Information Security Group

Review 20/21

ROYAL HOLLOWAY UNIVERSITY OF LONDON

INDEX

WELCOME
Peter Komisarczuk

> Professor ISG, Director, Information Security Group

Welcome to the ISG review. Another year has passed by in a flash and again we have been in interesting times. Certainly, the year has been challenging in many ways due to the COVID-19 pandemic and of course nothing stands still in the field of information security.

The year has seen the ISG teaching, supervising and researching remotely; with most of us working from home for much of the year. Like most universities Royal Holloway has gone online and engaged in "flexible learning" – a combination of online and on-campus, socially distanced learning. Everyone has been busy with video recording and enhancing online materials, online open book exams, blended learning, some flipped classroom engagements and so on. I would like to sincerely thank my colleagues for engaging in this and working tremendously hard throughout the year with patience and flexibility, especially as there have been a variety of changes, often at little notice, dictated by national and global policies and challenges.

As you will see in this issue, we have gone through some changes, including the retirement of Professor Jason Crampton in September and Daniele Sgandurra leaving in December 2020. There have also been a number of highlights throughout the year, with many new research initiatives and successes. Despite the challenges of the pandemic, colleagues have continued to produce high quality research proposals and research papers and provide additional support for their PhD students. Four of our first-year CDT students took the top prize at this year's Cyber 9/12 competition. We rose to the challenges of new initiatives such as the INCS-CoE virtual Country 2 Country capture the flag event, that was led by Daniele Sgandurra, Darren Hurley-Smith, Jassim Happa and Keith Mayes and supported by the CIM IT team and the EPMS School admin team. That was followed shortly afterwards by the 31st (virtual) HP/E Colloquium on Information Security organised by Rikke Bjerg Jensen and Martin Albrecht.

The new year saw our first January-start MSc cohort, a College initiative to help engage students affected by the pandemic. This has meant that we have double taught most modules as well as engaging in all our usual activities (albeit mostly virtually). While it has been a challenge to run our modules twice, it has been wonderful to engage with the 68 new students who joined us in January. The new year also saw the first meeting of our Practitioner Panel chaired by Professor Paul Dorey, and we look forward to working with this panel as we plan for future teaching, knowledge exchange and research activities. March also saw the launch of four new cross-College research catalysts at Royal Holloway. The ISG is primarily involved in the catalyst on "Transformative Digital Technologies, Security and Society" which has information/cyber security as a core pillar and began with a virtual meeting of over 80 researchers from across the College. Then, April saw the new MSc Cyber Security Project Management degree pass through the academic quality process, and we look forward to the first cohort arriving in September.

We hope that you enjoy the articles in this edition of the ISG review, as exciting as any other year, but also in many ways more challenging than expected.

JASON FAREWELL

Prof. Jason Crampton retired from Royal Holloway last year after almost two decades with the ISG. We wish Jason all the best for his retirement and thank him for his many contributions. We caught up with Jason for this year's Newsletter.

//

How did you end up joining Royal Holloway?
I joined Royal Holloway a few months after completing my PhD. Chris Mitchell was one of my examiners and also on the appointment panel, so I'm sure it helped that Chris was aware of my research and my research interests. At the time Royal Holloway had many excellent cryptographers but not many people who were specifically interested in computer security, so I was lucky to be in the right place at the right time.

//

Briefly tell us about your career with the ISG
I started as a lecturer in 2002, was promoted to Reader in 2007 and Professor in 2011. I served the ISG and Mathematics Department in a number of administrative roles, notably Examinations Officer for the ISG and then Director of Research for the Mathematics Department. In that capacity I was responsible for assembling the bid that won Royal Holloway recognition as an Academic Centre for Excellence in Cyber Security Research and compiling the submission for the Research Excellence Framework audit in 2014. I was also part of the team that bid successfully to host one of the first two EPSRC Centres for Doctoral Training in Cyber Security.

//

What did you enjoy best about being an ISG academic?
There were many things I liked: the support of extremely able and helpful colleagues; the freedom to focus on what interested me in terms of research; helping PhD students develop into researchers in their own right; and preparing teaching materials and examinations. (I really didn't like marking and I never completely conquered my nerves about speaking to large groups.) I think I probably enjoyed the research aspect of the job most. But I also got a great sense of satisfaction when I felt a tutorial or lecture had gone really well and the students had got a lot out of it.

//

What were your main research interests during your time at Royal Holloway?
I was mainly interested in several aspects of access control, including the development of improved models for role-based access control; languages for attribute-based access control, with a particular focus on expressiveness and completeness; efficient key derivation techniques for cryptographic access control; languages for expressing constraints in business systems, especially workflow management systems; and, most recently, the computational complexity of workflow satisfiability in the presence of constraints.

//

You are also an expert at setting and solving crossword puzzles. Did any of the same skills serve you well as an academic researcher?
I think a more interesting question is how being an academic served me well as a crossword setter! I left academia to focus on my new interest of setting cryptic crossword puzzles. My time at Royal Holloway turned out to be useful in a number of ways in my new career. Setting a crossword is a little like setting an exam - there's no point in making it too easy or too hard, and having a few relatively easy clues to provide a few crossing letters and thus enable the solver to make some headway with the more difficult clues is as important as providing structured exam questions that enable the candidate to make progress and apply their understanding.
The experience of academic publishing and reviewing was also very valuable, as it helped me in my dealings with crossword editors.

//

You've always been an independent thinker unafraid to challenge the status quo. Do you think it is harder in modern universities to do this?
I'm not sure that it's any harder in modern universities (I still felt able to challenge the status quo), but I do think modern universities are subject to far more constraints (whether externally or self-imposed) that makes them far less receptive to ideas that challenge the status quo, unfortunately.

//

What would you like to regard as your academic legacy?
My PhD students.

//

What's your plans going forward?
I'm now compiling crosswords on a regular basis for The Independent, The Financial Times and The Daily Telegraph. I'd like to join the team at The Guardian or The Times (or both!). I'm also part of the editorial team at The Magpie - a specialist, monthly crossword magazine - something I enjoy very much. I would really like to become the crossword editor for one of the broadsheets, although there aren't many jobs going. I'm also planning to spend more time in the garden and down at my allotment, learn to sing, and walk my new dog.

//

What can dogs teach us about life?
We should play more and work less.

//

Go on - give us a crossword clue for "Royal Holloway"...
Content-free article broadcast by King's College (5,8) [King's = ROYAL, Content-free = HOLLOW, article broadcast = homophone of A = AY]

ISG MSC UPDATE
Jorge Blasco Alis

> Senior Lecturer ISG
Programme Director MSc

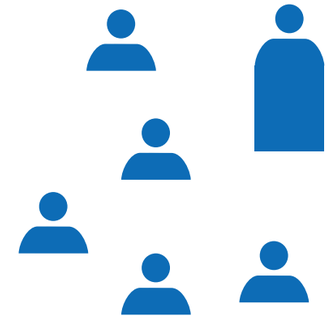
Launched in 1992, our MSc in Information Security has always aimed at offering a degree that meets the needs of the real world and prepares our students to succeed in their future careers. A proof of this commitment is the recent renewal of the NCSC accreditation for both our campus and distance learning degrees. The NCSC certification recognises Master's degrees "that provide well-defined and appropriate content and that are delivered to an appropriate standard". The certification involves assessing the academic team, MSc content, assessments and dissertations. As a novelty, this year's renewals used the Cyber Security Body of Knowledge (CyBOK, http://www.cybok.org) as a basis for assessing the content of our MSc. Out of the 120 credits of taught modules in our MSc, roughly 115 credits can be directly mapped to knowledge areas described within CyBOK. This means that our students are exposed to a broad spectrum of modules and content without sacrificing depth.

In March 2020, like most places, we had to adapt to new ways of teaching, engaging and interacting with our students – all within a single day. All teaching moved online and we had our first ever online assessments. This meant modifying all exams to suit the new online environment and required a huge effort from all academics, administrators and external examiners. But thanks to everyone's efforts we were able to run all the exams on their planned dates. Our students also had to overcome several challenges, including high levels of uncertainty, new modes of learning, home schooling and isolation. Despite these challenges, the results of our assessments were in line with our previous years, demonstrating the resilience of both students and staff in these unprecedented times.

For this academic year (2020/21), we knew that we had to adapt our teaching to be more flexible. This meant adapting all teaching materials for online teaching, creating new videos, lectures and interactive materials as well as being able to run sessions simultaneously face to face and online. While the course started with some face to face delivery, the development of the pandemic meant that we quickly had to move all teaching online again. The preparations we made during the summer allowed us to more or less seamlessly transition to online teaching again. While we miss the face to face interactions with our students, we are very proud of the new methods and materials we have developed. As a summary, our students can now access more than 100 hours of newly developed video content, in addition to their regular teaching – and are a single click away from us whenever they need us.

Again, I am incredibly proud of all my colleagues and our students; how they have kept the MSc community together in this difficult and challenging year.

As usual, I would like to finish this yearly update on a positive note. Each year, the British Computing Society awards the David Lindsay memorial prize to one of our MSc students. This award is presented to the student who, in the opinion of a selection panel, submits the best dissertation on an information security-related topic. This year, the prize was awarded to Giuseppe Raffa for his dissertation "Testing Antivirus in Linux: An Investigation on the Effectiveness of Solutions Available for Desktop Computers". Congratulations!!



