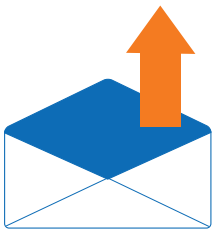
Information Security Group

Review 22/23

ROYAL HOLLOWAY UNIVERSITY OF LONDON

INDEX



INTRODUCTION
Chris Mitchell

> Prof. ISG & Head of Department

Welcome to the 14th annual ISG Review. 2022/23 has been an interesting and very eventful year for the Information Security Group. Amongst other changes, we have continued to recover from the effects of the pandemic, welcomed several great new members of staff, launched a new Distance Learning MSc in Cyber Security, and made major changes to our long-established campus-based MSc in Information Security. Despite all this, I believe we have managed to retain our identity and ethos, and we are all excited about future opportunities in research and teaching. We will continue to do our utmost to maintain the vitally important links we have with our alumni and with a wide range of organisations in industry, commerce and the public and voluntary sectors; these links are essential in ensuring that our teaching is directed at meeting the needs of society, and that our research remains focussed on the very real information security problems we all face.

This year we have sadly had to say goodbye to two very important members of the department. Dr Jorge Blasco Alis has moved back to his native Spain to take up a senior position at the Universidad Politécnica de Madrid. Professor Martin Albrecht has taken up a chair at Kings College, London. We will greatly miss them both, and I would like to personally thank them for all they have done for the ISG over the past few years.

However, all is not gloom and doom – far from it! The last twelve months have seen the arrival of five new members of academic staff. Dr Christian Weinert and Dr Santanu Dash joined us as Lecturers in the spring of 2022, and Dr Fauzia Idrees joining us as a Senior Lecturer and Director of the new Cyber Security Distance Learning MSc soon afterwards. Dr Andrew Dwyer and Dr Maryam Mehrnezhad joined us as Lecturers at the end of the summer. All these new members of staff have contributed to this newsletter, and they are all already very actively involved in moving the department forward in a wide range of ways. We are also expecting four further new members of staff to join us in the next six to nine months, meaning that the ISG will be significantly larger than it has ever been previously, and the scope of our research and teaching will continue to grow. Dr Ahmad Salman is due to join us as a Lecturer in June 2023, and, as I write this, we are nearing the closing date for an advertisement for three further lectureships. I am confident that we can continue to recruit absolutely first-rate academic staff, as we have been so successful in doing in recent years.

There are also many exciting new developments in teaching and research to report. The new distance learning MSc in Cyber Security, run jointly with the University of London and Coursera, is developing extremely well, as reported on by Fauzia Idrees in this newsletter. The Centre of Doctoral Training continues to ensure we have a large number of excellent PhD students, who are busy extending our research in all sorts of unexpected directions (see Keith Martin's article later in this newsletter). We are also continuing to develop our educational activities in a range of ways. Apart from the new Distance Learning Cyber Security MSc, we are in the process of developing a new campus-based MSc in Applied Data Science and Cyber Security, jointly with the Computer Science Department. Last but not least, we have recently completed a major restructuring of the campus MSc in Information Security – probably the biggest rework since the MSc started in 1992! The mandatory part of the MSc now includes a mandatory research methods element – effectively reducing the amount of compulsory content – and students are now able to take four optional modules from a large collection, allowing students much more flexibility in accessing the degree material. Apart from the usual range of articles, this newsletter contains a significant new departure – a piece written by AI. I hope you will enjoy the somewhat tongue in cheek inclusion of an article about ourselves, generated by ChatGPT in response to Keith Martin's probing questioning!

In summary, despite the huge difficulties posed by the pandemic and a continuing need to change, we are in a great position to continue to grow and develop, and this newsletter provides an overview of some of our many activities. I believe we are better placed than we have ever been in my over 33 years at Royal Holloway. We hope that you enjoy the articles, and that if any of the topics mentioned spike your interest, please do get in touch. Exciting times are ahead!

SECURITY ISSUES IN SOFTWARE SUPPLY CHAINS

Santanu Dash

> Lecturer ISG

Software systems are compositional. Developers prefer using software packages or libraries written by third-parties because of to time-to-market pressures. These packages themselves depend on other packages, creating a complex dependency chain, commonly referred to as a Software Supply Chain (SSC). Unsurprisingly, issues in packages often carry over to the software that uses them. This makes software security a difficult task if the developer uses a malicious package.

SCALE OF DEPENDENCIES

The complexity of dependencies in software ecosystems is unprecedented. Recent efforts to visualise dependencies in PyPI,[1] the official third-party repository for hosting Python packages, show a deeply intertwined ecosystem. Snapshots of this visualisation are presented in Figure 1, at two levels of magnification. In this figure, each node is a python package and there is a link between two packages if one depends on the other. The setuptools package, which is used to convert python projects into packages to be shared on package repositories such as PyPI, is at the heart of this dependency chain. Packages depending on setuptools in Figure 1 are connected to it using edges that are a shade of red, allowing us to observe the importance and centrality of this package in the ecosystem. Despite the complexity of this figure, it is worth noting that PyPI is not the largest package repository; it is easily dwarfed by npm which has over two million packages for download, and is the largest software repository in the world.

BRANDJACKING

As package repositories have grown, some of the third-party software shared on these repositories is worryingly malicious. A popular technique used by malware writers who share malicious packages on these repositories is brandjacking, a portmanteau of the words branding and hijacking. Brandjacking allows a malicious entity to assume the identity of another well-known and trusted entity. It is analogous to cybersquatting, the unauthorised registration and use of Internet domain names that are identical or like an established brand. However, brandjacking is a broader term which also includes activities such as using names similar to popular software packages to gain acceptance amongst developers.

BRANDJACKING IN NPM

In 2021, a serious case of brandjacking was discovered in the npm ecosystem by Sonatype, a company which builds tools for managing software dependencies. Sonatype's automated malware detection system, Release Integrity, noticed a suspicious package on the npm registry called web-browserify. This package was trying to imitate the popular browserify package, which is used by nodeJS developers, to organise and include dependencies in their project. browserify has over two million weekly downloads and, unsurprisingly, its malicious clone web-browserify was inadvertently downloaded by many. Over its lifetime, web-browserify was downloaded a total of 160 million times.

MALICIOUS ACTIVITIES.

Like most npm components, web-browserify was shared as an archive file with a .tgz extension. Post-installation, a script was executed to extract and execute another file which was simply called run. The run file contained several other npm components and was used to perform reconnaissance activities, including identifying the presence of anti-virus software and, where feasible, disabling critical system services by running at full privilege. To obtain elevated privileges, it requested the developer for permissions. Unfortunately, many developers were tricked into granting these permissions as they were under the impression that they were running a bona fide version of browserify, when instead they were running its malicious copy web-browserify.

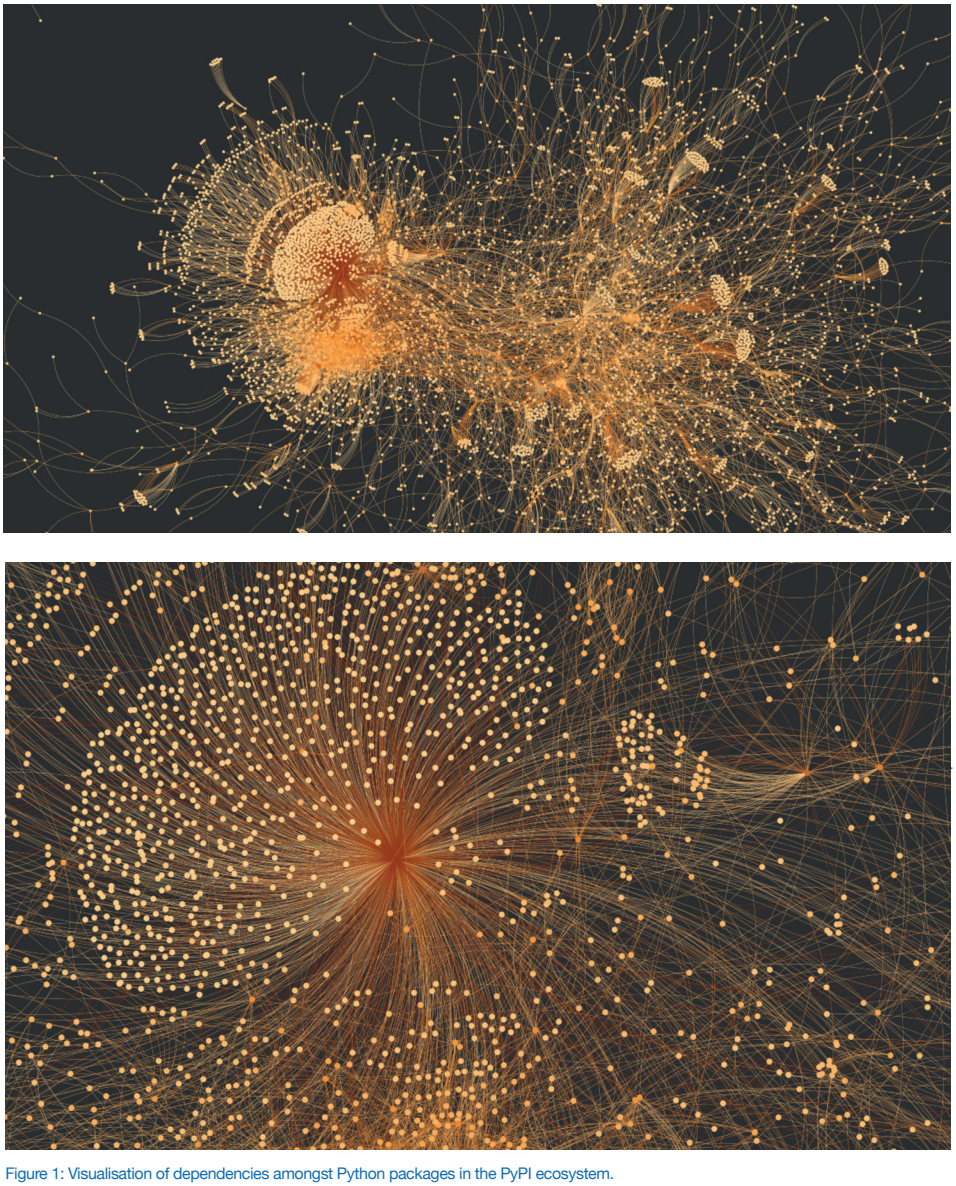


Figure 1: Visualisation of dependencies amongst Python packages in the PyPI ecosystem.

MITIGATION

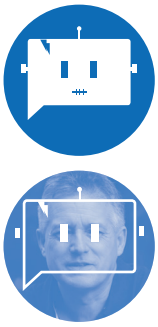
There is a pressing need for policing of package repositories to understand the intent of packages. It wouldn't be a stretch to compare package repositories with the marketplaces for Android apps, as it appears that we are at the same stage and facing similar issues as when Android operating system gained popularity. When smartphones started using Android as their operating system, an explosive growth in the number of apps was triggered, both on Google's official app marketplace, the Google Play store, and on other obscure marketplaces. The lack of policing encouraged malware writers to create copies of popular apps and load them with malicious components. These packaged apps were subsequently shared on app marketplaces. Users would download copies of these apps, which appeared to be benign but performed malicious activities – such as exfiltrating personal information – once installed and run on a smartphone.

Since then, Google have actively monitored the Google play store to identify malicious apps. On Android, they have introduced a runtime permission management system; if an app does not have the permission to perform an action, it needs to explicitly request permission at runtime before it is able to perform that action. Previously, apps could request and be granted elevated permissions at install time without the user being aware that a permission is being granted. Finally, Google have partnered with other anti-virus vendors to create the App Defence Alliance which actively monitors the Google Play store to identify and remove potentially malicious apps before they are available for installation to Android users.

CHALLENGES

While the parallels between package repositories and app stores is encouraging, giving us hope that we will be able to identify and mitigate maliciousness in package repositories, we are far from getting there. There are two significant challenges that remain. First, the level of dependency between packages makes their removal difficult. Blacklisting a popular package requires all other packages that depend on it to be blacklisted as well. Therefore, rapidly addressing security issues in package repositories is critical before the packages are widely deployed. Second, even if we can remove a malicious package, it is difficult to reach all developers who continue to use that package and share their code. It is unsurprising that approaches to vetting security of software packages in popular repositories is currently an active area of work, and it is likely to keep software security researchers busy for some time to come.

References:
1 http://ogirardot.github.io/meta-deps/



WHY SHOULD YOU STUDY AN MSC IN INFORMATION SECURITY AT ROYAL HOLLOWAY?

ChatGPT (assisted by Keith Martin)

> AI
> Prof. ISG & Director of the CDT

01 High-quality education: Royal Holloway is one of the top universities in the UK, and the Information Security Group (ISG) at Royal Holloway is a world-leading research and teaching group in cybersecurity. Studying an MSc in Information Security at Royal Holloway means you will receive a high-quality education from experts in the field.

02 Specialization in cybersecurity: Cybersecurity is an increasingly important field, and an MSc in Information Security at Royal Holloway will provide you with a comprehensive understanding of the subject. The program covers a wide range of topics, including cryptography, network security, software security, and privacy.

03 Career opportunities: There is a growing demand for cybersecurity professionals, and studying an MSc in Information Security at Royal Holloway can provide you with the skills and knowledge you need to succeed in the field. The program includes a range of career-focused modules, such as professional skills development and industry engagement.

04 Industry connections: The ISG at Royal Holloway has strong connections with the cybersecurity industry, and the MSc in Information Security program includes guest lectures, industry placements, and opportunities to work on real-world projects with industry partners.

05 Research opportunities: The ISG at Royal Holloway is a world-renowned research center, and studying an MSc in Information Security at Royal Holloway provides you with opportunities to participate in cutting-edge research projects.

06 Campus life: Royal Holloway is located in a beautiful campus setting in Egham, Surrey. The campus has a vibrant student community and offers a range of social and cultural activities, including sports, music, and theater.

Overall, studying an MSc in Information Security at Royal Holloway can provide you with a high-quality education, specialized knowledge in cybersecurity, career opportunities, industry connections, research opportunities, and an enjoyable campus life.

