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

I must first give huge thanks to my predecessor as Head of Department, Professor Peter Komisarczuk, for his tireless efforts in leading the department through some very difficult times over the last three years. When he took over as head back in the summer of 2018 he had the unenviable task of overseeing the move to online teaching and a January student intake happening almost overnight. That we have survived largely intact is a miracle in itself, and is down to Peter’s leadership and the hard work of all our colleagues. It has been another very challenging year for the department, and, of course, for the world. Whilst we have largely moved back to campus teaching for the 2021/22 academic year, we are still feeling the effects of Covid-19. We have had to continue live-streaming all lectures for the benefit of students unable to make it to campus, and some colleagues have been obliged to continue delivering material online as they are and/or their partners are vulnerable. In January 2022, our second cohort of ‘January start’ MSc students arrived, meaning that for the second year in a row we are teaching every masters course twice (and those in block mode three times). We have had to continue live-streaming all lectures for the benefit of students unable to make it to campus, and some colleagues have been obliged to continue delivering material online as they are and/or their partners are vulnerable. In January 2022, our second cohort of ‘January start’ MSc students arrived, meaning that for the second year in a row we are teaching every masters course twice (and those in block mode three times).

There are also many exciting new developments in teaching and research to report. We are in the process of launching a new distance learning MSc in Cyber Security jointly with the University of London and Coursera, as reported on in more detail in Keith Martin’s article in this newsletter. The Centre of Doctoral Training continues to go from strength to strength (see Keith Martin’s article later in this newsletter). Late last year the ISG received an Academic Centre of Excellence in Cyber Security Education (ACE-CSE) Gold Award recognising excellence in cyber security education and good practice from the National Cyber Security Centre (NCSC). Also, by the time this newsletter reaches you, the ISG will have another new Head of Department, as my short-term interim headship comes to an end, and I wish her or him all the very best in further developing and enhancing the work of the department.

In summary, despite the huge difficulties over the past couple of years, we find ourselves in a great position to continue to grow and develop, and this newsletter provides an overview of some of our many activities. We hope that you enjoy the articles, and that if any of the topics mentioned spike your interest, please do get in touch. Exciting times are ahead!
How did you become interested in Computer Science?

When I was in primary school, my parents got me one of these typical 90’s learning computers that run quizzes and other educational programs. It did not take long for me to find out that there was also a BASIC interpreter on this rather cumbersome, as the device only had a 16x2 character display, if fascination came a lot too Alo, I got hold of my sister’s C64, and that classic computer allowed me to learn much more on the topic. A few years later, I joined the local computer club and quickly became the administrator of their network, a perfect playground for me and the many different things. I discovered also my passion for teaching there and held programming courses.

How did you become interested in Information Security?

While working with networked environments, security became a hot topic for me. During my computer science studies at the University of Trier, I also worked part-time as the computer science department’s system administrator and became responsible for some central infrastructure, including some production systems of DBLP. Here, security was an essential aspect of my job. As a result, I had a steady flow of questions, and I was able to apply my knowledge and pass it on to others. I realized that I enjoyed sharing my knowledge and helping others.

What are the joy and challenges of being a lecturer?

The academic world comes with many benefits, such as freedom and independence of research and the opportunity to teach and engage with students. However, it also requires a lot of self-motivation and resilience to explore and combine new subject fields of knowledge and to educate new students. While I enjoy teaching, I also find challenges, such as dealing with different learning styles and maintaining a balance between teaching and research.

Tell us about your research.

I have co-authored the web infrastructure module of a comprehensive comparative model of the web infrastructure to data. With the WIM, we have uncovered several severe security flaws in central protocols, including single-sign-on and authorization protocols such as OAuth and OpenID Connect. This research even spanned a new conference series, the OAuth Security Workshop, that I am organizing in collaboration with the IETF.

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

Your research facilitates the discovery of new vulnerabilities. Isn’t that a double-edged sword?