WRITING FOR PUBLICATION: AN OPPORTUNITY FOR GRADUATE AND POSTGRADUATE STUDENTS

Siaw-Lynn Ng

> Senior Lecturer ISG

The ISG has a long tradition in cybersecurity research. It is one of the largest academic cybersecurity research groups in the world, consisting of academics and research assistants as well as a large group of postgraduate research students, working on a wide range of topics in information security. Alongside the research, the ISG also has a proud tradition of information security education. Founded in 1992, the ISG's flagship MSc Information Security masters degree programme has now produced over 3000 graduates from more than 100 countries.

One core part of the MSc programme is the MSc project, which is a major individual piece of work aimed at demonstrating an understanding of a specific area of information security or dealing with a practical aspect of information security. Because our students come from a range of different backgrounds – from new students seeking a foundation for a professional career in information security, through to experts in their subjects seeking to widen and deepen their knowledge of information security in general – our MSc projects cover a wide variety of topics. Every year, a number of outstanding projects are chosen to receive the Computer Weekly awards. These MSc projects are re-written in collaboration with the individual ISG project supervisors as accessible short articles for a general professional readership and published online on the Computer Weekly website (https://www.computerweekly.com/), and are also available on our Website (https://royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/computer-weekly-search-security-awards). Past topics include the security of autonomous vehicles, threat modelling and risk management, and the monitoring of the security of pervasive devices such as mobile phones and USB flash drives.

This year there are three articles, covering very different topics: the Computer Misuse Act, the security of investment platforms, and the effectiveness of anti-virus programs.

In `The Computer Misuse Act and the characteristics of convicted hackers', James Crawford (supervised by Rikke Bjerg Jensen) considers the individuals convicted under the Computer Misuse Act and whether they conform to the stereotype of the gifted and highly skilled hackers.

In the article `Protecting personal investors on UK investment platforms from cyber threats' Gerard Phillips (supervised by Geraint Price) describes a new threat model focusing on the risks to personal investors in the UK, who use UK investment platforms to manage their pensions and savings. This offers new insights allowing anticipation and defence against future attacks.

While anti-virus programs are recognised as an important defensive tools for desktop computers, these tools are not widely available for desktops running the Linux operating system. In `Testing anti-virus in Linux: How effective are the solutions available for desktop computers', Giuseppe Raffa (supervised by Daniele Sgandurra) evaluates the effectiveness of some anti-virus programs for Linux desktops using local installations as well as an online malware scanning service.

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

Another venue of online publication is the Infosecurity magazine (https://www.infosecurity-magazine.com/) Next-Gen Infosec series. These are very short blog-style articles from postgraduates for a readership of IT security practitioners. This allows graduate and postgraduate students to improve their technical and communication skills, to establish them as an expert in their fields of study, and to influence the development of those fields.

The article `Changing cyber security behaviours in the workplace: a critique of the evidence' by Amy Ertan (CDT student) outlines the key findings of a report on cyber security behaviours in organisations and recommends topics for future research. In the collaborative article `Principles of effective cybersecurity wargames', Peadar Callaghan (Game Designer) and Amy Ertan discuss the role of serious games in cybersecurity training and education of users, and in `Biases in perceptions of information security threats', Georgia Crossland (CDT student) discusses cognitive biases in the perception on information security risks in the context of the extensive shift to working from home.

These articles are written in a style that makes them accessible to everyone, and I would recommend them to anyone interested in various aspects of information security.

TEACHING IN A PANDEMIC

Darren Hurley-Smith

> Lecturer ISG

Teaching has been an immense challenge for all of us this last year, more so than usual. The move to fully digital delivery has been abrupt and, at times, experimental. COVID-19 has acted as a catalyst for the move to a fully digital curriculum, one which initially demanded adaptation to a dynamic challenge by teaching and administrative staff alike. In this article, I'd like to focus on the frontline teaching experience as an individual immersed in this challenging environment and focus on the tools, techniques, and open problems arising from this tumultuous period.

Technology is at the heart of this discussion. In the initial lockdown period (March to July 2020), staff were forced by circumstance to adapt to fully digital delivery. Lecture recordings were expected and live text and voice chat were features in high demand. The first challenge faced by any teacher was that of isolation compounded by the need for rapid, knowledgeable creation of online content. Discussions about streaming software became commonplace in staff chats, and back-channel solutions such as Discord and Slack supplemented early and unstable Microsoft Teams implementations. Due to the robust and healthy community within the ISG, this initial challenge was met head on and with a high degree of success through ad-hoc discussions.

We are now well supported by the Admin and IT teams who have worked tirelessly from the start to improve our digital services, such as Microsoft Teams, Moodle and RePlay. Educators must, however, accept and plan for community-driven solutions to problems that an institution (through no fault other than that of organisational inertia) cannot address in a timely manner. Reactive solutions have been effective but stressful: it is imperative that we develop community groups and toolsets to not only weather rapid change, but also ensure that outstanding issues are addressed. Our image rights and the appropriate institutional use of recorded media are topics that have become obfuscated by the pressing demand for online content, and we must not allow this to remain the case.

Fully-digital teaching has also highlighted challenges facing students: technological and wealth inequality most visible among them. Campus learning has the benefit of laboratory and library access. We previously took student internet and specialist resource access for granted as a result. Not so in this new era of sequential lockdowns and fully-digital learning. We as staff can draw on university resources where required, but students may have difficulty communicating their technological needs due to perceived embarrassment or lack of support. It has become important to discuss with students the laboratory and technological requirements of a course, and I believe it is imperative to begin devising solutions that equalise the student experience. Distributing inexpensive microcomputing platforms pre-loaded with course-appropriate and open-source software, or designing courses for consumption through mobile-devices are two potential paths forward.

There is also the issue of extra-curricular technical literacy. For my course, Security Testing – Theory and Practice, I have been far more involved in tech-support activities than in the previous year: simple misunderstandings, typos, and technical issues are amplified by the distance between student and teacher. The process of resolving queries has become more compartmentalised: a solution provided to one student and then published on Moodle, may need to be repeated multiple times regardless of visibility, if the students themselves are unfamiliar with how information is disseminated. Even if students are aware of public channels, they may feel embarrassed and prefer to pursue private channels instead. Ironically, the accessibility of digital teaching platforms and perceived increase in staff availability has amplified this desire for privacy. Referring students to public spaces (e.g., Moodle forums) which don't allow for anonymous queries is not a solution: there is a clearly demonstrated preference for privacy and we must embrace this increased level of engagement whilst identifying effective methods to manage the additional workload it represents.

In contrast to the increased participation of students in private chats, is the loss of a vital tool in identifying those suffering in silence. It is no longer possible for us to reasonably ascertain whether a student is silent but participating, or completely detached from the learning experience. Digital teaching denies us the ability to scan the room and see whether an individual is physically present. I have attempted to mitigate this through periodic evaluation of students through assessments, to identify those who may be having trouble with the course material. If we are to allow students to attend digitally in the future, a process of periodic review may be required to avoid nasty surprises when marking end of year exams. As we return to campus , we will need to revisit the open problem of truly hybrid teaching. Indeed, this form of 'blended learning' is nothing new. Initially defined in the 1960's, then revised in the 1990's to the definition we now use, blended learning is a hybrid pedagogical mode in which face-to-face and technology-enhanced teaching are used side-by-side. At Royal Holloway, blended learning has come to be used as a blanket term to describe any mode of teaching that includes a technological element: from recorded lectures to fully digital courses. I would argue that we currently reside at the fully-digital end of this spectrum, making blended learning somewhat of a misnomer.

There have been clear benefits to digital delivery: student engagement with recorded content may be a subject in need of rigorous study before we can quantify it, but the increased individual support available to students has proven popular. Initial attempts at split face-to-face and online delivery of live lectures in September 2020 were met with disapproval by students: a fact we must bear in mind when considering any future blended learning strategy. The perceived halving of contact time in split-sessions was a common theme in both individual discussions and broader complaints. Merged sessions placed more pressure on the teacher to split focus and ensure queries from the room and via text were addressed, but proved more popular with students. We must review our teaching methodologies, and receive appropriate equipment, support, and staffing, to deliver consistent online and offline teaching experiences.

This has been a year of heroic efforts from teaching staff, admin and IT. But heroism is often used at the abstract level to wallpaper over inconvenient problems, and we must temper our well-deserved pride in having navigated the most challenging teaching experience of our time by acknowledging that serious and pressing problems remain. Technical and wealth inequality continue to be issues. The engagement, retention and performance of students by demographic is as yet unknown and may unveil systemic inequalities that must be factored into our revised hybrid teaching strategy. The isolation of staff, woeful mental health support for employees, dependency on individual solutions, and exceptional commitment of time and effort must all be addressed if we are to stop courting disaster in the likely event of continued cycles of national lockdowns. Finally, a shift to online and recorded content as an expectation of teaching staff must be accompanied with appropriate protections for our image rights and use of content developed for our courses. Until the context of, and right to withdraw, recorded content is protected there will be justified resistance to providing a fully digital experience for students.

CDT UPDATE
Keith Martin

> Professor ISG and Director of the CDT

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

There are pros and cons of being a PhD student on a scholarship during a national lockdown. The pros are temporary job security (no furloughing!), and a job that is relatively self-contained and can be done remotely. The cons are almost the same of course! The job is temporary, so those coming to an end had to job-seek remotely. The autonomous aspects of a PhD can also make it a lonely and isolating experience. Indeed the whole idea behind the CDT model is to inject a supporting infrastructure and social cohesion into the process, everything that lockdown withdrew. For some students with more practical fieldwork to conduct, lockdown was highly disruptive and plans have been forced to change.