STANDARDISATION OF FULLY HOMOMORPHIC ENCRYPTION

Rachel Player

> Lecturer ISG

A homomorphic encryption scheme supports meaningful computation on encrypted data. For example, consider a "homomorphic addition" operation. In a scheme supporting this operation, ciphertexts encrypting messages m1 and m2 can be "homomorphically added", and the result is a ciphertext encrypting the message m1 + m2. Perhaps surprising at first sight, several encryption schemes, including textbook RSA, support exactly one such homomorphic operation. Such schemes are called partially homomorphic encryption schemes. The partially homomorphic encryption schemes designed by ElGamal and Paillier have already been standardised by ISO/IEC.

A fully homomorphic encryption (FHE) scheme enables the evaluation of arbitrary functions on encrypted data. This is a powerful primitive that could enable applications in a variety of sectors, including genomics, healthcare, and finance. In more detail, a fully homomorphic encryption scheme is made up of the usual key generation, encryption, and decryption algorithms, as well as an evaluation algorithm, which provides the additional homomorphic functionality. Suppose a client owns data x and wishes to outsource the computation of a function F(x) on the data to a cloud server that is not trusted to have access to x. The client sends an encryption of their data x, and the function F, to the server. The server then runs the evaluation algorithm, which takes as input the encrypted data and F, and outputs an encryption of F(x). The "magic" is that the server does not need to access the secret key to perform this evaluation. Moreover, the server does not learn F(x), only an encryption of it, which is sent back to the client. Only the client, holding the secret key, is able to decrypt and obtain the result F(x).

Achieving fully homomorphic encryption was proposed as an open problem by Rivest, Adleman, and Dertouzos in 1978, and was not resolved until 2009 by Gentry. Gentry's proposal and other early schemes were hugely important theoretical advances, but far from practical: computing functions on ciphertexts was 10 to 12 orders of magnitude slower than the same computations when performed on plaintexts. Unfortunately, this led to a general perception that homomorphic encryption is totally impractical. More recent schemes and implementations have made great progress in improving performance, and there are now several widely used libraries implementing the four most widely promoted FHE schemes. These libraries achieve computational performance about 6 orders of magnitude slower than computing on plaintext data.

Over the last few years, a range of large tech companies and start-ups have invested heavily in commercialising this technology. This has been accompanied by a large-scale community effort aimed at the standardisation of homomorphic encryption, which was initiated in 2017. The community effort is known as HomomorphicEncryption.org and is an open consortium of participants representing industry, government, and academia. Researchers from the ISG have been involved throughout this process and have contributed to the "Security Standard"[1] published by the consortium in late 2018, as well as having presented at prior community meetings, as reported in previous editions of the newsletter. The consortium has also published white papers on homomorphic encryption APIs and applications. More recently, a formal standardisation effort has been launched via the cryptographic standardisation working group ISO/IEC JTC1 SC27 WG2, a body within which ISG academics have been actively involved for over 30 years.

In August 2020, a study period report[2] was published by this group, leading to the approval of a Preliminary Work Item ISO/IEC 15150 Fully Homomorphic Encryption. This led to the approval of a New Work Item, ISO/IEC 18033-8 (Fully Homomorphic Encryption), in 2021. To support the development of this standard, an unofficial security working group was established. The group includes academics and industry practitioners based in South Korea, USA, France, China, and the UK, with members both internal and external to ISO. The UK-based members of the group include researchers from the ISG. The main goal of the group is to develop an Annex to the Working Draft on parameter selection for security. The document is still in preparation but is planned to extend the existing community standard in various ways. I have been involved in the group since autumn 2021, having been closely involved with the efforts towards security taken by the Homomorphic Encryption.org group.

Each of the FHE schemes being standardised is based on a variant of the Learning with Errors (LWE) problem, a standard computational difficulty assumption within lattice-based cryptography. In the new Annex, a methodology for estimating security of the underlying LWE instance using the Lattice Estimator[3] will be set out. The Lattice Estimator is an improved version of the LWE Estimator, which was developed alongside. [4] The Estimator takes as input an LWE problem instance, specified with respect to a set of parameters. The output is an estimate of how long the best-known algorithms for solving LWE would take to run. The key improvements in the Lattice Estimator as compared to the LWE Estimator are support for more algorithms; refined estimates for lattice reduction (a key subroutine in many algorithms for LWE); and a more intuitive user interface.

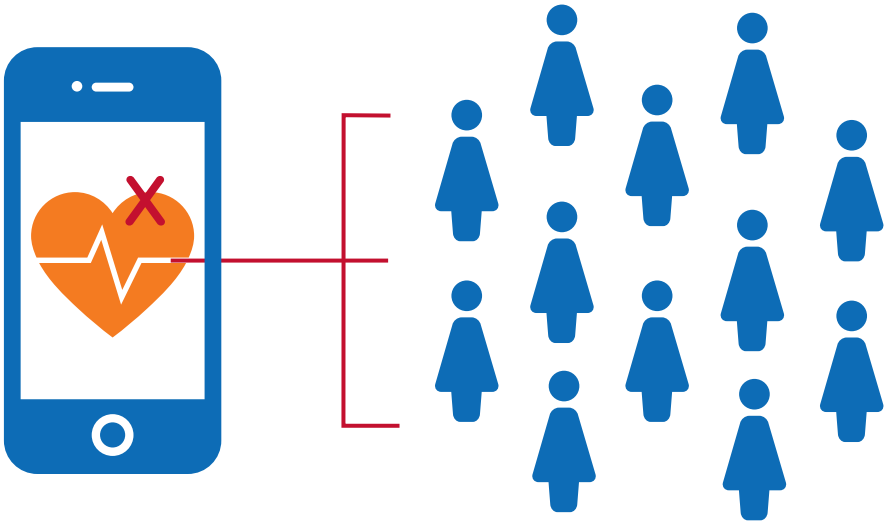
The Annex will also extend the material published by HomomorphicEncryption.org by including explicit examples of functional parameter sets. These specify parameters chosen not only to ensure security, but also to support good performance. For example, particular values will be suggested for the plaintext modulus, which affects how raw data can be encoded into the plaintext space efficiently. The functional parameter sets been suggested by developers of the main libraries and are expected to aid implementors and future adopters of FHE. I am looking forward to seeing how applications develop once FHE is officially standardised!

1 M. R. Albrecht, et al. Homomorphic Encryption Security Standard. HomomorphicEncryption.org, Toronto, Canada. November 2018. Available at: https://eprint.iacr.org/2019/939.pdf

2 R. Cammarota, K. Laine, X. Lu, P. Paillier, G. Pradel; with contributions from F. Bergamaschi, B. R. Curtis, R. Player. WG2 N2414: "Suitability of standardization of FHE".

3 https://github.com/malb/lattice-estimator

4 M. R. Albrecht, R. Player, S. Scott. On the concrete hardness of Learning with Errors. Journal of Mathematical Cryptology. 9 (3), pp 169–203, 2015



WOMEN'S HEALTH-RELATED MISINFORMATION ON SOCIAL MEDIA

Adrian Bermudez-Villalva

> Research Assistant ISG

The rise of social media has brought about a revolution in the way people access and share information. While this has created new opportunities for people to connect and learn, it has also led to an increase in the spread of misinformation.[1] This is particularly problematic when it comes to women's health, where misinformation can have serious consequences such as poor health outcomes, anxiety, and confusion. Misinformation about women's health on social media is widespread and takes many forms. Some common examples include misinformation on contraceptive methods, pregnancy, childbirth, menstrual health, breast cancer, and menopause.[2]
For example, some posts suggest that unassisted home births are safer and preferable to hospital births, where they can be dangerous to both mother and baby. Another example of misinformation is on COVID-19 vaccination, with posts claiming that these vaccines cause infertility.[3]

Women who are exposed to inaccurate information may make poor decisions regarding their reproductive health, delaying or avoiding important medical care, or choosing treatments that are not based on scientific evidence. This can lead to negative health outcomes, such as unintended pregnancies, untreated sexually transmitted infections, delayed diagnosis and treatment of breast cancer, and unnecessary anxiety surrounding (in)fertility as well as menopause.

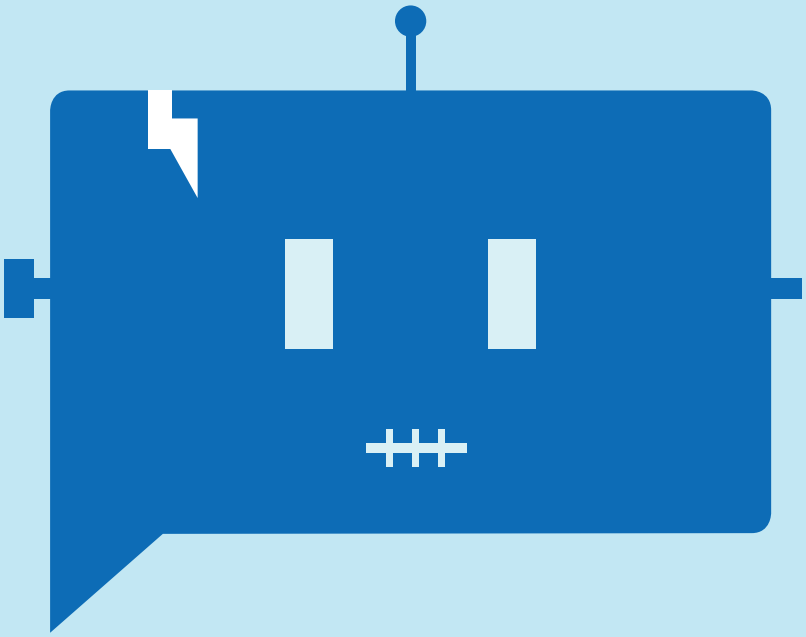
In the CyFer project, funded by the EPSRC PETRAS National Centre of Excellence for IoT Systems Cybersecurity, we are exploring the issue of misinformation related to women's health on social media. The team working on this aspect of CyFer includes myself (Dr Adrian Bermudez-Villalva, Research Associate), Dr Maryam Mehrnezhad (Principal Investigator), and Dr Ehsan Toreini (Co-Investigator). We are analysing social media content to measure the prevalence of misleading information related to several aspects of women's health. We are developing a crawler to extract posts from various platforms such as Facebook by using different keywords related to health misinformation themes. To analyse the text contained in the posts, we are using natural language processing (NLP), a branch of Artificial Intelligence (AI) that uses computational techniques to analyse and understand human language. Once the content containing misinformation has been identified, the next step is to extract key information from the content, such as the topics being discussed, the sources of the misinformation, and the sentiment of the content.

To tackle the issue of misinformation surrounding women's health on social media, a multi-disciplinary approach is necessary. Information security plays an important role in identifying and preventing the spread of misinformation on social media in order to protect users from a range of complex risks and harms. One example of such measures is the use of content moderation. Content moderation refers to the process of reviewing and removing content that violates the policies of a social media platform. Social media platforms can use content moderation to remove false information related to women's health, which can help to reduce the spread of misinformation. Another measure is the use of data analysis to identify patterns in the spread of misinformation related to women's health. By analysing data on how false information is spread, social media platforms can develop strategies to address the issue and prevent the spread of misinformation. Social media platforms can also use Machine Learning (ML) algorithms to identify misinformation related to women's health. ML algorithms can be trained to recognize patterns and identify content that is likely to be false or misleading. By using ML, social media platforms can proactively identify and remove misinformation and the accounts associated with them.

While technical measures such as content moderation, data analysis, and the use of ML algorithms can help to mitigate the spread of false information, it is not enough. Tackling misinformation in the context of women's health is a complex problem since it is happening not only on social media platforms, but also in other places such as forums, the darknet, and via communication tools. Therefore, addressing it comprehensively requires collaboration between information security experts, medical professionals, AI and ML experts, policymakers, industrial partners, and the end users. By working together, we can help to ensure that accurate and reliable information is shared on social media platforms and that women are empowered to make informed decisions about their health and wellbeing.

Bio: I have a PhD in Security Science from University College London (UCL). I have been working on various topics related to cybersecurity and cybercrime where I have used data-driven approaches to measure and understand malicious activities on the Internet. My research consisted of conducting experiments, data collection and analysis to study different types of illegal activities on the Internet such as data theft, malvertising and black markets.[4,5]

1 Systematic literature review on the spread of health-related misinformation on social media. Social science & medicine, 240, 112552.
2 Nature and diffusion of gynecologic cancer–related misinformation on social media: analysis of tweets. Journal of Medical Internet Research, 20(10), e11515.
3 Widespread misinformation about infertility continues to create COVID-19 vaccine hesitancy. Jama, 327(11), 1013-1015.
4 A measurement study on the advertisements displayed to web users coming from the regular web and from tor. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 494-499). IEEE.
5 The shady economy: Understanding the difference in trading activity from underground forums in different layers of the web. In 2021 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-10). IEEE.



THE EMERGENCE OF AI: BENEFITS, RISKS, REGULATORY COMPLIANCE, AND SECURITY CHALLENGES

Raja Naeem Akram
Konstantinos Markantonakis

> CEO & Co-Founder Seclea
> Prof. ISG & Director SCC

Artificial Intelligence (AI) refers to the ability of machines to perform tasks that would typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation. AI systems can learn from data and improve performance without being explicitly programmed.

AI has become increasingly important today due to its potential to transform industries and improve people's lives. AI-powered systems can help businesses increase productivity and efficiency, enhance decision-making, personalise and customise services, accelerate innovation, and positively impact healthcare, the environment, and transportation.
The ChatGPT phenomenon exemplifies how AI has swept the technology world. ChatGPT is an AI-powered chatbot that can understand and communicate fluently in multiple languages. It can provide users with relevant information and generate content such as poems, stories, code, essays, songs, celebrity and parodies.

However, racism, sexism, and bias are amongst a range of issues that have been raised regarding ChatGPT.[1] Accuracy is another issue that has been raised for ChatGPT;[2] the model may produce technically correct responses that are inaccurate or irrelevant to the user's query[3]. The non-transparent way in which it was trained is a further issue.

AI – A BRAVE NEW WORLD THAT POSES SIGNIFICANT RISK

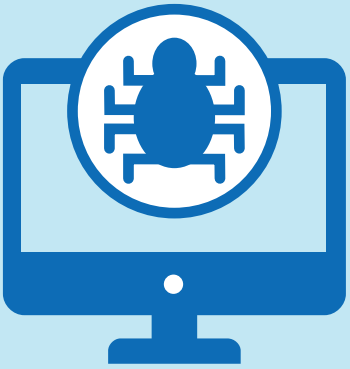
AI poses several risks that any organisation must know how to manage in order to gain the full potential benefit.