My primary motivation is to make systems secure. This is, in essence, it is essential to have tools to systematically and rigorously analyze a system for its weaknesses. Knowledge of these problems is key to eliminating them and making systems secure. While we might not have such methods at hand, it is up to chance and creativity who finds such problems first. If we're out of luck, the system might already leverage these vulnerabilities without the good team knowing about these issues. Having this research enables the good guys to identify and eliminate problems before they can be exploited.

What is your research focus?

My research focuses on developing methods to identify and analyze vulnerabilities in networked systems. I am particularly interested in analyzing problems in real-world systems and developing tools to help users identify and fix these problems.

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

When the pandemic started, I was teaching in Germany. We didn’t have any experience with distance learning or online teaching in our group. Moreover, we were just a few weeks away from starting teaching in the summer term. The course I was teaching was a master’s course, and it covered the same topics as the course I teach at the University of Stuttgart. I started by creating a series of online lectures that I recorded and made available to my students. I also held regular office hours to answer any questions they had. This approach worked well, and I received positive feedback from my students.

How did you get involved in the ISG?

I was interested in security research, and I was fortunate to find a position at the ISG, where I could work on security-related projects. I have been working at the ISG for over a decade, and I have been involved in numerous research projects and initiatives. I am currently the Director of the Royal Holloway Research Catalyst, and I continue to be involved in various research activities at the ISG.

What are your plans going forward?

I am currently working on several projects related to cybersecurity, including research on new security challenges and developing new security technologies. I am also involved in various industry partnerships and collaborations to help advance the field of cybersecurity. My plans for the future include expanding my research efforts and continuing to work with industry partners to ensure that our research is relevant to the real-world challenges faced by organizations.

What do you think is the most significant investment in your career?

I think the most significant investment in my career is the time and effort I have put into my research and teaching. I have been fortunate to work with many talented students and colleagues over the years, and I have had the opportunity to contribute to several important research projects. My work has helped to advance the field of cybersecurity and has had a positive impact on society.

What do you think is the most significant challenge in your career?

I think the most significant challenge in my career is the need to stay current with the latest developments in the field of cybersecurity. The field is constantly evolving, and new threats and vulnerabilities are emerging all the time. It is essential to stay up-to-date with the latest research and developments to effectively address these challenges.

What are you looking forward to the most at the ISG?

I am looking forward to the opportunity to work with my students and colleagues to advance our research and contribute to the field of cybersecurity. I am also excited about the prospect of working on new and innovative projects that will have a positive impact on society.

How would you describe your experience at the ISG?

My experience at the ISG has been very positive. I have had the opportunity to work with many talented students and colleagues, and I have been able to contribute to several important research projects. The ISG has a strong reputation for research and teaching in cybersecurity, and I am proud to be a part of this institution.

What are your plans going forward?

As an academic, my main focus is on research and teaching. I am currently involved in several research projects and initiatives related to cybersecurity, and I plan to continue to pursue these interests in the future. I am also interested in building new research collaborations and partnerships to help advance the field of cybersecurity.

What do you think is the most significant investment in your career?

I think the most significant investment in my career is the time and effort I have put into my research and teaching. I have been fortunate to work with many talented students and colleagues over the years, and I have had the opportunity to contribute to several important research projects. My work has helped to advance the field of cybersecurity and has had a positive impact on society.

What do you think is the most significant challenge in your career?

I think the most significant challenge in my career is the need to stay current with the latest developments in the field of cybersecurity. The field is constantly evolving, and new threats and vulnerabilities are emerging all the time. It is essential to stay up-to-date with the latest research and developments to effectively address these challenges.

What are you looking forward to the most at the ISG?

I am looking forward to the opportunity to work with my students and colleagues to advance our research and contribute to the field of cybersecurity. I am also excited about the prospect of working on new and innovative projects that will have a positive impact on society.

How would you describe your experience at the ISG?

My experience at the ISG has been very positive. I have had the opportunity to work with many talented students and colleagues, and I have been able to contribute to several important research projects. The ISG has a strong reputation for research and teaching in cybersecurity, and I am proud to be a part of this institution.
In my study of 18 UK-based, but predomin-
antly multinational commercial businesses, I
identified that CIOSs were relied upon to
provide protection for those organisations from
organized cyber threats that were difficult to
understand, even mystical in nature.