In the end, the ability to cope over the last year has probably, as for most of the population, come down more to personality, circumstances and resilience. Many CDT students have been able to progress relatively well, while others have been struggling. I don't suppose the CDT is different to any other community in that regard. We were rather fortunate in 2020 that lockdown only curtailed a few of the September 2019 cohort's first-year training activities, although sadly some of the most fun ones. We were unable to conduct any of our visits to cyber security workplaces, and the practical network security labs were postponed. On the plus side, students commenced summer projects earlier and were presented with a new challenge – to support dissemination of their projects with pre-recorded videos. They rose to this challenge well.

The eight students who started in September 2020 have had a much more surreal start. They were able to meet one another physically at the very start of term, but soon all training was online and they became increasingly used to knowing one another as animated digital rectangles on a screen. Fortunately they are all complete stars and, perhaps because of the adversity of the situation, they have pulled together as an outstanding cohort, delivering a fascinating group project on contact tracing apps and storming through all their virtual training events. They, too, have missed out on the various outings that we normally run but, through virtual support from our external partners, we have been able to run a full training programme.

I think students in the middle of their PhDs have had the hardest time. This can involve dark hours of ebbing confidence, when having others around to cajole onwards is so important. I am very impressed with all PhD projects that have nudged forward during the last twelve months, especially those where students had less-than-ideal working conditions and were suffering from personal anxiety. Every student deserves a pat on the back for pushing onwards. Both the EPSRC and Royal Holloway have also been very supportive and most students who felt the need have had scholarships and deadlines extended as partial mitigation for time lost. This has come as welcome relief for those concerned.

It's hard to provide a sense of community during lockdown but I know that our students use a variety of techniques to stay connected. A big shout out here is due to Tabby and Jenna, who ran a regular virtual quiz that was greatly enjoyed by many. A very tough virtual quiz, I have to say. I personally came to dread the music rounds! And – yes – despite it all, PhD theses kept dropping out the end of the production line during the last twelve months. It seems a shame to hold a virtual PhD viva but, in the end, I think everyone agrees that they work perfectly well. The one big deficiency is the inability to go to the pub at the end (although a special thanks to Nick Robinson for making the pub come to us after his – nice one Nick…)

There have been many other successes, with CDT students continuing to publish top-quality research, write articles, record podcasts and conduct virtual internships. Please visit our blog and see the social media feeds for more details about some of those highlights. However, I do have to single out the CDT team who won the UK Cyber 9/12 Strategy Challenge earlier in the year. This is the CDT's second triumph in this competition, on each occasion with an all-female team. I shouldn't have to single the latter fact out, but cyber security remains a primarily male-dominated discipline and it is so important to promote female role models. Well done Team Minerva!

Let's hope for a slightly less virtual future and that there will soon be opportunities to get the CDT community back together in anything other than a Teams or Zoom meeting. We have closed recruitment to the CDT earlier than in any previous year, such has been the demand from high quality applicants, so the CDT's future looks bright despite the chaos that surrounds us.

ON WINNING CYBER 9/12
Stephanie Itimi, Sofia Liemann Escobar, Kyra Mozley, Emma Smith

> First-year CDT students

This year, four first-year ISG PhD students from the Centre for Doctoral Training (CDT) in Cyber Security for the Everyday participated in the Cyber 9/12 UK Strategy Challenge. After a lot of hard work the team (Minerva Task Force) took first place for the competition and also won the most creative policy response award.

What does Cyber 9/12 UK involve?

The challenge, organised by the Atlantic Council, is an annual competition open to current university students to put their strategy skills to the test. Students are required to work through a scenario and decide how best to respond to prevent a cyber attack. In this year's scenario, students were required to adopt the roles of experienced policy advisers. As part of a hypothetical cybersecurity task force, they had to prepare a document outlining the scenario, present three policy options, including the advantages and disadvantages of each option, and a recommendation which they believed the government should follow. In addition to the document, students had to prepare a ten-minute oral briefing to the PM's office (played by the competition judges), outlining their options and recommendation as well as answering any questions they may have. As the competition progressed, the teams had less time to prepare for each round - the first round was around a month, the semi-finals were 12 hours, and the final, just 20 minutes! The competition requires a broad range of knowledge and skills, ranging from technology to international relations, which makes it a perfect fit for CDT students who have been exposed to more than just the technical elements of cybersecurity.

Meet the team

We are all first-year CDT students from completely different backgrounds - Maths, War Studies and International Security, Economics, and Computer Science - and the interdisciplinary knowledge, experience and skillset of the group definitely played a role in our success. We decided on the team name Minerva Task Force after the Roman goddess of wisdom and strategic warfare, given that we were an all-female team and that we assumed the diversity of knowledge and experience held within the team would also make us wise for the strategic challenge upon which we were about to embark.

We couldn't have done it without the support of our coach Nick Robinson (a former CDT student who competed in the competition a few years ago). He provided us with great advice and help throughout the challenge, including trying to reduce pre-presentation nerves by keeping us distracted with some great conversations.

CDT tackles Cyber 9/12

We received our first intelligence pack in mid-January; a 47-page document complete with many different pieces of evidence, all of which we had to digest, whilst considering and evaluating the credibility of the sources. We were certainly overwhelmed by all of this information, but through analysing a series of tweets, several reports from various UK and international government agencies and email threads, we managed to agree on what we believed the scenario was.

In theme with the pandemic, this year's scenario was centred around threats relating to oxygen delivery systems for ICU respirators, the vaccine supply chain, and disinformation on social media. Due to the diversity of threats, we decided to divide them among us within the team in order for us to conduct further research into the impacts of the threats, and how best to combat the risk. We believed the level of evidence provided was not sufficient to assess which of these threats was the most pressing nor if we should attribute the cause, so we decided to recommend the policy which focused on preparing the country to ensure the pandemic recovery would not be affected by the situation. This policy involved both long- and short-term recommendations, as well as measures across all levels of government (local, national and global). As the competition drew closer, we submitted our policy documents and began rehearsing our briefing presentation. After hours on MS Teams practising and timing ourselves, we ran like clockwork by the time of the competition. The hard work paid off! The judges praised us for our teamwork and professionalism, with one judge even tweeting his praise saying that he thought he was back at number 10!

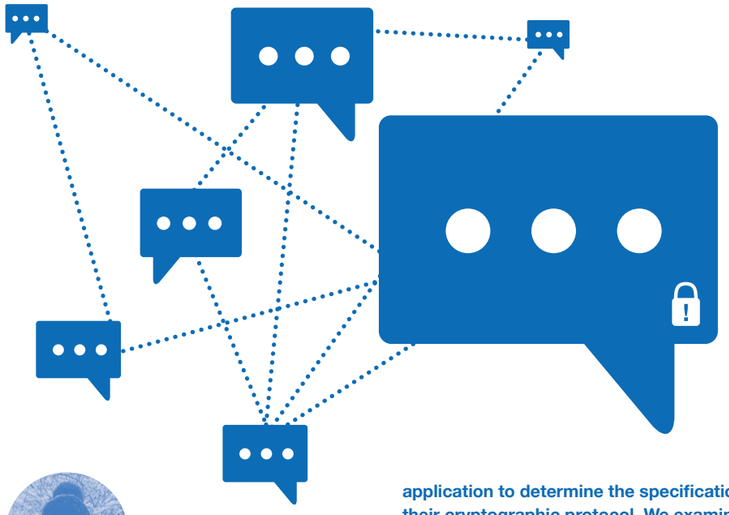
We were ecstatic at the end of the first day to not only learn that we had won the prize for the most innovative policy answer, but that we had also advanced to the semi-finals. As we waited for the next intelligence pack, we took a well-deserved break and made pancakes (it was Shrove Tuesday), before settling in for a long night of work - particularly for Kyra, who decided not to sleep! The scenario pack arrived around 7 PM and built on and escalated the previous one, as now serious cyber incidents had occurred. In the scenario, the ICU Oxygen systems in Manchester NHS Trusts had been hacked and were no longer functioning. The disinformation had also escalated and now we had further evidence suggesting a foreign state actor was supporting some of the campaigns. By 8 AM the following morning we had to submit our next document with our policy options, and then start working on our presentation to be ready to brief the judges a couple of hours later. Despite the group averaging around three hours of sleep, the second round of presentations went well and we yet again received great feedback - one of the judges even described us as a powerhouse.

After all the efforts we were delighted to learn that we had made it through to the final three. The next round was all a blur. We had to digest the final intelligence pack, prepare our policy response as well as what we would say in our ten-minute brief - all in 20 minutes! Before we knew it, we were presenting again; this time not just to the judges, but to all competitors, which definitely made us more nervous. Due to our lack of preparation time compared to the previous rounds we were rather critical of our performance. Once we had finished we reflected on it and reached the conclusion that this had been a great experience since it took us out of our comfort zones into a high-pressure environment that required us to think quickly. We eagerly awaited the results, and to our disbelief we came first place.

We are now looking forward to attending the Black Hat Conference in November and receiving our collection of cybersecurity books (our prizes for first place), as well as our new noise-cancelling headphones for the most creative policy response prize. Now that we have conquered the UK competition, we may even attempt the Geneva one next year, CDT road trip, anyone?