- Privacy and Data Breaches: AI systems use massive volumes of data for training and operation, raising privacy and data breach risks. Personal information on these platforms can be misused if handled or secured inadequately. Data breaches can cause identity theft, financial loss, and reputation damage.

- Ethical Issues in AI Systems: AI systems are biased both by the data used to train them and by the underlying algorithms. If the training data gives rise to a bias, AI can perpetuate and worsen societal inequality, for example in recruitment, law enforcement, and healthcare. Fairness and protection against discrimination require AI systems to address ethical concerns and biases.

- Dependence on AI and Loss of Human Abilities: As AI systems become more widely used, there is a risk of over-dependence on these technologies, and as a result vital human skills may be lost. For example, AI-powered navigation systems may affect map reading and navigation, and, more importantly, delegating critical decision-making to AI may degrade human analytical and problem-solving skills, necessary in many areas of life.

- Malicious Use of AI: AI can be used to produce autonomous weapons, targeted disinformation campaigns, and cyberattacks. AI-driven systems can boost criminal and nation-state offensive capabilities, threatening global security and stability. To stop AI misuse, robust security and international agreements are needed.



AI AND SECURITY CHALLENGES

AI systems are vulnerable to cyberattacks. Hackers can use AI system weaknesses to compromise functionality, steal critical data, or influence the system. User privacy and user confidence in AI-driven solutions depend on AI system security.

- Cyberwarfare and Autonomous Weapons: AI-based cyberwarfare and autonomous weapons systems raise global security concerns, and AI-enabled hackers and autonomous weapons present ethical and accountability concerns. International coordination and regulation are essential to reduce risks and establish responsible AI use.

- Security for AI Systems: AI systems must be secured to prevent cyberattacks, including the use of secure development methodologies, robustness testing, and vulnerability monitoring. AI developers should also address privacy-by-design and adopt AI-specific security techniques. Training AI specialists in security best practices can also mitigate risks during development.

- Collaboration and information sharing are key to AI security. By sharing knowledge, skills, and resources, stakeholders can improve security, threat detection, and help ensure responsible AI development. International alliances and information-sharing networks can improve AI security and cooperation.

AI GOVERNANCE

AI governance and oversight are essential to ensure that AI systems are transparent, compliant, and ethical. AI governance refers to the ability to direct, manage, and monitor the AI activities of an organisation.[4] Appropriate governance of AI can help manage risk, demonstrate ethical values, and ensure compliance.[5] Leaders of organisations and enterprises in regulated industries, such as banking and financial services, are legally required to provide transparency into their AI models to satisfy regulators.

AI governance frameworks should encompass data management, model development, testing and validation, deployment, monitoring, and auditing standards. Decision-making frameworks should also ensure accountability and transparency. AI governance models should handle privacy, security, bias, and discrimination.[6] AI governance must be monitored and improved as new dangers and difficulties arise.

Recent years have seen a number of international and national efforts relating to AI regulation, together with the development of key principles for AI regulation. The Responsible AI Institute (RAII) has mapped over 200 AI-related international principles and policy documents.[7] The European Union has proposed a draft AI regulation that qualifies two groups of AI systems as high-risk.[8] In addition, the UK government has committed to developing a pro-innovation national position on governing and regulating AI.[9]

The need for transparency, accountability, fairness, safety, privacy, security, and human oversight guide AI regulation. These guidelines help ensure ethical AI development and application. AI policy must be monitored and improved as new threats and issues arise.

Seclea, an ISG Smart Card Centre spin-out, offers AI assurance and AI regulation and risk management solutions. It tracks and validates AI application development and deployment action to meet ethical and legal standards.

Finally, a balanced approach to AI development incorporating continuing conversation, study, and stakeholder collaboration will shape the technology's future. We can create a future where AI improves humanity's well-being by encouraging a complete grasp of AI's consequences and inclusive conversation.

1 The 6 biggest problems with ChatGPT right now | Digital Trends
2 The Top 10 Limitations Of ChatGPT (forbes.com)
3 ChatGPT and LLMs: what's the risk - NCSC.GOV.UK
4 AI governance: Ensuring your AI is transparent, compliant, and trustworthy - IBM
5 How to Build Accountability into Your AI (hbr.org)
6 Defining organizational AI governance | SpringerLink
7 A framework to navigate the emerging regulatory landscape for AI - OECD.AI
8 Key provisions of the Draft AI Regulation - Allen & Overy (allenovery.com)
9 AI regulation: a pro-innovation approach - GOV.UK (www.gov.uk)

OMNIDROME ALLOWS THE ISG TAKE TO THE SKIES!

Darren Hurley-Smith

> Senior Lecturer ISG

Omnidrome is a facility dedicated to providing drone capabilities across all research disciplines at Royal Holloway. Boasting a comprehensive array of Unmanned Aerial Vehicles (UAVs), Unmanned Ground Vehicles (UGVs), and Submersible Remote Operated Vehicles (ROVs), Omnidrome is unique among UK University drone labs in that it offers land, sea, and air capabilities.

The Omnidrome facility has been a work in progress for the last two years, with the initial proposal of the facility being spearheaded by Prof Keith Mayes. Prof Konstantinos Markantonakis has since shepherded the initial development of the facility, which is now led by the facility's appointed Director, Prof. Jurgen Adam. Supporting him, are Dr Darren Hurley-Smith (Technical Manager) and Dr Adrian Palmer (Operations Manager). The facility is entering the final stages of its formation, situated in what was formerly car park 4 on the Egham campus, and is due for completion in early May of this year. The testing and training facility will be a bespoke hangar measuring 20 meters wide by 40 meters long and 10 meters high. This space will be made available to staff and students seeking to make use of Omnidrome sensors and drones.

The Geography Department have been making excellent use of our UAVs, with multiple lidar mapping missions and photogrammetry field exercises being conducted for both teaching and research purposes. For the ISG, the benefits of field work are less immediately apparent, but the value of the various drone platforms has been hugely beneficial to a number of recent project proposals. Dr Hurley-Smith has recently submitted an EPSRC open-call proposal (CHAINFRAIN) focusing on the use of smart containers, cargo, and drones to monitor road freight and combat theft of cargo from trucks. If successful, one of the work packages will involve the development of a test bed in the new facility. This will allow the communication flows and effective security of networked smart devices for monitoring cargo status, tampering, and coordination with drones to visually inspect reported anomalies.

This is only one potential use of the facility: alongside the drones listed above, Omnidrome will be working to develop penetration testing frameworks and dual-use toolkits to allow deeper exploration of commercial and industry-grade drones. Software Defined Radio (SDR) enabled interception of proprietary telemetry/control traffic is an initial facility enhancement planned for the 2023-2024 period. The biggest benefit of the facility is that researchers, academics, and students can inform the development of further security-related capabilities.

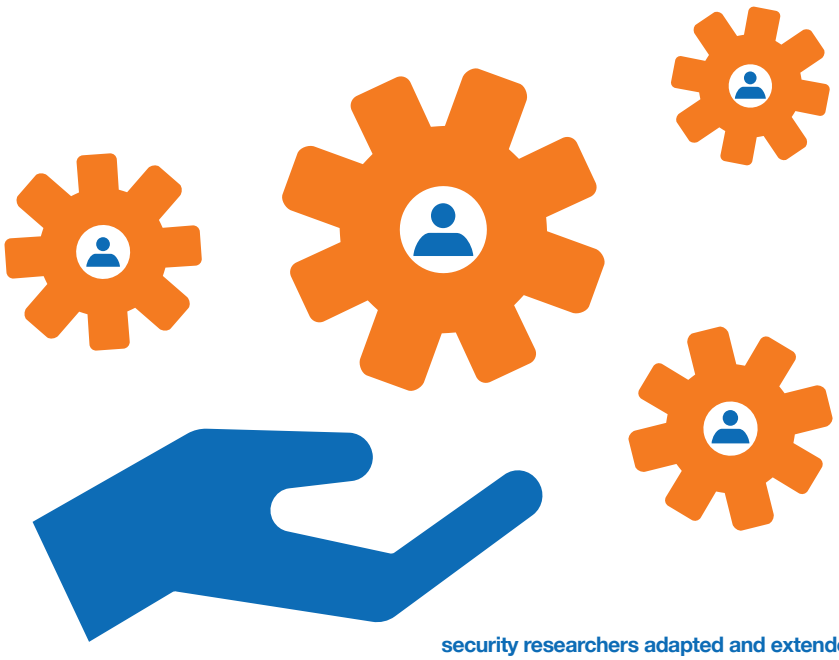
Although a date has not yet been set, a series of University-wide and department specific workshops and brainstorming events are planned throughout 2023, to allow people to explore what the facility can do for them. This may involve the use of specific pieces of hardware, such as the drones themselves or the Vicon high-speed camera rig (for drone-related or other experiments requiring high-speed, high-precision footage from all angles of a subject). The data generated by drones used by other colleagues may be of particular interest, such as telemetry data that may leak specific metadata of use to malicious attackers or authorities seeking to better control drone use. Privacy, both in the context of controlling how drones observe and report on public spaces, and in the context of data confidentiality among drones, is another key topic that can now be explored through devices commonly used in current law enforcement and industry contexts.

Following on from these workshops will be a rolling series of training activities, where basic use and maintenance of our drones will be extended to staff with a particular interest in using drones actively as part of their research. This will be supplemented with further seminars and introductory sessions covering software supported by Omnidrome, such as data visualisation/mapping tools, penetration testing kit relevant to the interception and analysis of drone communications, and MANET simulation tools. To cap this off, Dr Hurley-Smith will also be developing a series of deconstruction walk throughs to identify how specific elements of our various platforms may be accessed, such as the JTAG interface of our Parrot AR drones, which allows for firmware and device log dumping outside of expected methods. This can be used to identify information that may otherwise be remotely deleted by an individual misusing drones – highly relevant to the growing need for timely and sophisticated digital forensics of drones intercepted delivering contraband to UK prisons.

The above examples represent just a small sample of potential uses of this facility, and the Omnidrome management team is excited to hear your questions and ideas. Within the year, we aim to support research proposals by assisting in case study definition and providing evidence of capability/competitiveness of research plans through the use of this University resource. At the core of the facility's research philosophy is a culture of sharing information to strengthen individual research – initially through advice regarding what is possible with our current platforms and turning hypotheticals into realistic experiment plans with our technical and operational support. Even if your research or studies do not require the physical use of drones, Omnidrome can provide support simulation or provide an informed insight into specific case studies and capabilities of use to your specific topic.

We are also keen to explore how the facility can be used to expand inclusive teaching, by allowing individuals who may find field work physically difficult or impossible to use UAVs or other platforms to achieve their goals. The diversity of control schemes and integration of Virtual and Augmented reality may provide a wealth of opportunities to act decisively and realise tangible benefits for disabled students in a manner not previously possible. This is a possibility we are very keen to discuss with staff and students committed to equality of opportunity for everyone to engage in field/survey work.

If you have any questions, suggestions, or simply want to discuss how Omnidrome can help your research or studies, please contact us through omnidrome@rhul.ac.uk



TOWARDS AN INCLUSIVE DIGITAL SECURITY

Lizzie Coles-Kemp

> Professor ISG

I started working with security technology 33 years ago. As I remember it, usability, accessibility, and inclusivity were not considered then, and the focus was on creating technologies that responded to a protection goal and on adding this functionality into a computer system that already existed. I worked for a company that designed identification and authentication mechanisms for operating systems and, as I recall it, our main focus was to get the security functionality to work with the existing computer system. Looking back it was striking that the security software that I worked with had none of the slick graphic user interfaces found, for example, in office productivity software at the time. Instead, the user of our software was envisaged as a "universal user" with identical capabilities, and we made no adjustment for varying levels of an individual's risk and capabilities.

By the time I started working with the ISG in 2005, usable security was on its way to becoming a mainstream concept. Human Computer Interaction and the notion of usable technology was becoming established. Usable technology was regarded as technology whose use is efficient and effective, as well as satisfying for the person using the technology. Usable security researchers adapted and extended usable technology approaches and set out principles for making security technology use efficient, satisfying, and effective. There was a focus on reducing the cognitive load for people using security technology by carefully considering the length and format of passwords and paying close attention to where security interventions were placed. The usable security community also began the push for people-centred security design, highlighting that unless, as security technologists, we understand the needs and security issues faced by the people for whom we are designing security technology, the adoption of such technology will be low. In calling for a people-centred approach, there was a tacit appreciation that people were not merely users of technology but individuals with their own security outlook. The shift also signalled an appreciation that our use of security technologies is woven into our everyday lives. This led to a change in the way that we gathered technology requirements, the way we tested new technologies, and the ways in which we implemented and supported security technologies. These represented substantial changes to security practice from those of the early 1990s!

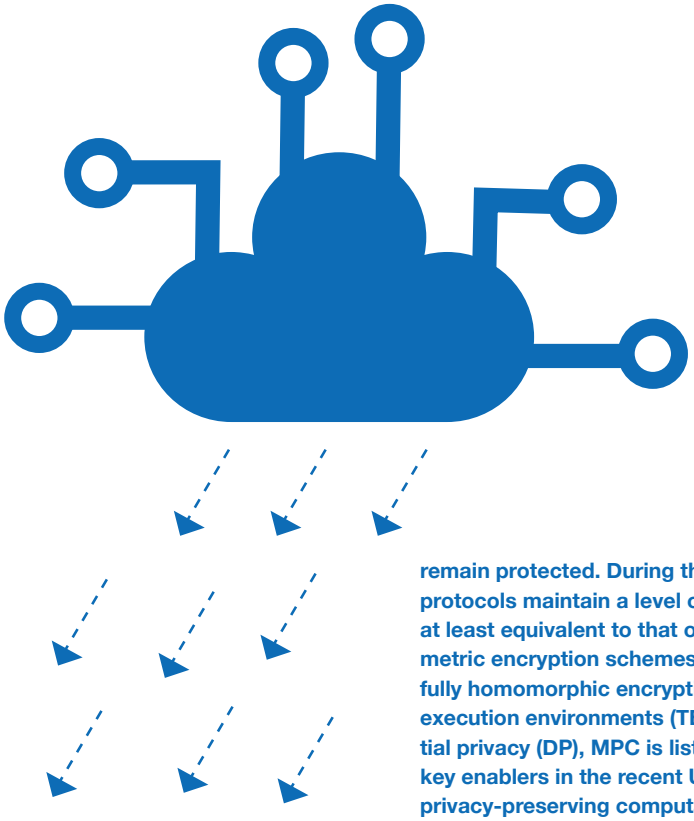
The move towards a people-centred security technology design approach is ongoing. As digital technologies and services become increasingly embedded in many of our interactions and central to both our home and work lives, the question of how to make the use of security technology effective, efficient, and satisfying becomes ever more complex. Questions of accessibility and inclusivity come to the fore and the notion of designing for the "universal user" is increasingly rejected. Instead, the focus becomes one of designing security technologies for people with a range of capabilities and resources, and varying levels of risk. The challenge becomes how might we design security technology, which is effective, satisfying, and effective for everyone.