The impacts from those threats were consid-
erable, with businesses feeling for the first
time that the threats continued existence as a
result. They desired both interpretation and prediction of those threats to gain a sense of comfort that they
would remain viable.

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

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

These narratives offer a number of benefits to
CIOSs and the cyber-security industry, but also
weaken power structures, which I discuss in
more detail elsewhere [5]. There is, therefore,
a motivation to maintain such narratives, which
may enhance the ‘cyber sophistry’. The CISO-as
soothsayer may have a self-interest in the reali-
sation of their prophecies, which may motivate
unintended, dysfunctional, and yet which could
be a factor of the jeopardous position that CI-
SOs are in, who, as soothsayers, are often
scapegoated.

The CISO-as-soothsayer concept has a num-
er of implications. First, it might be possible to
imagine that the role of a ‘soothing’ – or
indeed ‘policing’ – an organisation, it is a role
more akin to weather forecasting. Second,
managers and practitioners should be con-
scious of the potential for cyber-sophistry and
the unethical outcomes that such practices
may cause. Cyber-security education should either aim
to demystify the subject, or, alternatively, to
encourage the mysticism and logicians who need
the need for specialist interpretation. Adopting
the latter approach may result in staff being in-
structed in the use of systems whose security
with the security aspects of this being implicit
rather than explicit, and certain decisions on
acceptability of risk being deferred to cyber-se-
curity specialists. This is, however, potentially
problematic if it results in users feeling less
responsible for security and depending entirely
on others to protect them from threats which
they themselves powerless in the process.
Fourth, re-
gardless of whether cyber security is a dark art or
not, perhaps systems should be designed on the
basis that their security will need to be
interpreted by a specialist. Often special-
ist parts for domestic goods have a separate
‘information for installer’ section. Employing
this analogy, an ‘information for CISO’ section
could be provided by system designers.

I argue that there is value in acknowledging
the interpretive nature of cyber-security practice
and reclaiming soothsaying as a beneficial
advisory profession, rather than seeing the
form in a negative light. The soothsaying role
of one that many of the CIOSs occupy, and my
research continues to explore the multiple and
often conflicting narratives. Such analytical
lenses from a number of disciplines, including
sociology, international relations and
management theory. I hope to expand my
understanding of the purpose behind such
a varied, misunderstood and important role.

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

The expectation is that developers will
require clients to keep up with API changes.
Unfortunately, despite clear directives in the
documentation of libraries on how client software
should be updated, developers tend to defer
updating clients as they struggle to keep up with
rapidly evolving APIs. A study of 1,2M Android
apps showed that more than 85.6% use older versions
of libraries and, alarmingly, 16K apps used libraries
with known vulnerabilities [1].

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

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

Library Evolution

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

In the following sections, we discuss the
impact of APIs on a project, and the challenges
developers face when removing APIs. A
methodology is proposed to help developers
when removing APIs. This methodology is
expected to lead to more successful
removals, reducing the cognitive load of
developers when integrating with changing
libraries.

Update directives contain a mix of code and
natural language. We need to analyse this
text to identify replacements for deprecated
APIs. Recent advances in mixed-text processing
make it possible to try to parse update directives.
The code is formatted in a formal grammar of
programming languages with Natural Language
Processing to distinguish code tokens from
text [4]. While this is promising, many distinguishing
codes from text is not enough to identify
replacement APIs from update directives.

We need new forms of analysis to find
relationships between deprecated APIs and their
removals from the update directives. A
methodology is proposed to help developers
when removing APIs. This methodology is
expected to lead to more successful
removals, reducing the cognitive load of
developers when integrating with changing
libraries.
LEARNING TOGETHER: CYBERSECURITY FOR TODDLERS
Dr. Elizabeth A. Quaglia

> Senior Lecturer, ISG

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

My goal was to develop material for short, enjoyable and accessible stories that would convey in an intuitive way the basic principles and notions in cybersecurity in a general and cryptographic in particular. The idea for this project takes inspiration from the successful children’s books by Chris Ferrie (https://csferrie.com/), Associate Professor in Physics at the University of Technology Sydney, who has developed a series of “for babies” books, tackling topics such as quantum physics, quantum computing and Bayesian probability in an accessible and visually appealing way.