Overall, we had a great time participating. We developed our skills in policy writing and briefing, gained knowledge in areas outside of our comfort zones, and of course, got to know each other better too. If you want to participate next year, we definitely encourage you to, and maybe Royal Holloway can bring back the trophy for the third time.

More information can be found at https://www.cyber912uk.org/en/.



BREAKING BRIDGEFY

Lenka Mareková

> ISG CDT PhD Student

Mesh messaging applications allow users in relative proximity to communicate without the Internet by way of wireless technologies such as Bluetooth Low Energy. Among such applications, there currently exists only one viable offering. Bridgefy has risen to public awareness with reports of internet shutdowns among protests across the world, starting in Hong Kong with the anti-extradition law bill amendment protests (though an internet shutdown did not take place there) and later spreading to protests in India, Iran, US, Zimbabwe, Belarus, and other countries.

However, the application was not initially intended for such a use case. Bridgefy began as an application for “music festivals, sports stadiums, rural communities, natural disasters, traveling abroad”, and though its developers claimed it was secured by end-to-end encryption, none of its original use cases could be compared with the adversarial environment that result from situations of unrest, where attempts to subvert the application’s security are not merely possible, but to be expected, and where such attacks can have harsh consequences for its users. Despite this, the developers also began promoting it for the protest use case.

Researchers from the ISG performed a security analysis of the application as well as its underlying software development kit, which other developers can use to build their own mesh messaging applications. First, we reverse-engineered the Android application to determine the specification of their cryptographic protocol. We examined this protocol and found several vulnerabilities, affecting both common security goals such as privacy and authenticity as well as properties especially relevant in a protest such as reliability.

In Bridgefy as analysed, messages sent on the Bluetooth mesh network were first compressed with Gzip and then encrypted block-by-block using RSA with the deprecated PKCS#1 v1.5 padding standard. Without internet, all devices that came into Bluetooth range of each other automatically performed a handshake during which they exchanged their public keys. This handshake was not cryptographically authenticated and instead relied on user IDs and Bluetooth addresses to establish identity. As a result, two attacks were possible: an attacker could impersonate any user, as well as perform a full attacker-in-the-middle between any two users in range, without the users noticing that their messages are no longer private and may have been modified by the attacker. The use of PKCS#1 v1.5 was also problematic – thanks to composition with Gzip compression, we were able to instantiate a new variant of Bleichenbacher's attack that could decrypt a message using 130,000 chosen ciphertexts on average, a more resource-intensive attack that would however be within reach of an adversary with the ability to confiscate the target user's phone and hold it overnight (without unlocking the phone). Further, an attacker with a physical presence could easily track Bridgefy users and reveal their social graphs just by passively observing the network. Finally, it was possible to effectively shut down the entire network with a single specifically crafted message, a blow to the claims of resilience when faced with Internet shutdowns.

We verified the attacks in practice on Android devices using an attacker's device running a Bridgefy application modified with Frida, a dynamic instrumentation toolkit that allows injecting scripts into a running application. We disclosed the vulnerabilities to the Bridgefy developers at the end of April 2020, agreeing on a public disclosure date in August, as would be standard. However, the Bridgefy team began informing their users that they should not expect confidentiality guarantees from the current version of the application much earlier, though it did not stop them from continuing to promote the application for use in protests. At the end of October, the Bridgefy application was updated to use the Signal protocol. If implemented correctly, it would rule out many of the attacks we found, but we have not reviewed these changes and we have recommended an independent security audit to the Bridgefy team.

Since this research was concluded, it became clear that media reports may have exaggerated the real use of Bridgefy on the streets, especially in Hong Kong. However, there is some evidence to suggest that the media "stories" had taken on a life of their own, serving as inspiration for protesters who have decided to adopt the "Hong Kong protesters' playbook". The application recently continued to be promoted in Myanmar, where the military regime imposed internet shutdowns in an attempt to prevent dissent. While Bridgefy was not envisioned as a "protest app", its users have effectively made it into one, and so our work emphasises the need for analysing applications under the conditions they are used in, and the kind of adversaries they are likely to face. We would also like to draw attention to the problem space of secure mesh messaging to begin with, as it is clear that users only turned to Bridgefy because there were no alternatives. Thus, it is a pressing topic for future work to design communication protocols and tools that cater to these needs. We note, though, that this requires understanding "these needs" to avoid a disconnect between what designers design for and what users in these settings require.

DEFINITIONS, THEOREMS AND PROOFS IN CRYPTOGRAPHY

Martin R. Albrecht

> Professor ISG

Cryptography is foundational to securing information systems. It is thus no surprise that for every new use-case, application and scenario, cryptographic protocols are proposed to provide security guarantees. Practitioners then need to make a judgment on what to make of these protocols. For example, is that authenticated key exchange for IoT devices claiming post-compromise security and anonymity any good?

Fundamentally, such questions require a detailed knowledge and understanding of the theoretical security models that are widely used to reason about security properties. But there are a few things to look out for that help to get a first impression.

First, it is worth noting that the fact alone that a paper was published and thus went through peer review is, in itself, not enough to go on. Peer review is often a much less rigorous process than people outside academia make it out to be. It is also not enough to look for “IEEE” or “ACM” in the conference or journal title as both organisations give their names to outlets with varying quality. That is, you can find cryptographic protocols that are easily broken by a trained cryptographer also in IEEE and ACM venues. On the other hand, anything that makes it into their respective flagship security conferences – IEEE Security & Privacy and ACM CCS – will have passed at least some routine inspection by experts. Similarly, conferences and journals either sponsored by the International Association for Cryptologic Research (IACR) or held in cooperation with the IACR will have programme committees comprised of cryptographers which will have done some sanity checking.

There are also things to look out for in the paper. A surprisingly easy check for cryptographic protocols[1] is to look for formal claims of security – definitions and theorems – and formal proofs. This is in contrast to informal statements a la “this protocol gives confidentiality” and informal discussions of security a la “because we encrypt the data it is confidential”. This sort of formal treatment is by now a standard requirement for publishing cryptographic protocols and for good reason.

To illustrate this, consider structural engineering.[2] An engineer designing a bridge will be required to declare what and how much stress the bridge is meant to be able to withstand, say, a two-ton lorry and wind speeds of up to 200 km/h. The engineer would also be required to show this in a way that enables other structural engineers to verify the claim. Our engineer would not get away with claiming “this bridge is stable” or “this bridge can take a two-ton lorry” without such an argument. Over the history of structural engineering a disciplinary norm developed on what to require and in what form.

It is no different in cryptography. A cryptographer does not get away with claiming (a) “this protocol is secure” or (b) “this protocol achieves confidentiality against active attackers” without providing a proof that this is in fact the case. The former claim is too vague and cannot be checked: what does “secure” mean here? What precisely is secured against an attacker with what capabilities? The second claim requires to be backed up by a proof, a formal argument that can be checked by experts. A surprisingly high number of cryptographic protocols published in non-cryptographic venues fail to live up to this disciplinary norm of cryptography. Often such protocols are then broken when a trained cryptographer looks at them.

Then there are papers which have the form of theorem & proof but that do not actually deliver on this in content. A classical mistake is to formulate a theorem ruling out a specific attack a la “the attacker cannot guess the key because they only see …”. It is, of course, useful to know that a specific attack the designers thought of cannot be mounted but – returning to our structural engineering analogy – we want greater assurance than that a specific lorry will not bring down the bridge. We want to rule out the possibility that any lorry that makes it onto the bridge can bring it down.

A cryptographic theorem is more general, e.g. “No adversary running in less than 2128 steps and with complete control over the network can distinguish the key from a uniformly random string with probability greater than 1/264”. They do not rule out specific attack strategies but all attackers endowed with some capabilities (e.g. control over the network). Proofs of such theorems then typically proceed by assuming the counter factual: “Assume such an adversary existed, then this means we can use this adversary to break this specific security property of one of the building blocks we used in our protocol. Since we assume this cannot be done, such an adversary does not exist”. That is, such proofs “reduce” the security of the protocol to that of its building blocks. For this, we, of course, need formal statements about these building blocks to reduce to.[3] Finally, such arguments must then be vetted carefully on whether this proof is indeed correct. This is no different to any other area of science: people can make mistakes when writing a proof and we rely on (post-publication) peer review to find (and correct) such bugs.[4]

That is, checking for the markers of questionable cryptographic designs outlined above on its own will not give the assurance that the protocol is secure, but it should at least rule out that the protocol is trivially insecure. It is often said “cryptography is hard” when some protocol is broken. While this is true, the same holds for any science. Structural engineering, too, is hard. Just like structural engineering, cryptography has disciplinary norms and standards that allow us to proceed with the outputs of the science in confidence: definitions, theorems and proofs.

[1] Cryptographic primitives – block ciphers, hash functions, signature schemes, public-key encryption – need to be studied differently.

[2] Apologies to any structural engineers reading this, I’m sure I’m butchering the analogy in many upsetting ways.

[3] A nice discussion of formal statements of security is in Rogaway, P. (2004). On the role definitions in and beyond cryptography. In Annual Asian Computing Science Conference (pp. 13–32).

[4] It is not that uncommon that bugs in security proofs are only discovered after a few years when a PhD student checks them carefully because they want to extend the work.