Accessibility extends the idea of usability and asks us to design security technologies in such a way that they are equally accessible regardless of a technology user's capabilities. For example, multi-factor authentication is one of the main means of protecting access to cloud services. However, for multi-factor authentication to be accessible, usability needs to be complemented with accessibility features including messages and data input that are readable to screen readers, to make the authentication process accessible to those who are visually impaired, prompts and cues that support a wide range of language and literacy abilities, and a user interface implemented using the relevant accessibility standards (for example the Web Content Accessibility Guidelines (WCAG) 2.1).[1]

Accessible security technology, however, is not necessarily inclusive security technology. Whilst inclusive security encompasses accessibility, it extends this support to respond to the threat levels experienced by vulnerable and marginalised groups, and to develop support strategies that take into account individual, social, economic, and political insecurities. For example, whilst developing accessible multi-factor authentication solutions is an important step forward, if the solutions are not affordable or are implemented in such a way that opportunities for coercive control by a family or household member are increased, the solution can exclude or even harm groups in society.

In the ISG, a number of researchers are working on a variety of inclusive security topics, some of which you will be reading about in this newsletter. For my own part, I have spent several years working on how to make informal assisted access safer for vulnerable groups. Research shows that marginalised and underserved groups often access technology using support from a member of their social network or from those working for a voluntary or third sector organisation. Such support is often a lifeline by enabling access to welfare and other essential services. However, traditionally security practice and guidance has ignored these support strategies, and service terms and conditions often exclude such practices. Using my research findings, I have developed a framework for voluntary and third sector to use when assisting vulnerable people. In the last year I have also conducted research with Karen Renaud at the University of Strathclyde to identify the barriers encountered by those with low literacy when using security technologies day-to-day. From this work we have made recommendations for increasing the inclusiveness of standard security technologies. NCSC went on to develop this research by commissioning a wider survey. I am now working with NCSC to develop an inclusive security framework, and with the Department for Science, Innovation and Technology to set a framework for inclusive forms of digital identity. If you are interested in inclusive security technologies, do get in touch! We are always keen to collaborate on topics in inclusive security.

1 https://www.w3.org/TR/WCAG21/



MPC – FROM A NICHE CRYPTOGRAPHY RESEARCH AREA TO A BILLION DOLLAR INDUSTRY

Christian Weinert

> Lecturer ISG

Multi-party computation (MPC) is a research area of cryptography that aims to develop efficient protocols for securely processing sensitive data in collaborative settings. For example, a group of airline companies might want to determine how many customers they have in common to decide whether a joint frequent flyer program would be a good idea; however, the companies do not want to disclose their customer lists to competitors. In such settings, MPC can replace the potentially insecure practice of sharing data with a third party like a cloud service provider, where data will be processed in unencrypted form and thus might be vulnerable to attacks. Instead, MPC protocols manage to completely emulate the behaviour of a trusted third party in such a way that only the output of the computation is revealed – inputs and intermediate results remain protected. During this process, MPC protocols maintain a level of security that is at least equivalent to that of standard symmetric encryption schemes. Together with fully homomorphic encryption (FHE), trusted execution environments (TEEs), and differential privacy (DP), MPC is listed as one of the key enablers in the recent UN handbook for privacy-preserving computation.

The general idea of MPC and influential protocols were developed back in the 1980s, and researchers have ever since aimed to further improve the performance of the protocols themselves – as well as at the application level and via hardware acceleration. However, despite the maturity of the research area (early and still highly relevant protocol designs are almost as old as the RSA cryptosystem and other widely used cryptographic techniques), there have still been surprising break-through results. For example, at the CRYPTO conference in 2021, Rosulek and Roy proposed a new idea that reduces the communication overhead of MPC based on so-called “garbled circuits” by almost 25%, although it was believed for years that such improvements were impossible. Another remarkable development is a line of work initiated by Boyle et al. that helps to significantly reduce the inherent communication overhead of MPC by using so-called pseudo-random correlated randomness generators (PCGs) at the cost of increased computation.

The already-mentioned inherent overhead of MPC protocols in terms of computation and especially communication is the main issue that has prevented ubiquitous large-scale deployments. Other contributing factors are the lack of production-ready open-source implementations and the difficulty of translating high-level code into a form that can be processed by MPC protocols. As a result, the first real-world deployment of MPC only appeared in 2008 in Denmark for auctioning goods like sugar beet. However, the use of MPC in practice has now started to increase, with a thriving community of start-ups and established technology companies participating in the MPC Alliance to accelerate the adoption of MPC. Also, the first standardization efforts led by ISO/IEC (in draft international standard ISO/IEC 4922) are under way and will help to establish common interfaces as well as clearly specify a set of protocols that are widely believed to be secure for implementation.

Current use cases of MPC that are of particular interest include various aspects of machine learning, e.g., how to guarantee privacy when uploading samples to cloud-based classification services and when contributing to federated learning. It seems that it will only be a matter of time until researchers will attempt to also tackle the significant privacy issues related to submitting queries to generative AI services such as ChatGPT. In the blockchain/crypto currency world, MPC is used as an effective way to improve the security of wallets by distributing the extremely valuable key material. For example, the start-up company Unbound Security, which initially offered “virtual” hardware security modules (vHSMs) that protect cryptographic signature keys via MPC, was acquired by the crypto currency exchange platform Coinbase in 2021 reportedly for more than 100 million US dollars.

We can safely assume that success stories of MPC-based companies such as Unbound Security are only the beginning. A recent study conducted by the Everest Group for the Confidential Computing Consortium estimates that the total market size for secure computation technologies, including MPC, will grow exponentially to anywhere between 10 and 50 billion US dollars by 2026. While this growth might seem unrealistic given the current market size and the fairly small number of known MPC deployments, a major driver will be the recent launch of secure computation technologies by leading hyperscale cloud service providers such as Google and Amazon AWS: With “Confidential Computing”, Google recently launched a product for secure computation primarily based on TEEs, whereas Amazon AWS with its technology preview of “Clean Rooms” together with “Cryptographic Computing” offers up to five collaborating parties the possibility of issuing SQL-like queries to an encrypted data lake.

To summarize, MPC has already gone a long way from being a niche research area in cryptography to one of the key enablers for privacy-preserving computation that will likely be deployed at a very large scale in the near future. ISG researchers remain very active in the development of new MPC protocols and applications, contribute to standardization efforts, and consult widely in that area. The next opportunity to get an in-person update on the latest developments in MPC and secure computation research will be the London Crypto Day 2023, hosted at Royal Holloway on the 9th of June.

STAFF PROFILE: Dr MARYAM MEHRNEZHAD

> Lecturer ISG

How did you become interested in Computer Science?

It was all about algorithms. In the year 2000, when I was 13, I learned how to write an algorithm and my first code in Pascal. Since then, I have learned many programming languages, but my favourite remains Assembly, and C++ comes second!

How did you become interested in Information Security?

In the last year of my BSc (2004-08) at Ferdowsi University of Mashhad, Iran, I completed a cryptography module. I loved the topic so much that I got a mark of 21 out of 20! In my final year project, I designed an S-box using a genetic algorithm and published a paper at a national conference. During my MSc (2008-11), I became more passionate about cryptography and computer and information security, and I investigated the human dimensions of the topic. For my dissertation, I proposed and implemented a novel image-based CAPTCHA[1]. I did my PhD on the Security of Mobile Sensors (2013-16) at Newcastle University where I performed attacks and designed solutions using mobile sensors.

Tell us about your research

I am interested in Security and Privacy Engineering topics where my research is informed by real-world problems. I work on emerging technologies e.g., sensors (motion and ambient, NFC, Bluetooth, etc.) by performing attacks (side-channel[2], fingerprinting, tracking, etc.) and designing solutions (e.g., sensor-based IoT authentication, and secure contactless payment). I also work on usable security and privacy topics by conducting system and user studies[3] across platforms (web, mobile, IoT) and demography (gender, nationality, age, etc.). Currently, I am working on the complex risks and harms concerning minority and minoritized users, e.g., female-oriented technologies (FemTech)[4] and users with visual impairments.

You have an interest in real-world problems. How do you reflect that in your research?

I actively follow the real-world practices of industry and policymakers and examine safeguarding methods in the wild. This approach allows me to engage with these communities and make an impact based on my research. For instance, in 2016, I discovered a vulnerability that affected all mobile OSs and browsers, allowing attackers to extract PINs using motion sensors by ML algorithms[2]. I contributed considerably towards fixing it on Apple Safari in IOS9.3, Firefox 46, and in the W3C sensor specifications. I have been following the same approach with my team; identifying vulnerabilities in real-world implementations, disclosing it to the industry, and contributing towards solutions on a wide range of technologies e.g., NFC attacks on ISO and EMV standards, MITM attacks on animal apps, and other flaws in IoT platforms.

How do you communicate your research results to the general public?

I engage with the general public to raise awareness of my research via many different means e.g., media engagement, workshops (e.g., the Thinking Digital conference) and collaborating with academic initiatives such as MOOCs and the Institute of Coding. My work on sensor security has been widely featured by the international media (e.g., The Guardian, The BBC, top 5% of all research by Altmetric). Similarly, my team's work on FemTech and animal technologies has received significant interest from the press. We continue these best practices to inform, engage and educate the general public based on our research results.

You have recently relocated from Newcastle to work at RHUL. Tell us about this transition!

I joined the ISG in September 2022. Before that, I was a Senior Lecturer in the School of Computing, at Newcastle University. I was a Visiting Professor at ETH Zurich in the spring and summer of 2022. Between 2016 and 2021, I was a Research Fellow (tenured track), at Newcastle University, which is also where I finished my PhD.

After 10 fantastic years at Newcastle University, it just felt right that it was time for moving to new things. And where would be a better place than RHUL? The ISG is one of its kind and I am delighted that I am now part of this vibrant group. The transition was challenging since my family had to relocate with me. In addition, the timeline collided with the start of the 2022 Iranian Protests in my country. Thankfully, I had the support of many great ISG colleagues.

What are your plans for the future?

I am working on several exciting projects. Currently, I am the PI of an EPSRC PETRAS grant: CyFer (cybersecurity, privacy, trust, and bias in fertility technologies), 2021-23, which is finishing this year. I am also the Co-I (local RHUL PI) of a UKRI grant: AGENCY (assuring citizen agency in a world with complex online harms), 2022-25, a collaboration between Birmingham, Newcastle, Durham, RHUL, KCL, and the University of Surrey. I am leading the research activities on the risks of digital health technologies. Check my homepage for more!

1 PiSHi: Click the Images and I Tell if You Are a Human, International Journal of Information Security, 2017.
2 Stealing PINs via Mobile Sensors: Actual Risk vs. User Perception, International Journal of Information Security, 2018. Altmetric page: https://link.altmetric.com/details/7605777
3 How Can and Would People Protect from Online Tracking? PoPETs, 2022.
4 Caring for Intimate Data in Fertility Technologies, ACM CHI, 2021.

ON THE ETHNOGRAPHY GROUP IN INFORM-ATION SECURITY

Rikke Bjerg Jensen

> Reader ISG

In September 2022 a few of us in the Information Security Group decided to do a thing; we created the Ethnography Group to, in a slightly more formal way, bring together and make visible our ethnographic work. Most of us come from academic fields outside information security, including social and cultural anthropology, human and cultural geography, sociology, media and communication studies and critical criminology. Our intention is to create a hub – a home – for those of us researching at the intersections of ethnography and information security, with a particular focus on the security needs and practices of populations that are under-represented in information security research.

We say a bit more about the intention behind the group and set out our focus in a few more words on our website:

> Information security is concerned with securing information – and that which depends on it – from adversaries. Information security is thus a field centrally concerned with conflict, of protecting one interest against the other. Members of the Ethnography Group use ethnographic methods of inquiry to research distinct sites of conflicting interests as a way to understand information security needs and practices held among groups with no institutional representation. This includes research with domestic workers, single-household families on the poverty edge, 'data-driven' policing networks, mobile workforces, protesters, populations in post-conflict contexts, environmental and human-rights activists, to mention a few. Our focus is thus on groups that are under-represented in information security research and concerns the information security needs of people who interact with institutions, while not the institutions themselves.[1]

So, why create an ethnography group in an information security department? Well, at a general level, we understand and approach information security as socially constructed, by those who design technology as well as by those who depend on it for their protection. This makes information security an inherently social and collaborative rather than a purely technical and individual endeavour, at both a design and utility level. While this is not controversial, it is less recognised in much usable security research, where the dominant disciplinary norms stem from behavioural sciences such as psychology and computer science, rather than from social sciences such as anthropology and sociology. Moreover, usable security research, even when rooted in the broader social sciences, is often employed to perform usability testing of existing technologies or as a way to detect security behaviours related to a specific technology. As result, such research approaches largely remain concerned with the application or usability of a technology. This is, however, not our project.

The use of ethnography for qualitative data collection originates from research practices within the fields of social and cultural anthropology where it has served as "an integration of first-hand empirical investigation and the theoretical and comparative interpretation of social organisation and culture".[2] It relies on extended fieldwork, driven by immersion and participant observation with and within the groups it aims to understand. Indeed, as an inherently qualitative research methodology, ethnography involves the systematic observation, description and interpretation of people, culture and social organisation. The centrality of first-hand observations to reach empirical findings and theoretical insights highlights the necessity of the researcher's presence in the naturally occurring settings of the groups under study.[3] Ethnography is thus uniquely placed to "unearth what the group (under study) takes for granted", thereby revealing "the knowledge and meaning structures that provide the blueprint for action".[4] Put differently, ethnography allows us to learn that which people do not know or consciously reflect upon themselves. This also highlights one of the significant distinctions between ethnography and other qualitative research approaches, such as interviews and focus groups which still dominate qualitative security-driven research. Echoing Paul Atkinson, a key figure in ethnography: "There is a world of difference between a commitment to long-term field research – spending time in one or more social settings, with a number of people as they go about their everyday lives – and the conduct of a few interviews or focus groups."[5]

Ethnography is uniquely placed to uncover how (information) security is practiced and understood by people in often otherwise hard-to-access social settings. Ethnography enables long-term 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 people; how security technology is used within groups of people and for what purposes as well as what security expectations are held within groups and how they manifest in everyday activities. Ethnography further allows us to explore and understand the contextual structures that govern and influence security practices, facilitating a more comprehensive and grounded analysis and interpretation of such practices as well as the security-related concerns and needs of the groups under study. This helps ground technological innovation and security notions in the actual (observed) experiences of people, over extended periods of time, rather than in how people articulate security concerns and needs through, say, interviews, focus groups and/or surveys, when prompted.