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

Another event which didn’t happen in the manner of the past was what was previously termed our annual CDT Showcase. Before the pandemic, we held an outward-facing event where the CDT researchers were presented to our stakeholders. In November, partly due to pandemic restrictions and partly due to a need to reconnect with our school, we held an internal residential event at nearby Cumberland Lodge just for members of the CDT. It was a wonderful two days, and a reminder of everything good that is happening – without the need for anyone to move, attending workshops, conferences and events providing opportunities to build personal networks and reputation.

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

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

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

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

One of the highlights of Cumberland Lodge was an impressive team presentation by our CDT researchers. This is exactly the breadth and maturity that we hope for from our CDT researchers.

With this in mind, I was particularly pleased to see that those CDT researchers were among the winning entries in Royal Holloway’s internal COP26 competition inviting students to submit a creative response to climate change and related issues of sustainability. Students were asked to consider the challenge of addressing climate security and the impact that it is having, and will have, in both
The ISG SMART CARD AND IOT SECURITY CENTRE (SCC)
Konstantinos Markantonakis, Darren Hurley-Smith, Carlton Shepherd

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

The Smart Card and IoT Security Centre is spearheading the ISG’s effort in commercialisation, impact and student engagement activities. In 2021, we celebrated several achievements resulting from our challenge-led research activities. Our first project, Seclea, led by Dr Raja Naeem Akram (now Senior Lecturer at the University of Aberdeen) is now a fully-fledged company with several employees. Seclea, which offers a new platform to de-risk the adoption of artificial intelligence algorithms, has received substantial funding from private investors, including Europe’s largest venture capital fund and Innovate UK. The second project, Privisec, a year three project of Innovate UK’s competitive CyberASAP programme, generates real-time analysis of an organisation’s security and privacy compliance using causality chains and is now being applied to IoT security analysis. Our most recent endeavour, Tensorcrypt, led by Dr Carlton Shepherd, enables organisations to securely share and analyse sensitive datasets using confidential computing. Tensorcrypt was also a CyberASAP project (2021/22), winning grant funding of over £730,000 from Innovate UK. A patent application has been filed and a proof-of-concept was successfully developed, which provided employment to three exceptional Royal Holloway undergraduates. The whole journey is a great example of success stories being built from academic excellence and entrepreneurship.

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

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

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

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

Benjamin Semal, our PhD student, recently passed his PhD visa subject to minor corrections. His thesis examined the threats posed by microarchitectural covert channels in multi-tenant computing environments. Benjamin proposed a new framework for evaluating and scoring new threats and developed two new covert channel methods using CPU memory control. His method enables privileged adversaries to leak information across multiple virtual machines within a single native environment [4].

The second extends this to cross-VMC scenarios and was extensively developed. The method attacks resulted in responsible disclosure engagements with Intel, AMD, and Amazon Web Services (AWS).

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

The SCC continues to pursue Horizon and EPSRC grants. ZELDA is a Horizon proposal focusing on the development of novel, trustless network architectures to facilitate decision making using data from heterogeneous mobile and IoT devices. It aims to address significant privacy issues and auditing challenges regarding the transport and processing of confidential vehicular and cargo data across European borders. We hope that this short overview of our recent academic research into privacy and security will excite interest. Please do contact us at scc@rhul.ac.uk if you feel there are areas that we could explore further together.

References
INTERDISCIPLINARY EXPLORATION WITH THE CRITICAL SECURITY READING GROUP
Lizzie Coles-Kemp, Nick Robinson & Ian Slesinger

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

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

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

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

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

When the pandemic started, CSRG members asked that we move the reading group online and run it throughout the year. Moving the reading group online enabled the CSRG to widen its participation, invite authors of papers to join the conversation, and to maintain a consistent and steady presence throughout the academic year. With the CSRG now entering its 3rd year, we are keen to expand our audience and broaden the range of ideas and issues it promotes. Above all else, the CSRG is friendly, supportive and non-confrontational, allowing participants to discuss an array of ideas and issues in an open and relaxed environment.