ISO/IEC 27002 – PAST, PRESENT AND FUTURE

Paul Dorey & Chris Mitchell

> Visiting Professor ISG
> Professor ISG

Introduction

Most people working in information security are familiar with ISO/IEC 27002, the *Code of practice for information security controls*. This document is essentially a catalogue and guide to use of security controls, i.e. measures that can be used to help protect the security of information. The 114 controls it describes over 80 pages are divided into 14 categories, ranging from security policies to compliance. It is certainly not bedtime reading, except perhaps as a cure for insomnia, but it contains a wealth of good advice and functions more as a reference than something to be read from cover to cover.

It is very widely used and referenced in the industry, and must be consulted as part of gaining ISO/IEC 27001 certification. However, everything is about to change – as we describe below, a new completely revised edition will be published within the next 12-18 months.

BS 7799 – the origin

The first edition of BS 7799, the original ancestor of ISO/IEC 27001/2, was published back in 1995. The standard was created because the security of computer systems and information was becoming a significant business risk but there was no consistent way of specifying what suppliers and business partners needed to do to manage it. The standard came from very practical roots in actual security practice at the time, when a group of companies (led by the Shell oil company) got together to share their own internal standards and even ran some desktop attack scenario exercises to highlight undocumented controls. The resulting document was sponsored by the UK Department of Trade and Industry and launched as 'A Code of Practice for Information Security' at a press conference on 30th September 1993. Subsequent adoption of the code of practice as BS 7799:1995 came with a few changes to the content and with the advantages brought by official standards recognition, albeit predominantly within the UK. The second part BS 7799-2:1999, describing Information Security Management Systems (ISMSs), was added four years later.

Adoption by ISO/IEC

Although it was a British standard, in the absence of major competitors BS 7799 soon became very widely used worldwide. The first revision of the standard, BS 7799-1:1999, was published in April 1999 and, reflecting its widespread adoption, was proposed for adoption as an ISO standard via the "Fast Track" mechanism in October 1999, resulting in its publication, with minor amendments, as ISO/IEC 17799:2000 on 1st December 2000. Whilst ISO/IEC 27002 is very widely used and recognised internationally, it is not the only such guide to security controls. Of particular importance are the parallel documents produced by NIST in the US. The NIST Cyber Security Framework of 2014 contrasted significantly with the ISO/IEC 27002 revision from the year before, and took pains to highlight the importance of risk identification, and the security capabilities for detection and response in addition to protection which was the primary focus of ISO 27002:2013. The fact that ISO/IEC 27002 was increasingly being seen as outdated relative to current practices has helped to increase adoption of the NIST framework.

Integration into the ISO/IEC 27000 series

Building on the success of the BS 7799 series, a revised version of the ISMS standard, BS 7799-2:2002, was officially launched on 5th September 2002. This was eventually also fast-tracked as an international standard, resulting in the publication in 2005 of the first edition of ISO/IEC 27001, which was very closely based on BS 7799-2:2002. A history of ISO/IEC 27001 can be found on the Gamma website (http://www.gammassl.co.uk/27001/history.php), some of the content of which has been used in writing this article.

One significant addition to ISO/IEC 27001 compared to its predecessor was the introduction of the Statement of Applicability (SoA). Organisations wishing to be able to claim that their ISMS conforms to ISO/IEC 27001 are required to produce an SoA, which, for every control in ISO/IEC 27002, must indicate whether or not it has been implemented and in either case why. That is, whilst ISO/IEC 27001 conformance does not require implementation of any of the controls in ISO/IEC 27002 (it is, and always has been, a code of practice) it nonetheless plays a key role in compliance.

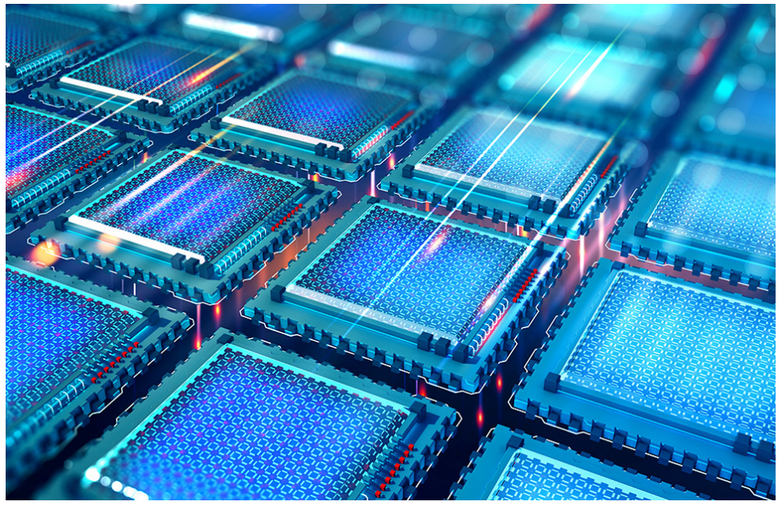
In the mid-2000s it was decided to re-organize the security management standards published by ISO/IEC SC 27 into a single 27000 series. This resulted in the re-badging of ISO/IEC 17799 as ISO/IEC 27002:2005. The first, introductory, member of the series, ISO/IEC 27000, was published in 2009, and introduces a range of basic terminology and many fundamental information security management notions, notably including the ideas of, and rationale for, an ISMS. Subsequently, many further standards have been added to the 27000 series, giving more detailed guidance on the implementation and use of ISO/IEC 27001.

A complete revision

During over 25 years of use, the coverage of controls in ISO/IEC 27002 has been updated at intervals (including in ISO/IEC 27002:2013, the second edition), but it became clear several years ago that a major revision was needed to remove obsolete material and include new areas of security technology and methods. One of the challenges has been the tendency to document the latest and emerging security practices as new (and often largely ignored) subsidiary standards within the 27000 series rather than incorporating them into the base 27002 standard. The 2013 revision seemed to suffer through the international standards agreement process and started to lag behind current practice, quite a contrast to how the original code of practice, written almost 20 years before, very much reflected best practice at the time.

One obvious change in the new edition is a complete re-organization of the security controls into four broad categories (organisational, people, physical, and technological controls) rather than the 14 categories in ISO/IEC 27002:2013. This avoids some of the awkward shoehorning of controls into categories in the current standard, as well as enabling some of the obvious duplication to be removed. Even more importantly, new controls have been added and redundant ones removed.

Such a radical change will no doubt require many in the security industry to revise their approach to the development and review of ISMSs; certainly, the structure of the SoA will inevitably change. This is almost certainly a positive development, as a shake-up of the ISMS/27001 consultancy world is probably overdue. Of course, in some ways the change is not so earth-shattering, as the new version of ISO/IEC 27002 provides a helpful annex giving a mapping between the new and old control sets. It remains to be seen how the change will be viewed by the industry – a welcome change or an unwelcome irritation – perhaps both!



POST-QUANTUM: WHAT'S NEXT?

Martin R. Albrecht

> Professor ISG

The NIST Post Quantum Standardisation Process is coming to a close. With the announcement of a set of seven finalists – Classic McEliece (code-based KEM), CRYSTALS-KYBER (lattice-based KEM), NTRU (lattice-based KEM), SABER (lattice-based KEM), CRYSTALS-DILITHIUM (lattice-based signature scheme), FALCON (lattice-based signature scheme), and Rainbow (MQ-based signature scheme) – NIST has narrowed down its list of options to almost a handful. What is more, as of writing, the future of Rainbow is a bit unclear.[1] NIST plans to make a draft standard available between 2022 and 2024.

The sense of "we are getting close to the deployment of this stuff" that is implied by the NIST process coming to a close is mirrored in the "UK Cyber Security Sectoral Analysis 2020", commissioned by the Department for Digital, Culture, Media and Sport. This document lists post-quantum cryptography as an emerging sub-sector: businesses are gearing up to commercialise post-quantum cryptography. Mission accomplished for academia?

Now, there are, of course, still a large number of issues that need to be resolved in order to facilitate a smooth transition to post-quantum cryptography. Furthermore, the security analysis of these schemes – of their underlying hard problems and of potential issues with implementations – will remain an area of focus for cryptographic research; after all, the pre-quantum hardness of RSA remains an active area of research and we have no indication that things will be dramatically different in a post-quantum world for, say, lattice-based cryptography.

That said, a question does present itself: "What's next?" Here, lattice-based cryptography is in a curious position. On the one hand, five out of seven of the NIST finalists are lattice-based, i.e. lattices provide a good performance/security trade-off among the families of post-quantum schemes for the most low-level asymmetric primitives such as key encapsulation (KEMs) and digital signatures.[2] On the other hand, lattices have underpinned many innovations at the "top end" of cryptography over the last decade or so: computing with encrypted data (FHE), computing with encrypted programs (obfuscation), cryptographic access control (attribute-based encryption), associating cryptographic keys to functions on the plaintext (functional encryption) and so on.

However, between these two "extremes" of the public-key spectrum of cryptography lies a wealth of constructions where the viability of lattice-based schemes – or, indeed, *any* post-quantum scheme[3] – is not well established. For example, it is not known how to instantiate an efficient non-interactive key exchange from post-quantum assumptions. We do not know how to make anonymous credentials as used in e.g. Cloudflare's PrivacyPass, post-quantum safe while remaining comparatively efficient. Nor do we know how to make lattice-based encryption schemes updatable such that they can be used to offer desirable security properties (e.g. post-compromise security) to group chat protocols. One such group chat protocol based on classical cryptography, MLS, is currently in the process of being standardised by the IETF and is designed to achieve a host of security properties for large group chats that are standard for one-on-one chats.