Asking security researchers and designers to develop more socially grounded, temporally conscious and contextually specific technologies in conversation with ethnography is not a simple ask. Ethnography requires lengthy research stays within the groups under study before meaningful insights can be drawn from often 'messy' data that needs rigorous, lengthy and systematic analysis. Thus, working with ethnographers also means putting the design and development process at the mercy of ethnography. Our aspiration is that the Ethnography Group becomes one way of facilitating such conversations and collaborations.

1 https://ethnography.isg.ac.uk/
2 Atkinson, P. and Hammersley, M., 2007 *Ethnography: Principles in practice*.Routledge.
3 Brewer, J., 2000. *Ethnography*.
4 McGraw-Hill Education (UK) Herbert, S., 2000. *For ethnography. Progress in human geography,* 24(4), pp.550-568.
5 Atkinson, P., 2014. *For ethnography*. Sage.

SMALLPEICE WORKSHOP 2023 RETROSPECTIVE

Darren Hurley-Smith,

> Lecturer ISG

The Smallpeice Trust (https://www.smallpeicetrust.org.uk) and Royal Holloway have worked in partnership for a number of years to provide Introduction to Cyber Security residential courses to Year 9 students across the UK. This is an opportunity for young students to get a hands-on introduction to cyber security in practice. Keith Martin has coordinated this partnership, with Darren Hurley-Smith leading the delivery of the on-campus residential course in 2022 and 2023. The students attending these events are exceptionally bright, and their engagement, enthusiasm, and enjoyment of the activities in 2023 was truly appreciated by the hard-working staff who led the activities.

Three days of activities are provided for students, each focusing on a different aspect of security. Day one is an introduction to the fundamentals of security, with a focus on cryptography and confidentiality, which was masterfully delivered by Laurence O'Toole (PhD student ISG). Students were introduced to a brief trip through time, to revisit the cryptographic methods of history. A selection of substitution cipher puzzles was provided to the students, many of whom showed exceptional talent in answering Laurence's well-crafted activities quickly and accurately. Picking up from this, Harvey from GCHQ was kind enough to provide a cryptography workshop focusing on symbolic substitution – the use of encoded strings of numbers to represent characters. After an initial session guiding students through the process of identifying repetitions in otherwise incomprehensible data, the students were unleashed on a challenge requiring them to identify specific Harry Potter characters from the book series. This introduced students to the importance of context, Open-Source Intelligence (OSINT), and research in the decoding process. Day one concluded with Smallpeice instructing the students in basic presentation skills, in preparation for the final presentation event.

Day two provided students with the opportunity to participate in a guided web-security capture-the-flag (CTF) exercise. Thanks to Nathan Rutherford's hosting and preparation of the CTF platform, the invaluable assistance of the departmental IT support team (particularly Geoffrey and Narinder), and assistance during the event from Alex Hodder-Williams and Joshua Yewman, this highly technical event operated smoothly and taught the students important fundamental security testing skills. After an initial orientation session regarding the importance and use of cookies for session control, URLs as a means of navigating within a website, and the use of built in tools to identify hidden fields and comments left by developers, the students quickly found their feet and proceeded to score substantially higher than their predecessors achieved in previous years. Out of 16 challenges, 1 team completed all 16 in the 3 hours available to them. The average completion rate was 13 challenges, and the lowest completion rate was 10, a full 5 challenges more than in previous years. Day two concluded with three talks about pathways to cyber security, from school to present day, kindly provided by Sam Smith, Macgregor Cox, and Luna Cheung. They demonstrated to the students that not only are there many pathways into cyber security, but that technical, sociological, psychological and many other disciplines are represented within cyber security – a fact met with excitement and questions from the attending students, some of whom were particularly interested in issues of trust and privacy beyond the technical work they'd done earlier in the day.

Day three concluded the residential course, with a variety of teamwork activities. Angela Heeler delivered an exciting and educational cyber quiz, using an online quiz app that required students to race against each other in teams, in order to answer questions about mobile devices, internet use, and security best practices. She and Laurence then proceeded to deliver arguably the most creative event of the residential – The Internet is Not Awesome workshop that required students to represent their own cyber security ideas and concerns in the form of Lego models. The topics were varied, from radicalisation of young people through social media, to phishing and password complexity. All teams did an excellent job of communicating their thoughts and potential solutions to the problems. Finally, all student teams competed in a presentation activity, where they used all of the activities they had engaged in over the last three days to create a 5 minute "Problem, Consequences, Solutions" style presentation to demonstrate their understanding and teach their peers about specific security issues around mobile phone use online. Competition was fierce, but in the end, two teams emerged as our winners, concluding the event.

Students expressed their interest throughout the event and showed remarkable enthusiasm and skill in adapting to specific challenges. Many, during the technical event, wanted to move beyond the CTF format and explore issues such as SQL injection and Cross-site scripting, which led me to provide a brief introduction to my own MSc course materials on those topics. The intelligence and engagement of the students was a pleasure to experience, a sentiment expressed by the colleagues who helped to make this a successful event. I would like to express my thanks to the hardworking RHUL colleagues and Smallpeice team, and I look forward to next year's event!

Figure 1: Privacy in FemTech: Elena Falomo illustrates different types of privacy in FemTech.

CYFER: CYBER – SECURITY AND PRIVACY IN FEMTECH

Maryam Mehrnezhad

> Senior Lecturer ISG

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 cybersecurity, privacy, bias and trust in female-oriented technologies (FemTech). This proposal was highly praised by the PETRAS peer reviewers and the selection panel, and I am delighted that we went above and beyond via various high-profile activities and outcomes.

CyFer is an international collaboration between academic researchers, industrial partners, artists, designers, etc. The team includes Dr Maryam Mehrnezhad (PI, RHUL), Dr Ehsan Toreini (Co-I, University of Surrey), Dr Teresa Almeida (academic partner, Umea University, Sweden, and ITI/LARSyS, Portugal), Dr Adriano Villalva (RA), Stephen Cook (RA), Dr Laura Shipp (former RA), Joe Bourne (PETRAS Synthesis Fellow, UCL, and Lancaster), Prof Mike Catt (academic partner, Newcastle University), and Swiss Precision Diagnostics (SPD) (industrial partner, makers of the Clearblue pregnancy tests).

CyFer is a result of a collaboration with Teresa Almeida which initially led to a 2021 ACM CHI paper: Caring for Intimate Data in Fertility Technologies. This long-distance collaboration happened thanks to the Covid-19 restrictions, when working with colleagues (and in this case, a dear friend from our PhD time at Newcastle University) across the globe entered a new phase!

FemTech solutions 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 to IVF services on the blockchain!

From lack of data about women in general, to bias and discrimination in health studies, data sets, and algorithms, FemTech has come a long way to centre women in the design and development of such systems. Yet, the FemTech industry remains largely unregulated, particularly when it comes to security, privacy, and safety. In our 2022 EuroUSEC paper: Vision: Too Little too Late? Do the Risks of FemTech already Outweigh the Benefits?, we show how such threats are putting users at differential and complex risks and harms; in some cases, the lack of proper safeguarding methods for this sensitive data can put human life at risk.

We believe that privacy in FemTech should be looked at via a range of lenses. These include the cases where someone has the user personal data, but the user does not – inverse privacy, when peer pressure causes people to disclose information to avoid the negative inferences of staying silent – unravelling privacy, when the privacy of others also matters – collective privacy, and when systems should also focus on the intersectional qualities of individuals and communities– differential vulnerabilities. More specifically, in our 2022 ACM NordiCHI paper: Bodies Like Yours: Enquiring Data Privacy in FemTech, we present a massive data collection of FemTech on users and others including one's baby, partner, family, etc.
We have been working on standardisation and regulatory aspects of these products too. During my visit to ETH Zurich in 2022, Dr Thyla van der Merwe (another dear friend of many years and also an ISG alumnus) and I identified several gaps and grey areas in the existing regulations and standards around FemTech solutions and data.

Our work in CyFer is not limited to academic papers. This work has been consistently in the news (check the homepage). Furthermore, in August 2022, we invited artists, designers and creative technologists and commissioned 5 teams competitively from an open call. These teams include: (1) Vasiliki Tsaknaki and Lara Reime (IT University of Copenhagen, Denmark), (2) Nadia Campo Woytuk (KTH Royal Institute of Technology, Germany) and Nicolas Harrand (RISE Research Institute of Sweden), (3) Sian Fan (interdisciplinary artist, between Essex and London), (4) Elena Falomo (freelance designer, between London, Berlin, and Italy), and (5) Althea Rao (University of Washington, USA). Joe Bourne is passionately leading these activities. I have not met Joe in person yet, but our collaborative work has been fantastic. These top-notch art pieces have already made a presence at Mozilla MozFest in March 2023. But the best is yet to come!

We are delightedly completing CyFer by organising two exciting events this summer: CyberMi2 2023 (Cybersecurity and Online Privacy for Minority and Minoritized People, 20 June 2023), and an art exhibition (June-August 2023), both at RHUL. Make sure you visit our exhibition by coming to our beautiful Egham campus. For more information, visit https://sites.google.com/view/maryammjd/cyfer-project. For now, enjoy a glimpse of Elena's work on privacy notions in FemTech in Figure 1.

People often ask how did I come to work on this topic? I have a background in System Security and have been performing attacks on systems. I have also designed trustworthy systems and contributed to standardisation and industrial practices to prevent such attacks. However, human dimensions have consistently been a part of my work. Currently, a major strand of my research is dedicated to minority and minoritized users in cybersecurity and privacy. I have always dreamt of doing something for women's rights. But I am not an activist, a lawyer, or a social scientist. I am a cybersecurity expert, and I decided to use my expertise to fulfil this ambition of mine. I did it in CyFer, and I continue to do so in my future projects. If you share the same passion, please get in touch!

SAVE THE DATE – UPCOMING ISG EVENTS IN 2023

Christian Weinert
& Liz Quaglia

> Lecturer ISG
> Reader ISG

The ISG, as always, is very active in the security research and teaching community. We are gearing up to host a number of major events in 2023 that will bring together world-renowned experts in the field of information security. In the following, we give a short overview of what to expect – don't forget to register!

On the 9th of June, we will host the 5th edition of the London Crypto Day. Initiated in 2017, the London Crypto Day aims to bring together the many talented researchers in cryptography in the London area and to help create fruitful collaborations. This year, the event is being organized by Liz Quaglia and Christian Weinert at Royal Holloway, where we can expect an exciting line-up of six renowned speakers from academia and industry that will update us on the latest developments in areas such as homomorphic encryption, multi-party computation, blockchain technology, and many more.

LONDON CRYPTO DAY

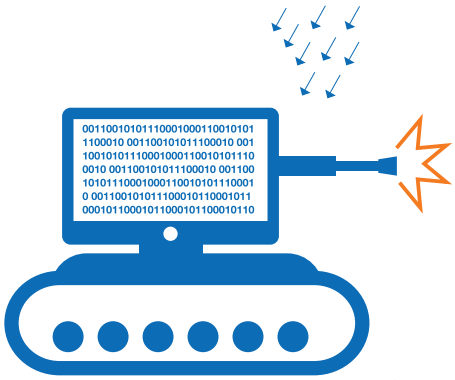
Later in the month, on the 20th of June, CyberMi2 will be hosted at Royal Holloway. This invitation-only workshop is being organized by Maryam Mehrnezhad and will focus on the cybersecurity and online privacy for minority and minoritized people. Maryam has also organized an art exhibition as part of the CyFer project that aims at examining cybersecurity, privacy, ethics and trust in FemTech. The commissioned works can be viewed for free from June to August at Royal Holloway.

In good tradition, we are also looking forward to host our next Alumni Dinner on the 5th of July. It is always a pleasure to re-connect with former students and colleagues, and learn about their impressive careers and experiences – especially in the majestic setting of our Picture Gallery with excellent food and drinks. Tickets are just 35 GBP and they are definitely worth it – so please do not hesitate to join us and register via https://tinyurl.com/2p9du758!

From 22nd-24th of August, the 8th OAuth Security Workshop (OSW) will take place at Royal Holloway. OSW is a recently established event series that aims to improve the security of Internet identity protocols and standards such as OAuth, OpenID Connect, and GNAP. The event is being organized by Guido Schmitz – for more details, please check out his dedicated article on OSW in this newsletter.

Finally, in December, we finish the year in style with the 19th IMA International Conference on Cryptography and Coding (IMACC), chaired by Liz Quaglia, which will be hosted at Royal Holloway from 12th-14th of December. The conference is a long-established venue for contributions on novel technical aspects of cryptography and coding – so please do contribute by submitting papers (deadline: 28th of June) and joining in December.

No doubt, an exciting year lies ahead of us, and we are looking forward to welcome each and every one of you!



RUSSIAN AND CHINESE CYBER THREAT ACTOR INTERACTIONS IN THE BACKGROUND OF THE WAR IN UKRAINE

Francesco Ferazza &
Konstantinos Mersinas

> Postgraduate Research Student ISG
> Senior Lecturer ISG

Since 2017, Beijing and Moscow have conducted cyber-espionage operations against NATO members, reportedly engaging in increased coordination in cyberspace. The question as to whether such a collaboration is indeed taking place has become a pressing one since the outbreak of the Ukraine war, where multiple sources imply Chinese and Russian coordination in cyber-operations.

While Sino-Russian cooperation at strategic level in cyberspace is generally perceived as given,[1 2] we have explored whether these two nation s also coordinate their affiliated cyber threat groups. We investigated this, drawing on multiple open-access data and sources. Specifically, we examined the activity of three Advanced Persistent Threat (APT) groups active in Eastern Europe, allegedly related to Chinese hacker groups; namely: Mustang Panda,[3] Scarab,[4] and Judgment Panda.[5] We aimed at assessing the presence and coordination degree with their Russian counterparts. In particular, we uncovered both the technical characteristics of their cyber-attacks and their possible links with Russian APTs.