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

ISG MSC UPDATE
Jorge Blasco Alis

> Senior Lecturer, ISG
Programme Director MSc

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

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

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

As usual, I would like to finish this yearly update on a positive note. Each year the department awards the best project of the year with a special prize. This year, with two cohorts we were very happy to award them two of our students. The prizes went to Chris Underwood and Ioan Bieres. Congratulations!
Security culture can be defined as the totality of human aspects, including behaviours, attitudes, beliefs, knowledge and values, that contribute to the protection of information in an organisation (Da Veiga and Effoh, 2010). Although many authors agree that culture is a subset of organisational culture, and although it has been extensively studied in the industry, studies within academia are less frequent. In a project funded by the National Cyber Security Centre (NCSC), we conducted 19 interviews with professional services / administrative staff, students, academics and senior management members across three Higher Education Institutions in the UK (Durojaiye, Mersinas, Watling, 2021). Our goal was to examine security culture in higher education institutions (HEIs), within the UK, and to identify the complexities of establishing a security culture within HEIs.

University users’ findings

A subset of the study’s key findings is presented here. First, we observe that HEIs have various cyber security-related structures in place, but these are not clearly visible to users. All subjects reported that they know someone to contact in case of a security incident. Most interviewees identified the IT helpdesk as the most appropriate point of contact. However, we found that individuals overall identify too many points of contact, thereby creating uncertainty for users, who communicate with the university in an additional survey. A principal component analysis is that members of staff who are involved more closely with specific processes trust these mechanisms and processes, whereas those who are not involved with the underlying mechanisms are sceptical of them. This further ignited my desire to pursue a career in modern cryptography, and the subject instantly became relevant. This is why I took a course in cryptography at university. The demonstration and profound observation, he taught me to think critically and out of the box. I have fond and unforgettable memories of spending hours playing with the Commodore 64 with my father as a kid. I felt a true sense of belonging with computers and it was great thought given to the design and development of these schemes when they were being thought up. We now know for sure that they are secure.

Second, information exchange and communication on security-related issues is generally insufficient. The term “security entity” is basically unilateral, i.e., from users to the security entity. Communication security messages are vital in nudging cyber security entity’s behaviour. Research indicates that involvement in security processes does influence security culture in organisations, especially if the tenets of trust, cooperation and risk management imply responsibility and ownership (Anathwar et al., 2012).

Building on insights

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

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

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

References


How did you become interested in Computer Science?

Computers have permeated every aspect of my life, and growing up around them sparked my interest in computer science at a young age. My father, who worked in IT, was genuinely enthusiastic about mentioning me, which fuelled my passion. He aroused my curiosity and taught me to think critically and out of the box. Today, I can achieve the “how” by combining technical demonstration and profound observation, he devised new solutions and coached me through the process, I have communicate with the universe in a unilateral fashion (as in the case of reporting incidents). The design and dissemination of security and risk messages to users is also important. Our survey findings indicate students feeling significantly more comfortable engaging in risky cyber behaviours, concerning other user groups. Therefore these messages might need to be customised for target groups.

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

References


How did you become interested in Information Security?

My father was also my first contact with information security. He had (and still has) a small red folder with descriptions of all the known viruses at the time. It was a stack of 20 A4 sheets containing all available information on a single virus. Reading about attack pathways, mitigation measures, and recovery strategies piqued my interest. These thoughts stayed in my head, and I was eventually determined that not only would I study information science but also study security. I’m not sure when it started, but I’ve always visualised a future in information security research. This decision was reinforced in the final year of my undergraduate studies, where I took an elective module in Information Security. This is where I first learnt about modern cryptography, and the subject instantly captivated me.

How did you cope with the impact of the pandemic?

As a PhD student, the pandemic had both positive and negative impacts. For example, I’m now working on Witness Encryption and its sequel Smart Encryption, which are (relatively) new primitives.