Running with the assumption that large-scale quantum computers are viable means to expect that post-quantum cryptography will cease to be a sub-discipline of cryptography: all cryptography would need to be post-quantum in a world where large-scale quantum computers exist. For this to happen, there is still plenty to do. Encryption and signatures are just the first step.

[1] https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/official-comments/RAINBOW-round3-official-comment.pdf

[2] Technically, digital signatures are not an "asymmetric primitive", they exist in "Minicrypt". But in practice we tend to build them from assumptions that also enable public-key encryption.

[3] The big exception being CSIDH with a known class group which enables to do pretty much all that can be done from Diffie-Hellman. However, computing such a class group is a super-polynomially hard problem, limiting how big we can select parameters.

Ethnographic fieldwork in Nuuk, Greenland (picture: author's own)

WHY ETHNOGRAPHY MATTERS TO INFORMATION SECURITY

Rikke Bjerg Jensen
Nicola Wendt

> Senior Lecturer ISG
> Research Associate at DLR & former PhD student ISG

An emerging body of information security scholarship has explored the security needs and practices of distinct groups of people, often focusing on those who are either marginalised or at higher security risk, e.g. activists, refugees, undocumented migrants. What these works highlight, among other things, is that information security relies as much on people's experiences of security in their interactions with technology as on the security of the technology itself. Underpinning this work, while not expressed explicitly, is an understanding of information security rooted in collective behaviours and practices, where the security of the individual is grounded in trust relations and shared security goals within groups.

The understanding of information security as a collective endeavour is the starting point for our work on security needs and practices with people living and working on what we might call 'the edge' of societies. More specifically, our work engages the often hidden or unvoiced social groups not generally considered in the design of security technologies. While existing studies have employed qualitative research approaches, such as interviews and focus groups in particular, to understand such security needs and practices, we take a different approach. Our work starts from the premise that in order to truly understand information security as something that is practised by social groups as much as by individuals, we need a methodological approach that is grounded, over time, in the settings and groups it aims to understand: namely, ethnography. Indeed, ethnography has already established itself as a methodological practice within various branches of research into technology use, focusing in particular on informing human-centred technology design and often within a workplace setting [1].

The distinction between ethnography and qualitative research more generally is articulated by, among others, 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" [2, p.3].

For security, this distinction is particularly important as interview and focus group based studies rely on participants self-selecting to take part. This often leads to a skewed sample, where study participants have pre-established ideas of security or consider themselves security conscious. Indeed, qualitative studies with, for example, higher-risk groups often end up engaging security trainers for these groups or "community leaders", instead of those who have to rely on security technologies for individual or collective security [3]. Therefore, ethnography, rooted in extended field studies and driven by immersion and observation with and within the social groups it aims to understand, is uniquely placed to uncover actual security practices and needs as they transpire in people's everyday lives. Put differently, it allows us to learn that which people do not know themselves. With Atkinson we can say that interviews and focus groups "are 'qualitative' but they are certainly not ethnographic" [2], while for security they fall short when trying to establish actual and lived security needs and practices.

Ethnography enables long-term explorations of, for example, what security looks and feels like for the groups under study and how this might change over time. How security is experienced and voiced as well as how it is negotiated and shared between group members. How security technologies are used within groups and for what purposes. What security expectations and goals are held within groups and how they manifest themselves. Ethnography further allows to explore and understand the contextual structures that govern and influence collective security practices, facilitating a more comprehensive analysis of social groups' security behaviours, concerns and needs; thus, opening up the potential to ground technological innovation and security notions in the actual (observed) experiences of people, rather than in how people articulate security concerns and needs through, say, interviews when prompted.

It is, however, important to distinguish between different ethnographic approaches. In line with Crabtree et al. [4, p.885], ethnography is "an empirical matter of uncovering through fieldwork the methods that *members employ* to account for, accomplish and organize action and interaction in the settings they inhabit" (emphasis in original). Ethnographic work is thus capable of unearthing 'social facts' about the groups we study and go beyond rhetoric, cultural interpretation or critical discourse found elsewhere [4,5].

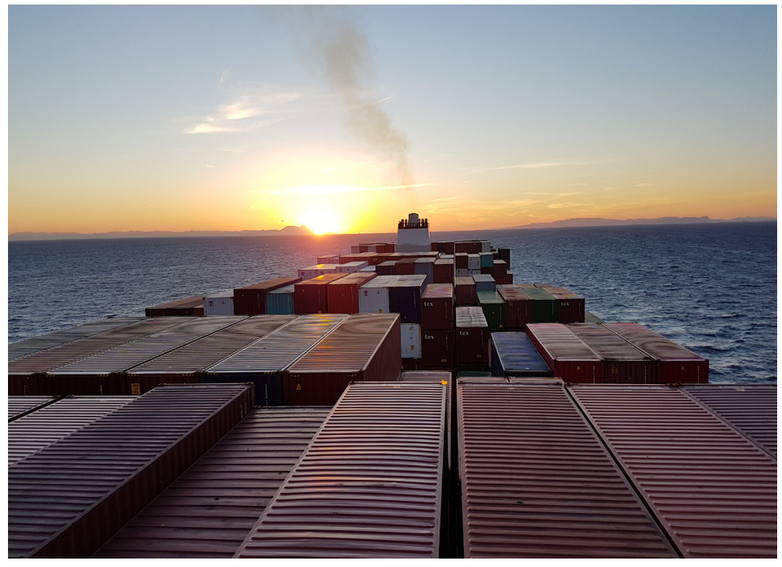
To exemplify this, we briefly draw out a few insights from two separate field studies: (1) seafarers onboard two container ships and (2) Greenlanders living in Nuuk, Greenland and Copenhagen, Denmark. Both studies were grounded in ethnographic research and comprised extended fieldwork with the groups under study. While Nicola spent one month in Nuuk and two weeks in Copenhagen, Rikke spent five weeks onboard two container ships in European waters [6]. Each study aimed to understand how (information) security is practised by these groups and what security concerns arise in their use of digital technology. While the insights differ for the two settings, they share some overarching findings made possible through ethnography.

We observed how the particularities of the physical environments distinctly influenced people's digital practices and security needs in ways they themselves took for granted. In both settings, digital connectivity was limited and disrupted, which led to a series of workarounds. In the seafarer study, onboard observations highlighted how seafarers rationed their Internet usage by using low data consumption applications or by structuring their work and rest routines to connect when the ship was within phone signal range. This need to connect every time the opportunity arose often perturbed established security practices onboard the ships, including navigating the ship through busy and narrow sea passages. Observations also revealed specific collective practices, such as the sharing of account details in order to access each other's data allowances and collective strategies to circumvent monitoring mechanisms put in place by the ship's operating companies. Trust relations between crew members emerged as the bedrock of onboard notions of security. This was underpinned by the fact that the confinements of the ship (limited shore leave, ship monitoring, increased automation, stricter socialising and alcohol consumption policies and larger ships with smaller crews) led to increased isolation and separation from wider support networks, which meant that seafarers largely relied on each other for security. However, this security was short-lived and had to be constantly re-established. Variations in employment contracts (from three months for the captain to nine months for the crew) and uneven manning logistics, meant that crew compositions were repeatedly changing, making it difficult - if not impossible - for crew members to maintain continuous relationships or establish sustainable collective practices to mitigate shared vulnerabilities.

In the Greenlandic context, unreliable and expensive digital connectivity forced many of Nuuk's inhabitants to restrict online work activities or interactions with friends and family to places with WiFi access, generally their homes or workplaces, with transitions between these places being perceived as disruptive. As the only place which offered publicly accessible WiFi, Nuuk's library had evolved to become a meeting place for economically disadvantaged Greenlanders who came there primarily to use different online services. After opening hours, people of all ages were observed leaning against the library's outer walls with their phones in their hands, continuing to use the WiFi. Digital connectivity hence emerged as an increasingly important tool for a number of individual and collective security practices. As Greenland's population lives dispersed across a vast area with little physical infrastructure connecting individual settlements and towns, digital connectivity has materialised as a central tool to counteract the effects of physical and social isolation. Digital connectivity offers access to platforms for entertainment but also civic engagement, education, business development and the maintenance and creation of bonds with friends and family. Particularly Greenlandic women, who noted that digitalisation was paralleled with an increase in harassment, were observed engaging in the shaping of these online 'safe spaces' to foster digitally enabled collective security practices. Through observations, digitalisation itself thus emerged as an emancipatory agent, enabling and fostering economic independence, political engagement and personal security; particularly for Greenlandic women.

While only covered in brief and high-level terms here, both studies show how an ethnographic approach can uncover security practices and needs that social groups take for granted. They reveal the emergence of distinct collective security responses to individualising technologies and environments as well as institutionalised structures. This is precisely why ethnography matters to information security.

Ethnographic fieldwork onboard container ships (picture: author's own).



References and notes:

[1] See e.g. Paul Dourish. Implications for design. Proceedings of the SIGCHI conference on Human Factors in computing systems. 2006; and Hernan Palombo et al. An Ethnographic Understanding of Software (In) Security and a Co-Creation Model to Improve Secure Software Development. SOUPS, 2020.