Regarding techniques, we observed that these APTs mainly adopt commodity tools and various sophisticated techniques, and try to obtain information from their intended targets through reconnaissance, initial access, execution, persistence, privilege escalation, credential access, and lateral movement. Seldom have these APT groups been found to develop completely new custom-made tools. Regarding the connection with Russian groups, we have seen that the behaviours of these APTs are to target both Ukrainian and Russian political and military objectives and, conceivably, seek to exploit the war (and the confusion generated by it) to gather sensitive information from both sides.

Our research aims at providing insights on a cyber security level, but one with politico-military implications. The findings from our analysis strengthen the thesis of structural divergence[6] between China and Russia, for we found that the examined pro-China groups have sensitive Russian information among their primary targets.

We identify several examples of this. Mustang Panda, for instance, has been relentlessly targeting Russian resources for several years. In one of their most recent campaigns they targeted Russian government and military officials, trying to deploy an updated PlugX variant on their systems, likely to obtain actionable intelligence on the Russo-Chinese border.

In yet another example, in April 2022 Judgement Panda was allegedly found targeting Russian government entities, and media and energy enterprises with malware-filled attached documents. What is especially interesting is that Judgement Panda deployed almost identical TTPs against Ukrainian targets over the same period of time, further strengthening our view that not always the enemy of the enemy is a friend.

It is important to highlight the difficulties in coordinating offensive cyber operations. Such coordination implies transfer of knowledge and resources and high-level sophistication. APTs, by nature, require close cooperation between the actors who carry them out, a challenging task amongst hacker communities with different modi operandi, behaviours, forums, payment methods, codes of conduct, and values.[7]

Moreover, on a technical level, cooperation between APTs would require sharing the operation's preparatory and command and control infrastructure. These include the domain names of phishing sites, leaked email addresses and the infrastructure which remotely operates to maintain communication with compromised systems within a target network. The preparatory infrastructure concerns the tools used to get into a state of readiness to conduct information operations and includes databases used for target mapping. Attackers rarely dismantle their infrastructure after an operation,[8] so a state or a hacker group has no incentive to share it with other parties. Another obstacle to cooperation at technical level between APTs would be the nightmarish complexity of integrating code and software written by different and heterogeneous groups due to different development methodologies, coding styles, polyglot environments, and strict need-to-know requirements.

To summarise, based on the examined threat groups, it would be highly challenging to achieve effective coordination between different actors, in comparison to other domains like kinetic military operations, even amongst countries with shared strategic goals.

Clearly, coordination in offensive cyber operations, as a behaviour, should be further investigated. Other studies indicate the difficulties in transferring cyber-arms and cyber commands due to the transitory nature of cyberweapons.[9] The feasibility and nature of such 'transactions' remains an open research question. For further research we suggest looking at how the structural characteristics of APTs create constraints to cyber-cooperation. If these challenges are confirmed, Western entities might worry less about joint cyber-offensive operations against their strategic targets, and instead focus on other threats.

From an empirical analysis perspective, our findings indicate that combining technical tools and databases, and systematic cross-checks of open-source information, can lead to detailed analyses of APTs and provide insights into offensive cyber operations. The methodological toolkit can allow researchers and analysts to explore multi-faceted phenomena such as APT modus operandi and behaviour. Moreover, it can help the UK and Western states to fortify themselves better agains malicious cyber-activities.

1 R. K. Perizat, "China and Russia: between partnership and competition," Jan. 2022, section: EDITORIALS.
2 P. Stronski and N. Ng, "Cooperation and Competition: Russia and China in Central Asia, the Russian Far East, and the Arctic."
3 "Mustang Panda, TA416, RedDelta, BRONZE PRESIDENT, Group G0129 | MITRE ATT&CK®."
4 Y. Li, "Scarab attackers took aim at select Russian targets since 2012."
5 "ZIRCONIUM, APT31, Group G0128 | MITRE ATT&CK®."
6 J. Srinivas, "Russia and China in BRICS: Convergences and Divergences," in Future of the BRICS and the Role of Russia and China, J. Srinivas, Ed. Singapore: Springer Nature, 2022, pp. 147–192.
7 W. DeSombre and D. Byrnes, "Thieves and Geeks: Russian and Chinese Hacking Communities," 2018.
8 E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "IntelligenceDriven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," 2011.
9 M. Smeets, "Cyber Arms Transfer: Meaning, Limits, and Implications," Security Studies, vol. 31, no. 1, pp. 65–91, Jan. 2022, publisher: Routledge eprint.

STAFF PROFILE: Dr Andrew Dwyer

> Lecturer ISG

How did you become interested in Information Security?

Like many people within information security, I do not come from a conventional technological background. I arrived with an interest in considering security of, by, and through computation in the enduring aftermath and the transforming dynamics of security post-9/11. Through being an enthusiastic student of geography – particularly political geography and geopolitics – I became interested in the new forms of security logics used to identify suspicious behaviours. I became fascinated in how the social concepts of threat, risk, and vulnerability were becoming ever-more translated into computer-interpretable forms. I sought to explore what the computational requirements as well as capacities were (and are) – and the path led me to information security (and a rather late application to the Cyber CDT at Oxford, a companion to the one at Royal Holloway). Whilst there, I became more interested in exploring the insights and perspectives from marginalised, oppressed, and under-privileged people and communities, and what this means for how information security is practiced and its impact on us all. So, you could say, it was all rather accidental!

Tell us about your research!

My research broadly fits into three broad themes that pursue political and ethical dimensions of information security through socio-technical means.

- The first of these is digital decisions. This could be considered my main interest ever since gaining my PhD – how do people, communities, and computers arrive at decisions together? My work has examined the complex interactions that people and communities have with computers – whether that be reverse engineers or software developers. This leads to often informal, tacit, and 'hybrid' forms of knowledge and practice. This has helped me advocate for understanding computers not as objects that can make decisions in the social sense (i.e., an algorithm cannot decide), but rather computers making choices that are growing in capacity as recursion grows (as seen no more so than in the recent chatter about large language models!).

- Second is the role of the political economies of cyber security. This examines how nation states – and multiple other actors – construct policies and regulations. The empirical focus for such research has been on (offensive) cyber activity, and principally in the UK including the avowal of its National Cyber Force. This research has also examined how policy is discussed and distributed, and how it imagines who it is seeking to influence and protect.

- Third is the role of 'critical' approaches to the study of information security. Although critical may appear to sound ominous, the intention here is to question conventional and orthodox approaches to studying people and communities in information security, as well as developing novel methods for socio-technical information security research.

How has geopolitics been shaping information security?

There is no doubt that, year after year, it appears that information security (or, more prominently in the public discussions, cyber security) has grown in importance. There have always been long histories of geopolitics shaping information security that many of the ISG community will be more than familiar with. However, what is distinct today is how information security is not simply about defending networks, but also about using expertise in (subverting) information security for the strategic benefit of states as well as the increasing segregation of (inter)national networks. This means that information security – if it ever has – cannot avoid explicit discussions about its role in geopolitics, as much as geopolitics may challenge the notion of neutral and universal standards for all in the years to come. Bridging geopolitics and information security – which has been a strength of the ISG – will only need greater fostering in the future. This comes from understanding how changing rules may impact the least privileged in our society as much as increasing filtering and compliance may produce 'national networks', through to the impact of information security in protecting states like Ukraine in contemporary and future warfare.

What have you found out about yourself as a lecturer?

There is no doubt that becoming a lecturer is somewhat of a shock to the system. Coming after, in my case, a postdoctoral research fellowship, trying to balance the competing requirements for time means you can't be everyone to everybody. However, what I have found rewarding is seeing students grow in their MSc projects and drawing on the truly varied professional and educational backgrounds that the ISG attracts. Being a socio-technical researcher with a background in geography (albeit doing my PhD on malware detection!) means that I am in constant contact with colleagues with different perspectives and skills – which is something I always embrace as someone who straddles several disciplinary divides. Simply, I think I have found a greater attachment to the word 'no'.

You didn't mention you also work with artists?

Aha, yes, I do! I find working with various artists – or indeed those who craft creative interventions – to be so rewarding for rethinking how to do information security. I often wander around a gallery or exhibition in my spare time, and just stepping outside of the confines of what we typically consider as information security to be so rewarding. This is because, ultimately, information security must be as complex and nuanced as the people and communities that we work with. This means that some of the solutions will be technical as much as some will be social, political, as well as artistic. This has made moving to London such a great experience – as it gives me much greater access to art from across the world on my doorstep!

EXPANDING OUR INTERNATIONAL COMMUNITY VIA THE INTERNATIONAL CYBERSECURITY CENTER OF EXCELLENCE (INCS-COE)

Konstantinos Mersinas

> Senior Lecturer ISG

Royal Holloway is one of the six Founding Members of the International Cybersecurity Center of Excellence (INCS-CoE), along with Imperial College London (UK), Keio University (Japan), Kyushu University (Japan), UMBC (USA) and Northeastern University (USA). Keith Mayes, former ISG Head, initiated the formation of the Center with the aforementioned universities. I am currently the Royal Holloway board member.

Since its creation, INCS-CoE has identified research on 'issues and problems related to cybersecurity' as one of its main purposes. In this spirit, the network of affiliate institutes has expanded to 12, to include University of Cambridge and Queen's University Belfast (UK), University of Limoges (France), Technion Israel Institute of Technology and Ben-Gurion University (Israel), and Edith Cowan University (Australia). In parallel, there is a growing community of experts formed by individual researchers from founding and affiliate member institutes.

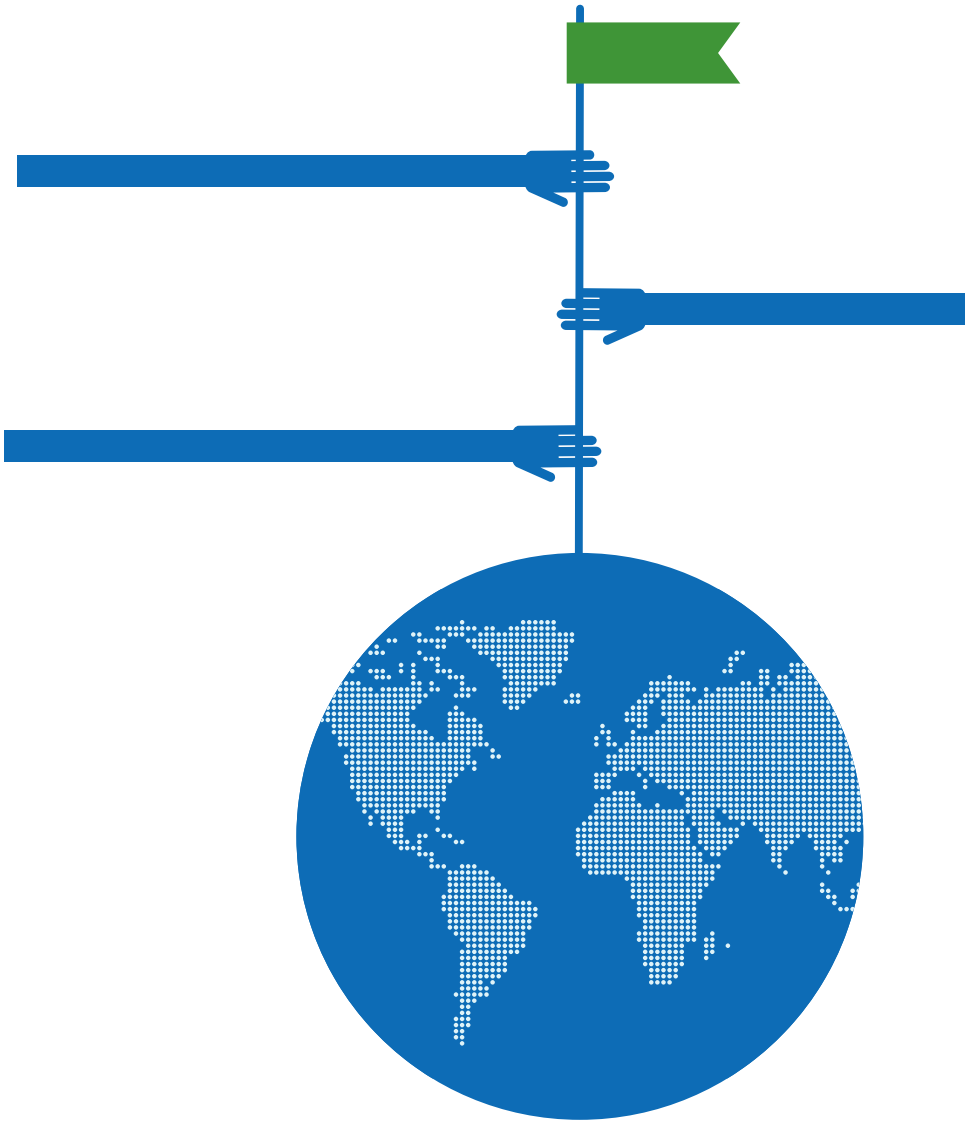
In August 2023, the Country-to-Country Capture-The-Flag (C2C CTF) competition is hosted at Keio University, Tokyo. This year, the competition is particularly important as it will be held in-person, for the first time in the last 3 years. The C2C CTF is a hacking competition which is carried out over 24 hours, between teams of students enrolled in full-time degrees all over the world. Royal Holloway students have been a part of the top 3 teams for the last 3 competitions, and all levels of studies are represented, from bachelors to PhD. The ISG's Darren Hurley-Smith leads the C2C CTF activities at RHUL, and Jassim Happa is a member of the organising committee, coordinating UK universities with the hosting institutions to ensure that the event run smoothly.

The CTF offers our students the opportunity to meet other cyber security enthusiasts from across the world. The competition is becoming a truly international event: registrations to the competition reached 250 students from UK, US, Japan, France, Israel, Australia, India, Malaysia, and Indonesia, representing 45 universities.