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

The world of computing and information and disruption are inevitable. The digital world is evolving at breakneck speed. This means that, as academics and researchers, we must either foresee the future or spend time playing catch-up. While it is notoriously difficult to forecast the future, we can nevertheless forecast what will happen. I’m currently interested in the development of new cryptographic primitives, such as the “Smart Encryption” project I’m working on now.

How did you cope with the impact of the pandemic?

As a PhD student, the pandemic had both positive and negative impacts. For example, I’m now working on Witness Encryption and its sequel Smart Encryption, which are (relatively) new primitives.

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

The world of computing and information and disruption are inevitable. The digital world is evolving at breakneck speed. This means that, as academics and researchers, we must either foresee the future or spend time playing catch-up. While it is notoriously difficult to forecast the future, we can nevertheless forecast what will happen. I’m currently interested in the development of new cryptographic primitives, such as the “Smart Encryption” project I’m working on now.

How did you cope with the impact of the pandemic?

As a PhD student, the pandemic had both positive and negative impacts. For example, I’m now working on Witness Encryption and its sequel Smart Encryption, which are (relatively) new primitives.

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

The world of computing and information and disruption are inevitable. The digital world is evolving at breakneck speed. This means that, as academics and researchers, we must either foresee the future or spend time playing catch-up. While it is notoriously difficult to forecast the future, we can nevertheless forecast what will happen. I’m currently interested in the development of new cryptographic primitives, such as the “Smart Encryption” project I’m working on now.
We were glad to organise another edition of the Winter Networking Event in December 2021, where we heard from two speakers about their career experiences to date. In particular, Dr Elena Iosoglio, from Universita degli Studi di Torino, Italy, walked us through her academic journey, and gave us a taste of her research interest in stochastic differential equations. We also had a talk from Nat M, from NCSC, who shared her experience as a mathematician in various roles, now part of a sociotechnical security group that applies a multidisciplinary approach to delivering security that works in the real world.

This year, the October 2021 welcome event was very well attended, and it was great to see members from across the EPMS welcome guest contributions, so please get in touch via wisdom@rhul.ac.uk if you have something to share.

We would like to thank them for their enormous efforts in driving the group forward. Anyone who is interested in taking a more senior role in Wisdom and continuing their excellent work is invited to get in touch.

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

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

We would like to thank our speakers for their contributions. The speakers joined online, but we were glad to be able to see members in person to watch the talks together. After the talks, the discussions continued over coffee.

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

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

In the early days, the WISDOM group worked hard to establish itself as a network to support and raise the profile of women working in cyber security that works in the real world. This was by hosting now-traditional events, outreach efforts, and socials. The committee representatives work together to organise events, outreach efforts, and socials. The mailing list counts over 100 members, who are invited to attend events and volunteer in outreach efforts. (New WISDOM members are always welcome!)

In the early days, the WISDOM group worked hard to establish itself as a network to support and raise the profile of women working in Information Security and Mathematics at Royal Holloway. One step towards achieving this was by hosting now-traditional events such as the welcome event at the start of the first term, and the Winter Networking Event. This year, the October 2021 welcome event was very well attended, and it was great to meet new faces from across the School.
The Discribe Hub+ has been established to bring to fruition a commercially viable demonstration of the CHERI technology based on the Instruction Set Architecture, while the Discribe Hub + website can be found at https://www.discribehub.org.

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

 hops://msrc-blog.microsoft.com/2022/01/20/ an-armful_of_cherts/
A few years later I met Professor Thomas Rid.

The First of Five PhD Supervisors

experts had been little consulted. I wondered stalled, and the policies that did progress were the next few years, I watched as digital policy preached, must tear down the Internet, our reform, we, the hacker community, Falkvinge If the governments of the world would not amongst the world's most powerful collectives. committed suicide. Falkvinge proclaimed the act. On facing what many considered the elite could scale. But he was caught in online, not bound behind paywalls that only cornucopia of knowledge. He believed the months earlier, Swartz attempted to download displayed a picture of Aaron Swartz. A few Towards the end of his keynote, Falkvinge Gathering in Europe'.