[2] Paul Atkinson. For ethnography. Sage, 2014.

[3] In this piece, we do not cover how quantitative studies fail to provide insights into people's actual security needs and practices, but simply note that both surveys and questionnaires are rather futile means of inquiry here.

[4] Andrew Crabtree et al. Ethnography considered harmful. Proceedings of the SIGCHI conference on human factors in computing systems, 2009.

[5] Harold Garfinkel. Studies in Ethnomethodology. Prentice-Hall, 1967.

[6] In ethnographic terms, the time spent conducting fieldwork in both settings was somewhat short.

THE SERIOUS PRACTICE OF CLOWNING AROUND ONLINE

Lizzie Coles-Kemp

> Professor ISG

I joined the ISG in 2008 and in that first year I was part of a team that was awarded funding for a project called Visualisation and Other Methods of Expression (VOME). The goal of VOME was to discover why people shared personal information online and how these acts of sharing related to people's notions of privacy. VOME primarily worked with underserved and marginalised communities who had been swept up in the UK government's digital by default agenda. The traditional methods of research engagement were not always well received by the communities that VOME worked with and it soon became clear that we needed to rethink our methods of engagement. VOME recruited clown and artist Freya Stang to be the project's artistic co-ordinator and she worked with the researchers to develop a form of engagement that was more inclusive and participant centred. Working with Freya fundamentally changed the way that I practice research. However, it also put things in motion that was to change Freya's practices too.

Freya, now the Artistic Manager for French theatre company Simsalabim Productions, is also the Recruitment and Educational Manager for the Norwegian Hospital Clowns, Sykehusklovnene. Until the pandemic, Sykehusklovnene had been providing professional clowning for over 20 years in hospitals the length and breadth of Norway. Sykehusklovnene, with 60 professional actor-clowns, perform in 17 hospitals in Norway, from the south in Kristiansand to 1382 kilometres further north in Tromsø. They clown for patients aged up to 18 years and their families. The work these clowns do is regarded as vital to patient wellbeing. In March 2020, for the first time in Sykehusklovnene's history, hospitals closed and the Norwegian medical clowns were no longer able to enter their workplace. Even when access to the hospitals began to open up three months later, blended forms of clowning were needed.

Artistic Director for Sykehusklovnene, Vibeke Lie, together with the Senior Clown team had the idea to urgently develop a digital clowning programme and Freya was appointed as the initial manager. This is where her work with us provided an input into the design of the programme. Medical clowning places safety and security at the core of all its practices; not only is patient confidentiality essential but so, too, is the emotional and physical wellbeing of both patient and clown. It is vital that digital clowning also reflects these principles.

Norwegian hospitals have a near country-wide digital healthcare platform Norsk Helsenett, broadband is widely available across the country, and the children that the medical clowns visit usually have easy access to tablets and laptops. Whilst this meant that the digital clowning programme could be built on top of a robust and secure digital infrastructure, it also meant that the programme had to comply with the hospital information security policies and procedures. However, from her work with us, Freya knew that a secure technological platform was not enough to provide the kind of safety, privacy and security that was needed. So Sykehusklovnene developed a form of digital clowning that fuses technology with policy, process and performance practice to meet their security goals.

Access to the digital platform had to be carefully specified: secure logon to the platform, access control to the individual platform spaces to be used for the sessions, and a secure process for the closing and opening of platform spaces. Access was further complicated because Sykehusklovnene's clowns work in clown duos and this meant that three digital spaces had to come together securely to form a shared space in which the personal information generated during a session was protected. Access control was also needed to regulate access between patient sessions. For example, there had to be a secure means for the clowns to rest and prepare without coming out of the platform, while having the option to remove their red noses and come out of clown character.

Patient privacy was paramount, particularly when the clowns worked with patients isolating at home. Privacy controls also became part of the clown practice as performance techniques had to be developed to quickly determine who was in the room with a patient at the start of a clowning session – something not always easy to see on screen. Clown, as well as patient, privacy was also important since, due to the COVID lockdown, the clowns had to access the digital space from their own homes. Peer-review and assessment is key to maintaining high quality medical clowning. Digital clowning therefore had a mechanism whereby clowns could learn from each other and be independently assessed in a way that did not break the multi-layered privacy and security of the clown-patient interaction.

Secure digital clowning is not just a question of technology, policies and processes. Performance techniques also play a vital role in creating safe and secure performance spaces. A triangle of communication between the clown duo and the patient creates a secure perimeter around that space enabling the clowns to safely play and bring joy, allowing the most vulnerable in our society to forget about the challenges and difficulties they face on a daily basis. This perimeter is achieved by creating a simple home digital studio with appropriate (non-scary) lighting and adjusting the clown duo's physicality, movement, sound, timing and rhythm for each patient visit. Freya's training programme invites her colleagues to consider the use of the screen, the role of face and breath, as well as body gestures moving beyond the screen, when learning to adapt their performance practice to create this secure triangle of communication.

One year later, digital clowning is an integral part of Sykehusklovnene's clown-patient meetings. Digital clowning now enables Sykehusklovnene to reach patients when hospitals are on COVID red alert and physical visits are no longer possible. They can also remain part of the care programme when a patient returns home and is still in treatment. Children in palliative care are prioritised and digital-clown visits for this patient group are often longer.

Freya has now developed a programme that ensures that all of Sykehusklovnene's performers are trained in digital clowning. I have been following the evolution of Norwegian digital clowning whilst re-working my own research practice in response to COVID restrictions. Once again, I am struck by how much clowns can teach us as they pioneer safe and inclusive engagement in a post-COVID world.

Image: Medical Clowns Beatriks B. Bringebær and Lucas coming to terms with new technology. Photo credit: Efrem Stein

THE ISG SMART CARD AND IOT SECURITY CENTRE (SCC)

Prof. Konstantinos Markantonakis, Dr Darren Hurley-Smith, Dr Carlton Shepherd

> Director SCC and Professor ISG
> Lecturer ISG
> Senior Research Fellow ISG

The ISG Smart Card and IoT Security Centre (SCC) was founded in 2002 and is at the forefront of the ISG's teaching and research in trustworthy autonomous systems. Recent activities are described below, with more details on our website (https://scc.rhul.ac.uk/).

Firstly, the SCC would like to thank Dr Raja Naeem Akram for his contributions. Raja completed his MSc and PhD with the ISG and, after several years in industry and academia, rejoined us in 2014 as a post-doctoral researcher on the EPSRC-funded project 'DICE' and H2020 project 'EXFILES'. He also supported other research activities, including the wireless avionics 'SHAWN' project. Raja led numerous other initiatives including our summer internship program and some event organisation. Raja has now been awarded a Senior Lectureship at the University of Aberdeen. Thank you very much Raja, and all the best!

A few years back, the SCC made a strategic decision to drive some new commercialisation activities. We are now celebrating our first achievements. In March 2019 we secured two grant awards from Innovate UK's Cyber Security Academic Start-up Accelerate Programme (CyberASAP).

The first project, Seclea, led by Raja, is building a novel solution for transparent, accountable, and auditable machine learning. This project was also accepted on the highly-competitive ICURe Programme and secured commercialisation funding from Innovate UK. It is testament to the hard work of the Seclea team, which also involves two Royal Holloway Computer Science graduates, that it attracted match funding from Europe's largest venture capital fund and an enterprise fellowship from the Royal Society of Edinburgh to establish a thriving spin-out company. Watch this space!

Our second project, PrineSec, led by Konstantinos, generates real-time analysis of an organisation's security and privacy compliance using causality chains. This was amongst the finalists of the CyberASAP programme, where we developed a working prototype (minimum viable product). We are currently exploring the next steps in its commercialisation.

In 2019, we welcomed Dr Darren Hurley-Smith as a new lecturer affiliated with the SCC. Darren's expertise will further strengthen the SCC's strategic research and teaching expansion into hardware security, side-channel analysis, ransomware mitigation, and verification of quantum random number generators. He currently teaches Security Testing as part of the MSc in Information Security.

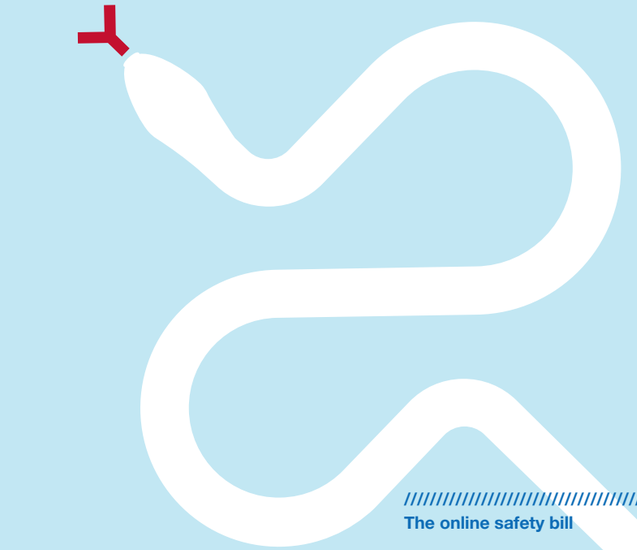
The ISG recently received a £177,000 equipment grant as part of the UKRI World Class Laboratories initiative. Darren helped to lead this bid, which resulted in the acquisition of state-of-the-art GPU and Snapdragon mobile development boards, unmanned aerial vehicle (UAV) equipment, and high-specification FPGAs suitable for digital signal processing and prototyping hardware-implemented cryptography. The ISG now possesses an autonomous vehicle prototyping platform (PIXKIT). The Computer Science Department also acquired a high-speed UAV camera array, and the Electrical Engineering Department received an ECG test-bed for human sleep studies. This equipment will allow the ISG and other researchers to experimentally verify their work and spearhead commercialisation activities in an open-use environment. This is all part of a growing emphasis within the ISG and the wider research community on multi-disciplinary, collaborative research.