The Center of Excellence serves as a point for research collaborations. In this spirit, INCS-CoE funded two research projects this academic year: 'Enabling Trust in Autonomous Cyber-Physical Systems through Verifiable Neural Networks' and 'International Digital Trust Interoperability between US, UK and Japan'. Research activities are further being promoted via a thread of recently established research seminars on issues such as maritime security, IoT security, and IT and OT for manufacturing technology. We are continuing the vision for INCS-CoE to serve as a hub for connecting researchers and fostering collaborations.
https://incs-coe.org/

INCS-CoE

HIVE



MAKING SECURITY SUSTAINABLE

Jassim Happa

> Lecturer ISG

The term ``sustainability'' traditionally refers to the protection of the environment or economy. If we broaden our perspective and apply the concept to security, other concepts might emerge, such as: security under resource constraint, long-term security, security with limited environmental footprint, or security to protect the stability and growth of society. However, very little work has examined how to sustain the security of systems. The work we are doing in this space aims to re-contextualise security with sustainability in mind as a key component of protecting systems.

There are many approaches to build security. Two common paradigms include:
1) “defence in depth”, i.e., building systems with a layered security model, akin to how fortresses have an outer wall and potentially multiple walls inside as well; and 2) “loosely coupled & highly cohesive”, i.e. building systems whose components can operate independently, but together function greater than the sum of their parts. Many more paradigms, frameworks and standards exist, but notably few propose how to make the security last long term, and this is far from a new concern. Many systems built in the 1970s and 1980s are still active today, including industrial control systems such as Supervisory Control and Data Acquisition (SCADA) have long struggled with managing security of legacy systems. Legacy systems still in use may have vendors who have long since folded or moved on, leaving those systems unsupported. Some system maintainers therefore resort to binary hardening by hiring experts who specialise in older programming languages to reverse engineer old-system binaries and make them more secure. Needless to say, this is not a particularly sustainable solution to security. Sustaining security of systems is a complex and dynamic task that involves many challenges. Example concerns include:

• Attack surface expansion. As systems become more interconnected and complex, they also expose more entry points for attackers. This requires monitoring, assessment, and mitigation of risks across the entire system lifecycle – perhaps also after the intended end-of-life of the system in question.

• Attacker/defender arms race. As attackers improve their capabilities, they can evade present-day detection and prevention mechanisms. This arms race continually requires new responses from defenders.

• Evolution and reframing of security practices. As systems evolve and change over time, so do the security requirements and expectations of stakeholders. This requires security practitioners to adapt to new contexts, regulations, standards, and best practices.

• Adapting to emerging technologies. As systems move on to emerging technologies such as cloud computing, edge computing, 5G, autonomous vehicles and Internet of Things, they also face new challenges such as scalability, interoperability, reliability, and privacy. This requires practitioners to rethink how they design, deploy, and manage systems using these technologies, as well as how they balance innovation with security.

The bigger question that needs answering here is: how can we keep systems secure for the long-term? Generally speaking, the answer has been to not do so – instead, we tend to build new products (hardware and software) and we require stakeholders to move onto those platforms. This can be a difficult endeavour, especially for organisations responsible for safety-critical functions. Today, the capability leaps between each new generation of technology are nowhere near as great as they were in the late 20th century. We should therefore be able to afford security that is able to last longer.

Another answer has been to follow good security practices, and then the systems will be easier to maintain – and thus easier to sustain. Recent work aimed at building more robust and resilient systems can enable them to “cope with” and “recover from” adverse effects, but none of these efforts examine how to do so long term, or even estimate how long those efforts are valid for. Furthermore, recent discussions on the DIE triad (Distributed, Immutable, Ephemeral) suggest we should now also reconsider how we conduct asset management in the first place, in order to make the attack surface leaner. This allows for more efficient recovery but still fails to recognise the need for sustaining security.

Last year, as part of a RITICS fellowship (https://ritics.org/), we conducted a series of workshops that examined security experts’ opinions about what the concept “sustainable security” might include.
We explored terms such as Adaptability, Adoptability, Agility, Assurance, Autonomy, Dependability, Durability, Eco-friendliness, Economical, Extendability, Learnability, Longevity, Maintainability, Memorability, Predictability, Reliability, Resiliency, Resourcefulness, Robustness, Self-sufficiency and Usability, and the degree to which they can help us understand what makes security sustainable. As part of this work, we also circulated a questionnaire in which we obtained professional opinions on this topic, including their rating of what such a term might be comprised of, and whether considering sustainability for security can be useful if well-defined, and in example scenarios.

Our preliminary findings suggest that the concept (broadly speaking) makes sense and likely involves the reduction of resources necessary to provide security services while optimising their capacity and use. The concept likely exists across infrastructures and organisation processes and is multi-faceted with both technical and social factors playing vital roles. We are currently developing a framework with a set of guiding principles, a set of metrics and exploring how novel tools can aid systems developers to build systems that intrinsically remain secure and are straightforward to maintain. We hope to publish this in the coming months, and are keen for feedback from security practitioners, developers, and researchers alike.

CDT IN CYBER SECURITY FOR THE EVERYDAY SHOWCASE: APRIL 20TH 2023

Keith Martin

> Prof. ISG & Director of the CDT

The EPSRC Centre for Doctoral Training (CDT) in Cyber Security for the Everyday was delighted to host the return of our annual Showcase as an in-person event at Cumberland Lodge in Great Windsor Park. The CDT funds around ten PhD research studentships each year, with each cohort of researchers undertaking an immersive year of training in cyber security, followed by three years of research. The Showcase welcomed members of the CDT, colleagues at Royal Holloway, and external partners, to learn about some of the fascinating work being undertaken by researchers across the CDT cohorts, and across the many disciplines that relate to cyber security.

The opening session featured presentations by several students who have already commenced their studies. Nicola Bates discussed her use of `systems thinking' to improve the accessibility of knowledge in the cyber domain for key organisational decision makers. Giuseppe Raffa then presented his work on evaluating the effectiveness (sometimes ineffectiveness due to significant delays in reaction times) of various anti-virus software packages for Linux. Rebecca Hartley introduced her research on how place-based digitalisation projects such as smart and connected cities are conceptualised, examining sometimes hidden issues, such as considering whose security concerns are really being represented by the narratives underpinning these initiatives. Finally, Taylor Robinson set out her plans to investigate how digital technology impacts the security of the many (35%) `female-headed' households in Thailand, who are often marginalised through social stigmatisation, and represent a large, but previously unstudied, online community.

We then heard from the newly-formed Digital Security in Latin America (DSLA) Group, established by three CDT researchers (Jamie Barr, Sofia Liemann Escobar, Jessica McClearn) who have, co-incidentally, based their projects around different aspects of cyber security in Latin America. The DSLA aims to bring together researchers across the world who have interests in aspects of digital security of societies throughout Latin America. Beyond knowledge sharing, the DSLA aims to establish a network of interest in this area, and has already held an inaugural workshop which brought together over 30 researchers from Latin America and elsewhere who discussed regional cyber security policy and the impacts of political change in the region. The DSLA also aims to conduct short studies that traverse individual interests of its members, and has investigated and reported on the activities of the Guacamaya hacktivist group, as well as cyber security issues arising from recent elections being held in countries within the region.

The last session before lunch featured five-minute lightning talks by thirteen new CDT students in the first training year, who had recently completed six-week mini-projects on topics of their choice. These provided an excellent overview of the breadth of work being done by the CDT and included work on cryptographic support for anonymous networks, the imbalance between perceptions of risk by designers and users of secure messaging protocols, reasons behind the failure of the UK track-and-trace technology, how to strengthen the security of Automated Identification Systems in shipping, improvements in cyber-criminal profiling, cryptographic proofs based on functional encryption, identifying gaps in research on cyber economic espionage, speeding up homomorphic encryption, benefits and risks of using gamification in cyber security, limitations of current evaluations of trusted execution environments, measuring effectiveness of cyber security strategies, and vulnerabilities arising from dependencies in software development. Wow! It was definitely time for lunch, especially as this was held in the sunny courtyard behind the main building while Red Kites soared overhead …

The afternoon began with a poster session, providing an opportunity for guests to discuss research projects directly with those undertaking them. It was hard to bring the room to order for the next set of presentations, so the posters evidently went down well!

The first afternoon presentation was another testament to cohort building within the CDT, as three first-year researchers presented their joint work on exploring security attitudes amongst software developers. Their research seeks to determine to what extent software developers are concerned with security, how they engage with automated toolkits, and what sources they trust when confronted with security issues. The work represents a collaboration between two Computer Scientists (Cameron Jones and Sam Smith) and one Social Scientist (Mikaela Brough), with the latter providing guidance on research methodology, particularly on interview design and data analysis.

Next up was Marcos Tilleria, bravely presenting the (at the time unfinished) story of his PhD journey on the day before his PhD viva! Marcos' thesis concerns security and privacy in app-based ecosystems, and he gave a short overview of the main findings. Marcos developed novel frameworks for information flow analysis in new platforms such as Android Wear and Android TV. His frameworks have helped uncover new issues in both platforms, including very worrying privacy practices in the apps being developed for the Android TV platform. He has also developed new benchmarks to help other researchers evaluate their proposals for similar flow analysis for these devices. He then went on to discuss his personal experience of undertaking a PhD during the pandemic. He framed this as the good: the `best experience of my life' in going through the intellectual and personal challenge of a PhD, with special thanks reserved for his supervisory support; the bad: the awkward process of `divorcing' from his initial supervisor, and how this process taught him to always communicate with others when difficulties present themselves; and the ugly: the mental stress and loss of opportunities experienced during the height of the pandemic. We are very pleased to postscript Marcos' story with the news that he passed his viva with flying colours.

The last presentation was by CDT graduate Amy Ertan, who titled her talk `The CDT and Me'. Amy overviewed her thesis work on exploring the security implications of artificial intelligence in military contexts. She also discussed her current role as a policy officer in NATO Headquarters in Brussels, where she is tasked with providing a strategic view of the cyber threat landscape and considering what NATO can do to defend against potential threats. She reflected on how motivational her experience on the Cyber 9/12 Policy competition event was in determining her future career. Her advice to current researchers was to embrace every opportunity to experience different environments (whether on CDT visits, internships, or fellowships) and to practice presenting in different ways, since it is these experiences that best prepared her for life beyond the thesis. However she cautioned that while facts and arguments can deliver an excellent PhD thesis, in the workplace an ability to influence others is also necessary, otherwise the best facts and arguments can so often be lost in the wider debates. This is something we have noted for possible future CDT training.

At the close of another fascinating day, everyone was left to reflect on the breadth of work being undertaken in the CDT, having revelled in the opportunity to discuss it in person rather than through a maze of shifting squares on a digital screen. Located in the magnificent former residence of the Rangers of the Great Park, we were also humbly reminded of the march of history and how today's research speculations and formulations will soon become the target of reflections on past work by future scholars. Please look out for details of next year's event – do get in touch if you wish to be added to our invitation list (CyberSecurityCDT@rhul.ac.uk).


THE ISG SMART CARD AND IOT SECURITY CENTRE (SCC)

Konstantinos Markantonakis & Joshua Yewman

> Prof. ISG & Director of the SCC
> Research Assistant ISG

The Smart Card and IoT Security Centre is continuing its dedicated effort within the ISG to promote commercialisation, research excellence, impact, and student engagement activities. In 2022, we celebrated the achievements of our active and previous research projects. Seclea, which offers a new platform to de-risk the adoption of artificial intelligence algorithms, led by Dr Raja Naeem Akram, continues to be a successful company with multiple employees, and looks to welcome new employees in the coming year. We are currently looking for students within the ISG and Department of Computer Science to join our other project PrineSec, which generates a real-time analysis of an organisation's security and privacy compliance using causality chains to accelerate the growth from proof-of-concept to ready-to-market product.

As we reflect on the past year's achievements, we would like to extend our heartfelt gratitude and appreciation to Dr Carlton Shepard for his invaluable contributions to the Tensorcrypt project and the SCC's research efforts in the European Horizons 2020 project EXFILES. As Dr Shepard embarks on a new chapter in his career as a Lecturer in Computer Science at Newcastle University, we celebrate his many accomplishments and lasting impact on our community. Please join us in extending our warmest congratulations and best wishes to Dr Carlton Shepard as he begins this exciting new journey!

We also want to congratulate Dr Darren Hurley-Smith on his promotion to Senior Lecturer in Information Security. Darren has also been appointed as the Technical Director of Omnidrome. Omnidrome is a Research and Innovation Centre for world-leading research, innovation, education and knowledge exchange for air, land, and water-based drones. The Omnidrome Research and Innovation Centre will allow Royal Holloway to meet the future needs for challenge-led research and innovation in areas such as drone and sensor technology, Robotics, and Artificial Intelligence.

Prof Markantonakis has embarked on a three-year appointment as the Director of the "Transformative Digital Technologies, Security and Society Catalyst", responsible for coordinating multi-disciplinary research across RHUL. The Digital Catalyst enables colleagues to present ideas for research and impact collaboration, and amongst its success stories is the creation of the Omnidrome research and training facility. The ISG, via Prof Markantonakis, is also acting as the secretariat for the All-Party Parliamentary Group (APPG) on Cyber Security.

Over the last three years, the SCC has been involved in the EU Horizon 2020 EXFILES consortium, which unites law enforcement agencies, universities, and the private sector towards developing novel mobile forensics methods. The project has critically examined existing approaches that often contain unrealistic practical assumptions making them unsuitable for deployment without extensive time and expensive equipment. Dr Carlton Shepard and Prof Konstantinos Markantonakis led the publication of the first comprehensive analysis of physical fault injection and side-channel attacks on mobile devices. This work has continued into the final stages of the project involving the public dissemination of the research carried out by the project, and research into the legal and ethical aspects of the research. We have been joined by three new Research Assistants, Joshua Yewman, Amir Rafi and Gozde Hussain, to assist in our final contributions to the project. Joshua and Amir, both members of the SCC, have been working on the dissemination aspects of the project, while Gozde, along with colleagues from the Department of Politics and International Relations (including Dr Jonathan Seglow), have been examining the ethical and legal aspects of the project. The first public engagement event held at Royal Holloway for the EXFILES project will be on the 17th of May, 2023, and will focus on ethical and legal challenges around public security, cybersecurity, and privacy relating to the project.

We have welcomed two PhD students to the SCC this year: Amir Rafi, after completing his MSc in Information Security at Royal Holloway, and Zhanyu Sha, having completed his MSc in information security at King's College London before joining the SCC for his PhD.

The focus of our existing challenge-led research in mobile prototyping and RISC-V development platforms has continued to expand. Carlton and Joshua have successfully developed proof-of-concept attacks for the RISC-V architecture, including successfully profiling the complete RISC-V instruction set to reconstruct executing instructions based on power analysis alone.