Blackhat & Vitriol

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

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

The First of Five PhD Supervisors

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

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

The Greek Mafia and the ISG

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

First Visit to the ISG

I couldn’t quite believe it. Keith had found not one, but two other potential co-supervisors, one from Royal Holloway’s Department of History, another from the Department of Geography. Together we sat gathered in his office whilst Keith’s dog joked around the room politely keeping out the strangers. As my elation that people were interested in my research subsided, I became worried: How was I possibly going to keep up with them? On joining Royal Holloway I’d already decided this was the project’s last chance. If I were to lose a third supervisor, I would concede defeat. Pursuing research that seemed destined for failure, alongside a demanding full-time job, was just too punishing. I agreed to meet whoever Emmett’s replacement would be out of courtesy, but confided to Keith that I would almost certainly be bringing down the curtain on this project that had haunted me for almost half a decade.

Supervisor Number Five

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

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

A Disruptive Pandemic

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

Supervisor Number Five

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

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

The Digital Cold Shoulder

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

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

The Interviews: Spies, Professors and Lawyers

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

The Viva

Professors Richard Aldrich (external) and Klaus Dodds examined my thesis. They told me at the start of the defense that I was passing, which reduced my heart rate by about 50%. Despite this, the next hours were tough, if enjoyable. I was thrilled that the examiners were so engaged with the subject matter – they’d even read my oft-meandering footnotes! Aldrich and Dodds saw myriad angles that I had not considered, reinforcing to me that whilst at the conclusion of my PhD journey, it was only the end of the beginning of my learning curve as a researcher. I was elated when no changes were requested to the thesis.

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

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

STAFF PROFILE: DR CHRISTIAN WEINERT

Dr Christian Weinert

STAFF PROFILE: DR CHRISTIAN WEINERT

Staff profile: and machine learning inference.

Applications, I helped to provide efficient interactive protocols for specific real-world multi-party computation. By optimising such cryptographic protocols in the area of secure communication, we also discovered several privacy vulnerabilities that potentially affect billions of users worldwide.

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

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

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

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

I mainly work on privacy-preserving security-related courses and decided to do my undergraduate course with almost 1000 registered students to a new digital teaching format that replaces everything from in-person lectures to tutoring sessions and examinations. This worked out quite well, however. It was a massive effort, especially since we had to come up with many custom solutions. Here at RHUL, with the universiy provided and well-integrated communication infrastructure, scheduling meetings works with an ease and results in great interactions. I’m also looking forward to the upcoming summer term and students coming back to campus – it was way too quiet so far.

You recently relocated from Germany to the UK. How is your experience so far?
Apart from hefty visa application fees and several bureaucratic “chicken-and-egg” problems when trying to set up life in the UK, the experience so far is great! I love the beautiful RHUL campus and the surrounding nature. Also, it’s great to have so many supportive colleagues within the ISG and the school office.

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

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

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

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

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

Down
1  Pungent allium (6)
2  Destructive individual who might rout base? (8)
3  Noble gas (4)
4  Uncharged elementary particle with negligible rest mass (8)
5  Inexpensive restaurant (4)
6  More than enough (6)
7  Hot-headed mythical beast? (6)
8  Club sport? (4)
9  Japanese drink/English author (4)
10  Japanese drink/English author (4)
11  Brass instrument (8)
12  Hard shell (8)
13  Japanese drink/English author (4)
14  Japanese drink/English author (4)
15  Fire ______ velocity (6)
17  Japanese drink/English author (4)
19  Japanese drink/English author (4)
20  Japanese drink/English author (4)
21  Japanese drink/English author (4)
21  Japanese drink/English author (4)
22  Greek letter used to denote wavelength (6)
23  Signal used to guide shipping or warn of danger (6)
For further information about the Information Security Group, please contact:

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

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

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

Twitter:
twitter.com/isgnews
@ISGnews

LinkedIn:
linkedin.com/groups?gid=3859497

You Tube
youtube.com/isgofficial

CONTACT INFORMATION:

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

Twitter:
twitter.com/isgnews
@ISGnews

LinkedIn:
linkedin.com/groups?gid=3859497

You Tube
youtube.com/isgofficial