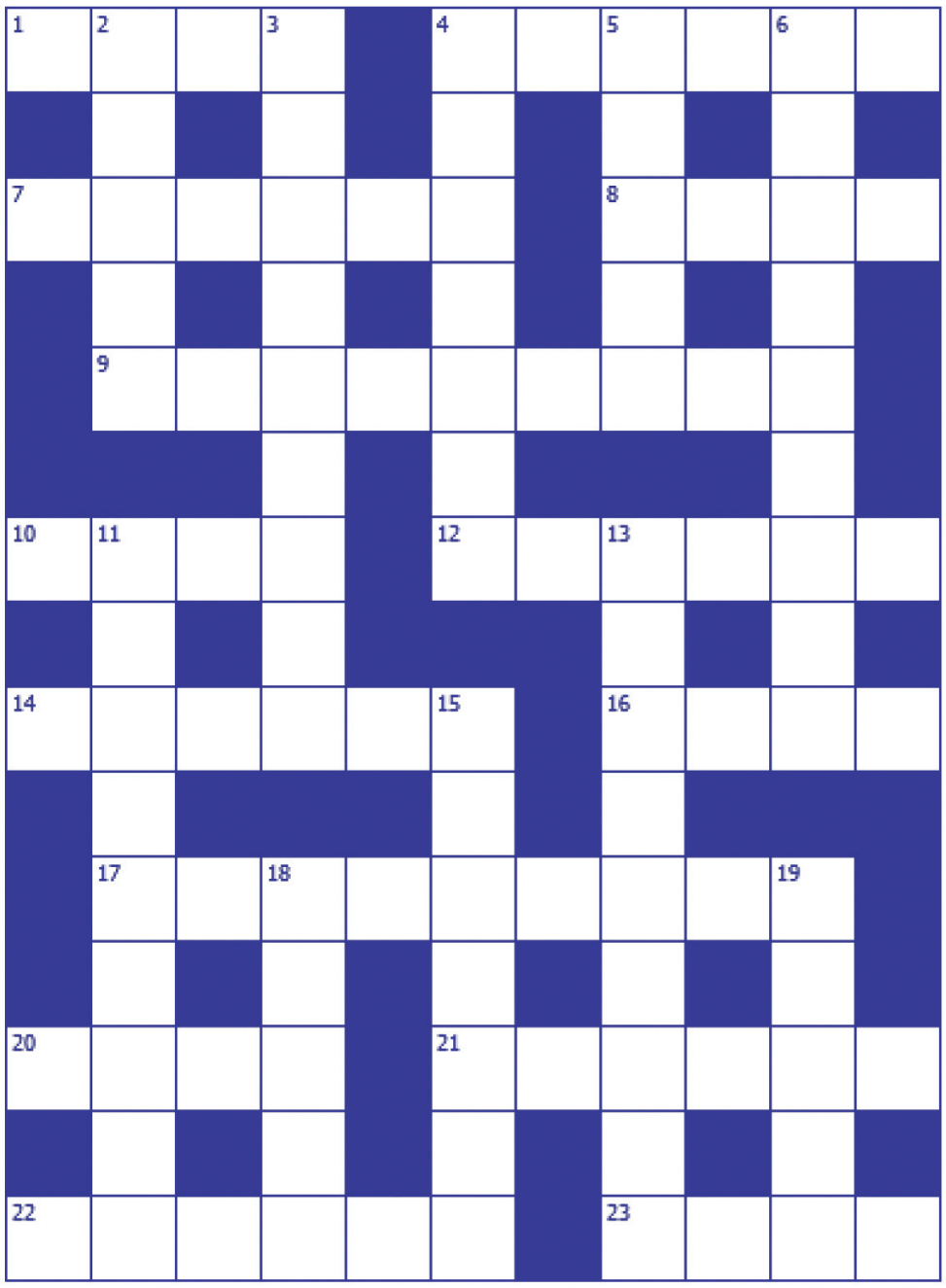
Looking to the future, I see no shortage of important topics for the APPG meetings with actions being planned on Maritime Cyber Security. Initial discussions have already taking place at the ISG about forming an inter-parliamentary group to promote good practice across the maritime nations. Another topic that we have in the pipeline is drones and how to secure them. Furthermore we would like to look at the development of microprocessors and related hardware as well as the need for the UK to be a centre of expertise in this sector and security interactions between hardware and software.
My goal is to further ensure that the valuable outputs from our discussions are captured and used to influence parliamentary strategy. In this venture I am most grateful for the assistance of the ISG, not only for supporting the secretariat, but for the cyber security expertise that it brings to the APPG discussions.

Yours Sincerely

James Morris MP
APPG Chair and Member of Parliament
for Halesowen and Rowley Regis

By Serpent

> Emeritus Professor ISG



Each answer must be encrypted with a Caesar 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 (8,5). If the first letter of the key phrase were B and the answer to 1 across were FRED, for example, then GSFE should be entered at 1 across.

Across

//

1 Skin condition (4)
4 Delight (anagram of asleep) (6)
7 Place for storing wine (6)
8 Main part of church (4)
9 Fruitfulness (9)
10 Young deer (4)
12 Yellow fruit (6)
14 Where a forger might work (6)
16 0.9144m (4)
17 The _____, book by Donna Tartt (9)
20 Principal male figure in story (4)
21 Type of quark (6)
22 Agreement (6)
23 Source of metallic ore (4)

//

Down

//

2 Man-made waterway (5)
3 Disaster at sea (9)
4 Idle chatter (7)
5 The opposite of right (5)
6 Addictive substance? (9)
11 Laid down (sediment, etc.) (9)
13 The I in GUI (9)
15 Flamboyant style of architecture (7)
18 Glaringly bright (5)
19 Wild dog (5)

//

CONTACT INFORMATION:

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

Information Security Group
(Bedford Building 1-29)
Royal Holloway
University of London
Egham Hill
Egham
Surrey TW20 0EX
United Kingdom

T: +44 (0)1784 276881
E: isg@royalholloway.ac.uk
W: www.royalholloway.ac.uk/isg

Twitter
twitter.com/isgnews
@isgnews

LinkedIn
linkedin.com/groups/3859497/