The SCC continues to pursue EPSRC grants, including the CHAINFRAIN and HEAL proposals. CHAINFRAIN is an EPSRC open-call proposal focusing on road freight and theft prevention in that domain. A key challenge that will be addressed is transporting and processing confidential vehicular and cargo data across European borders. HEAL is an EPSRC proposal to develop innovative artificial intelligence technologies to accelerate health research.

Last but not least, the SCC has acquired a class 4 laser etcher and a wire bonding station that will extend our capabilities in side-channel analysis by allowing us to directly probe integrated circuits after a chip has been decapsulated!

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.

RISC-V INSTRUCTION DISASSEMBLY USING POWER ANALYSIS

JOSHUA YEWMAN

> Research Assistant ISG

Hardware security is an ever-growing concern, not just for manufacturers but for consumers as well. Mainstream media brought hardware security to broad public attention in 2018 with the discovery of the Spectre and Meltdown attacks for the x86 architecture.[1]

Side-channel analysis, such as power analysis, has been an active field of research since 1998.[2] Power analysis involves observing the current draw from microprocessors to retrieve data from the chip during execution, such as the secret keys used in cryptographic algorithms.[3] The work described in this article builds upon previous efforts in profiling ATMega163 and 24C256-based smart card processors[4] by the SCC, as well as research conducted by Dr Carlton Shepherd (now of Newcastle University) on RISC-V remote attestation.[5] RISC-V is a relatively new RISC architecture, with the initial instruction set released in 2011[4]. This architecture differs from its counterparts, such as x86 or ARM, since RISC-V is an open-source framework. The open-source framework of RISC-V allows manufacturers to develop and produce processors conforming to the RISC-V specification with no licensing fees, and to incorporate unique add-on functionality such as integrating hardware-based cryptography, graphics and networking.

Along with Dr Carlton Shepherd and Prof Konstantinos Markantonakis, we developed a method of profiling every instruction within the RISC-V instruction set with the intention of reverse engineering currently executing programs on a HiFive RISC-V chip by observing only the current draw of the chip. An automation method was created to collect individual traces to reduce the time required to profile each instruction. To analyse each instruction, a software toolkit was developed to trigger an oscilloscope to capture the current trace for each instruction 250 times and save the data in CSV format for analysis. The number of collected traces is somewhat arbitrary in that the number of captured traces for each instruction can be changed. However, an increase in collected traces increases the accuracy of the analysis.

Once data collection from the device is complete, the toolkit can import the collected traces and perform template learning using scikit-learn.[5] Using this method, a trained model is produced based on the profiled power traces for each instruction. Instructions can then be executed again on the RISC-V chip to verify the model's results, and the data collected is then correlated to the most likely instruction. The result of this analysis enables both pre-collected and real-time power traces to be correlated to their respective power consumption curves without any knowledge of the device's current instruction or program.

There is still yet more to be done with this research. The chip used is a HiFive SoC with no other executing operations other than the uploaded assembly programs. This contrasts with other RISC-V implementations that allow a complete Operating System (most often Linux) to be used. The decision to profile a device without background processes or operations was made to simplify gathering "clean" traces, where the target instruction is the only operation that the processor executes.

The collection of power traces from this board does not limit the findings or scope of the research, as this research provides a proof-of-concept model with evidence to confirm that executing instructions on a RISC-V-based processor can be identified solely based on the observed power consumption. As with smart card power consumption profiling, this work can be used to ascertain a platform's overall behaviour and enhance verification and secure application execution.

I want to thank Carlton and Kostas for their continuing support and assistance in this research. If you are interested in finding out more, please do get in touch at joshua.yewman@rhul.ac.uk

1 BBC, "Meltdown and Spectre: How chip hacks work," BBC, 04 01 2018. [Online]. Available: https://www.bbc.co.uk/news/technology-42564461.
2 P. C. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," Annual International Cryptology Conference, vol. 1666, p. 388–397, 1999.
3 H. J. Mahanta, A. K. Azad and A. K. Khan, "Differential Power Analysis: Attacks and Resisting Techniques," , 2015. [Online]. Available: https://link.springer.com/chapter/10.1007/978-81-322-2247-7_36. [Accessed 25 4 2023].
4 A. Waterman, Y. Lee, D. Patterson and K. Asanovic, "The RISC-V Instruction Set Manual. Version 1.," 13 05 2011. [Online]. Available: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2011/EECS-2011-62.pdf.
5 scikit-learn developers, "scikit-learn," scikit-learn developers, 23 04 2023. [Online]. Available: https://scikit-learn.org/stable/getting_started.html.

DISTANCE LEARNING MSC IN CYBER SECURITY UPDATE

Fauzia Idrees Abro
& Daniel Miller

> Senior Lecturer ISG & Director
MSc Cyber Security (Distance Learning)
> Distance Learning Administration Manager

Introduction

In October 2022, 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. 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:

01 Cyber security foundations;
02 Applied cryptography;
03 Network and infrastructure security;
04 Computer systems security;
05 Security management and governance;
06 Cybercrime;
07 Software and application security;
08 Research methods for cyber security;
09 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. Students also have the option to interact with each other and the academic staff through group discussion forums on Coursera.

In parallel with the ten MSc modules, we are also delivering six Massive Online Open Courses (MOOCs) together with a 'specialisation' in Cyber Security. The six MOOCs are:

- MOOC1: An introduction to Cyber Security, prepared by Chris Mitchell (launched i n June 2022);
- MOOC2: Introduction to Applied Cryptography, prepared by Keith Martin (launched in November 2022);
- MOOC3: Introduction to Computer Security, prepared by Peter Komisarczuk (launched in March 2023);
- MOOC4: Introduction to Network Security, prepared by Guido Schmitz (launched in April 2023);
- MOOC5: Security Management and Governance, being prepared by Andrew Dwyer (to be launched in June 2023);
- MOOC6: Cybercrime, being prepared by Konstantinos Mersinas and Martin Warren (to be launched in August 2023).

The specialisation requires students to take MOOCs 3-6.

Current Status

During our first intake in October 2022, we launched CYM010 Cyber Security Foundations and CYM040 Applied Cryptography. In January 2023 we launched two more modules: CYM050 Network & Infrastructure Security and CYM060 Computer Systems Security. The second intake of the programme was launched in April 2023 with one further new module, CYM020 Cyber Security Management and Governance, together with one revised module: CYM010 Cyber Security Foundations. We will launch two more modules in autumn 2023 and the remaining three in 2024. This will complete the module development phase of the programme. We will then focus on further improving modules wherever possible to cater for the rapidly growing cyber security market.

We have also completed four out of a total of six MOOCs and will complete the remaining two MOOCs by August 2023. We also aim to launch the specialisation by October 2023. This will complete the development of the open content that complements the MSc.

The programme has attracted many applications in both intakes, and recruitment has significantly exceeded projections; the number of registered students less than a year after launch is double that anticipated. Our first ever MOOC, Introduction to Cyber Security, launched in June last year, has attracted around 10,000 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

Finally, an extra feature deriving from our partnership with Coursera is the provision of MOOCs in addition to the regular modules that make up 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.

Conclusions

Currently, Royal Holloway runs four distance learning programmes, of which the Cyber Security MSc is the most popular in terms of applications per intake. To our knowledge, the programme is the first DL MSc in Cyber security which utilises Cyber Range to give students a realistic experience of cyber-attacks. With our dedicated specialist staff, and demand that exceeds expectations, the programme has incredible potential and we look forward to an exciting journey ahead.

THE OAUTH SECURITY WORKSHOP

Guido Schmitz

> Lecturer ISG

The Open Authorization Framework (OAuth)[1] is an indispensable protocol suite for authorisation as well as authentication. Many services protect access to their interfaces and APIs with OAuth, and users login to applications and web interfaces using OpenID Connect, a widely-used single sign-on protocol with OAuth at its core.

At first glance, OAuth might look quite simple. At a high level, the default protocol flow for a user to authorise a service (say, A) to access their resources at another service (say, B) is as follows. Service A redirects the user to the website of a central authorisation service. On this website, the user consents to A being granted access to the resources at B, and gets redirected back to A along with some code. Service A then redeems this code for an access token at the authorisation service. Service A then uses this access token as a credential when accessing the user's resources at B.

However, even after several security analyses had deemed the logical core of this mechanism to be secure, our research[2] revealed several severe vulnerabilities that allowed an adversary to obtain credentials exchanged during the OAuth flow.
In contrast to previous analyses of OAuth, we employed formal methods to rigorously reason about well-defined security properties. Our work is based on our Web Infrastructure Model (WIM)[3], which allows us to not only take subtleties of the Web into account but also enables us to formally prove strong security properties within a well-defined model. The WIM also helped us pinpoint the issues to specific points in the protocol flow, develop fixes, and prove that our proposed fixes are indeed sufficient.

After reporting our findings in late 2015 to the relevant standardisation body, the OAuth working group of the Internet Engineering Task Force (IETF), the chairs invited us to present our results at an emergency in-person meeting in Darmstadt, Germany, with selected core members of the working group, who travelled from all over the world. At this very productive multi-day meeting, we had several intensive and fruitful discussions, not only on our findings and alternative mitigations but also on future developments and extensions of the standard. While we brought the fixes to the standard on their way to becoming an RFC, it became clear that with future versions and stronger attacker models in high-risk settings (such as online banking), there is a continuous need for security reviews and in-depth security discussions. This insight has motivated us to initiate a new workshop series to foster exchanges among researchers, the OAuth working group (and other related standardisation bodies), and the broader user base in industry: the OAuth Security Workshop (OSW).

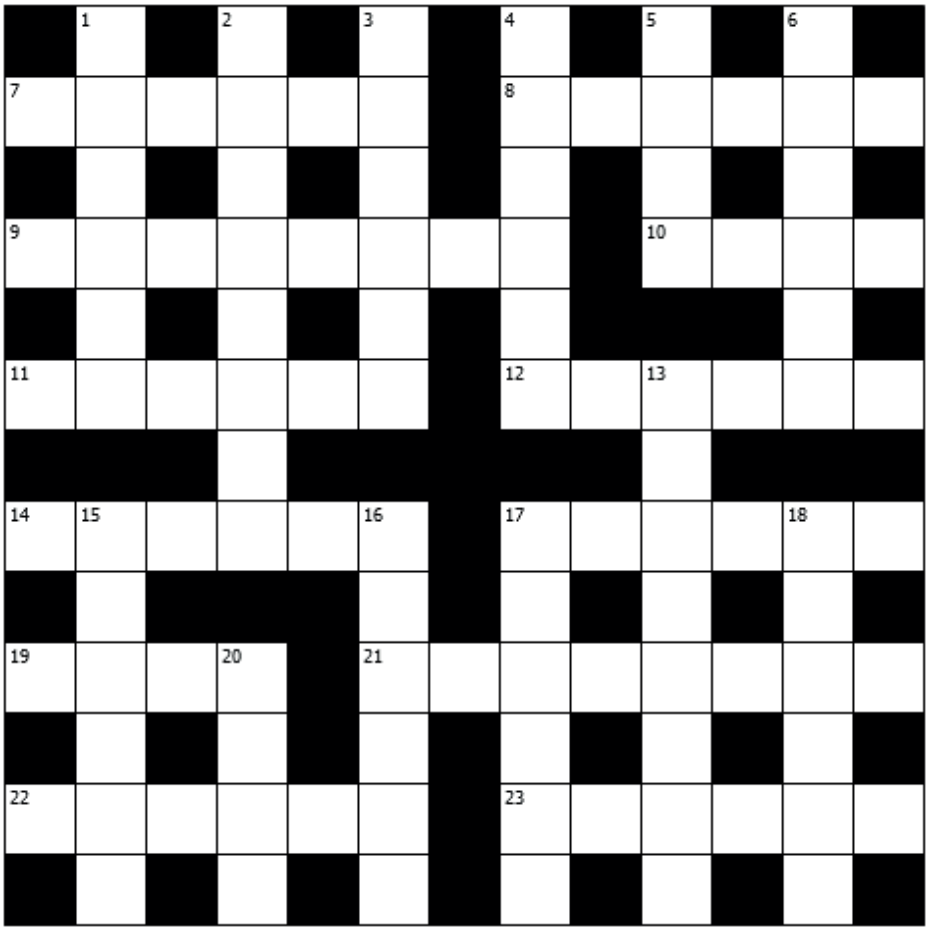
While the meeting in Darmstadt could be regarded as the very first OSW, we held our official inaugural event in 2016 at our then-home institution, the University of Trier, Germany. Since then, the OSW has taken place annually at various locations, including ETH Zurich and the University of Stuttgart. The agenda of the OSW consists of classical conference-style talks, hands-on workshop sessions, and numerous barcamp-style sessions that allow for ad-hoc presentations and discussions. This unique mix is highly valued by our participants and has facilitated many fruitful debates and sparked the development of several new RFCs.

The next OSW will be hosted by the ISG on-campus in Egham on August 22-24, 2023. For more information, please visit the event's website: https://oauth.secworkshop.events

1 Dick Hardt, "The OAuth 2.0 authorisation framework," IETF, 2012, RFC6749.
2 Daniel Fett, Ralf Küsters, and Guido Schmitz, "A Comprehensive Formal Security Analysis of OAuth 2.0," in Proceedings of the 23rd ACM SIGSAC Conference on Computer and Communications Security (CCS 2016), 2016, pp. 1204--1215.
3 Daniel Fett, Ralf Küsters, and Guido Schmitz, "An Expressive Model for the Web Infrastructure: Definition and Application to the BrowserID SSO System," in 35th IEEE Symposium on Security and Priv

SHIFT WORK II
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 (6,6); the letter C, for example, means A should be encrypted as C, B as D, etc.

Two entries appear *en clair*.

Across

7 Grain typically used to make whisky (6)
8 Temporary store for data (6)
9 Amphibian (8)
10 George _____, French writer (4)
11 Follow and watch (6)
12 Meeting point of lines (6)
14 Half a beat (6)
17 Impoverished individual (6)
19 Test to check accessibility of network nodes (4)
21 What one has to do? (8)
22 Intimate (6)
23 Member of domestic staff (6)

Down

1 Strong dislike (6)
2 Protector (8)
3 Invasive bird species? (6)
4 Place of worship (6)
5 Smallest non-negative number (4)
6 Sharpness (of vision) (6)
13 Food fish rich in Omega-3 fatty acids (8)
15 Ten years (6)
16 Head covering worn by nuns (6)
17 Non-expert (6)
18 Insole (anagram) (6)
20 Style of music using syncopation and improvisation (4)

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/