Darren and Konstantinos are currently involved in the final stages of an Innovate UK Smart Grant proposal to develop a secure communications module for heterogeneous networks of robots, focusing on agriculture and logistics applications. The developed hardware module will be platform agnostic and transferable into other robotic contexts. In July 2020, the SCC secured a three-year H2020 project (EXFILES) to develop new digital forensics methods for mobile devices. This project unites European law enforcement agencies, universities and the private sector. It is a great honour to welcome back Dr Carlton Shepherd, an expert in Trusted Execution Environments (TEEs), to lead our contributions. We collaborated with Dr Rebecca Roache and Dr Jonathan Seglow from the Department of Politics, International Relations and Philosophy, to develop an accompanying ethical framework. Carlton has also helped to secure a grant award from CyberASAP. Drawing from Carlton's industrial experience in financial technology, this project ('Tensorcrypt') will develop a confidential business analytics and data collaboration platform using TEEs.

Recent SCC research has explored the emerging RISC-V processor architecture. We developed a new lightweight remote attestation system without traditional roots of trust using new RISC-V CPU features. This work was recently accepted at the IEEE Workshop on the Internet of Safe Things (SafeThings), co-located with IEEE Security & Privacy [1]. We also presented the first paper to investigate Return-Oriented Programming (ROP) attacks on RISC-V, which was accepted at ACM ASIACCS [2]. Both works are collaborations with Georges-Axel Jaloyan (Ecole Normale Superieure), who the SCC hosted as a visiting researcher in 2019. Our PhD researcher Jan Kalbantner recently published a report on decentralising national-scale energy distribution, allowing for free-floating peer-to-peer contracts that can be created, renegotiated, and ended more quickly than present [3]. PhD researcher Benjamin Semal published three papers on covert channels in cloud environments, most recently at IFIP SEC 2020 [4].

We hope that this short overview of our recent activities will excite interest. Please do contact us if you feel there are areas that we could explore further together.

[1] C. Shepherd, K. Markantonakis, & G-A Jaloyan, "LIRA-V: Lightweight Remote Attestation for Constrained RISC-V Devices," IEEE SafeThings, IEEE Security and Privacy Workshops, 2021. (To appear)
[2] G-A Jaloyan, K. Markantonakis, R. N. Akram, D. Robin, K. Mayes, & D. Naccache, "Return-Oriented Programming on RISC-V", ACM ASIACCS, 2020.
[3] J. Kalbantner, K. Markantonakis, D. Hurley-Smith, R.N. Akram, & B. Semal, "P2PEdge: A Decentralised, Scalable P2P Architecture for Energy Trading in Real-Time," Energies, 14(3), p.606.
[4] B. Semal, K. Markantonakis, R. N. Akram, & J. Kalbantner, "Leaky Controller: Cross-VM Memory Controller Covert Channel on Multi-Core Systems," 35th IFIP SEC, 2020.



THE BATTLE AGAINST ‘ONLINE HARMS’

Konstantinos Mersinas

> Lecturer ISG

Online communication has evolved into having its own norms and standards, especially on social media these days. These norms include forms of expression and communication which would not be acceptable in ‘offline’ physical environments and face-to-face interactions.

The term ‘online harms’ serves as an umbrella notion containing a number of offensive and abusive behaviours and activities online. These include, amongst other activities and behaviours: cyberbullying, trolling, cyberstalking, grooming, child sexual exploitation, sexual coercion and extortion and live distant child abuse. They also include obscene and indecent content, hate speech, radicalisation, extreme pornography, revenge pornography, eWhoring (tricking people into buying stolen personal data), child sexual abuse materials, misinformation and disinformation.

The online safety bill

The UK government has announced the formation of a new bill to tackle online harms [1]. Underpinning the bill is a realisation that law enforcement lacks skills and resources to tackle admittedly complex online misbehaviours. The idea behind the bill is simple: utilise service providers and tech giants who own the online platforms to assist in combating online harms. This means that companies will be held responsible for the content and activities on their services and platforms, and this responsibility will be proportionate to their individual size and popularity.

This might be a smart move; indeed, it has been brewing for some time. Indicatively, the Head of the National Crime Agency commented in 2019 that tech giants utilise AI for the purposes of advertisement, so why not use AI to protect children online? [2]. One cannot easily find counterarguments on this statement.

Of course, there are limitations to the scope of the bill, for example, it does not capture any type of online fraud. But, importantly, it raises – and hopes to address – difficult questions; questions debated lively in the UK and other western societies.

First, it assumes that a distinction between freedom of speech and misinformation (or offensive views, for that matter) can be objectively identified and agreed upon. Second, given that not all harmful materials and activities are illegal (e.g. something might be offensive but not illegal), it aspires to be able to articulate potential harm (e.g. indirect, psychological harm) within legal boundaries. Third, harm can be disproportionately inflicted on vulnerable groups (children, the elderly and others), but also on individuals, depending on their personal characteristics (namely, personality traits). For example, people who, in personality tests, score highly on being open to experiences and low on conscientiousness and emotional stability are found to be more susceptible to cyber crimes [3]. Moreover, such harms are often intangible and related to mental health. Fourth, people have different perceptions about what constitutes acceptable behaviour.

So, how can we overcome these limitations and minimise online harms?

The bill is a step in the right direction, but it is not sufficient on its own. In a recent presentation to an All-Party Parliamentary Group on Cybersecurity, we proposed three key components which need to be understood:

1) The individual;
2) The environment;
3) The attack vector.

Understanding these three components means understanding the phenotypic online (mis)behaviours, and, promisingly, it also means that we can equip ourselves with more suitable and effective solutions.
The first point (1) refers to individual personality traits and characteristics. Variability in these traits is to an extent genotypic, plus these individual traits remain relatively stable [4]. An indicative categorisation of these traits is the five-factor model [5] with the corresponding mnemonic OCEAN (Openness to experience, Conscientiousness, Extraversion, Agreeableness and Neuroticism). Several patterns of personality traits are found to be positively corellated with misbehaviour or criminal conduct.

But there are two sides of this phenomenon: individuals are not equally likely to behave offensively online (or offline, for that matter), but they are also not equally susceptible to victimisation [3]. The idea of utilising personality traits does not imply a kind of extensive user profiling, to ‘identify’ people inclined to misbehave or be offensive online; this would raise justified ethical cocerns. But, given that i) people with certain personality traits (as mentioned above and in [3]) are found to be more susceptible to online victimisation; and i ..) assuming that these individuals are not aware of this personality-related susceptibility; then, offering personality tests and education to users, could reduce victimisation through awareness.

Then we have the environment as the second point (2). We know that people behave differently online due to the online disinhibition effect. That is, a perceived anonymity, invisibility, and the asynchronous nature or communication cause people to behave differently – and often more offensively – online, although they would not do the same in a face-to-face context [6]. Our workshops through the Hub for Research into Intergenerational Vulnerability to Exploitation (HIVE) with law enforcement, charities and industry indicate that only a small fraction of online harmful activities are being reported. And indeed, increasing the reporting of harmful behaviours, either by the victims themselves or by ‘bystanders’ is an important and longstanding objective in combating online harms.

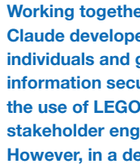
In order, however, for an intervention to be efficient, e.g. increasing the reporting of offensive content on social media, some behavioural functionality is required. Let’s assume, as an example, that the goal is to increase user reporting of abusive and offensive activity online. The intervention which would make this happen would need to be – to use a short mnemonic – EAST, i.e. easy, attractive, social and timely. Otherwise, if users are not ‘nudged’ in the desired direction, they will not be part of the solution. Note that this is a completely different approach as opposed to a company proving that they have a reporting system in place, i.e. checking a legal tick-box.

Lastly, the ‘attack vector’ (3) suggests that a significant subset of online communications includes deception, social engineering or methods of manipulation. In particular, grooming, sharing of self-generated personal materials, cyberbullying in groups, disinformation, eWhoring, encouraging of radicalised actions and speech, and hate speech can all be linked to manipulation online. Social engineering and manipulation are core components of online communication and maybe we have underestimated their power.

The battle against online harms is challenging, the new bill indicates a willingness to tackle this elusive problem, but we need to see whether the government will apply the necessary mechanisms for its implementation.

References

[1] Home Office (2020, December) Consultation outcome. Online Harms White Paper: Full government response to the consultation. Retrieved from https: www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response
[2] Hymas, C. (2019, August). *AI is not being developed fast enough to stop child abuse.* Retrieved from https: www.telegraph.co.uk/news/2019/08/24/ai-not-developed-fast-enough-stop-child-abuse/
[3] Van de Weijer, S. G., & Leukfeldt, E. R. (2017). *Big five personality traits of cybercrime victims. Cyberpsychology, Behavior, and Social Networking,* 20(7), 407-412.
[4] McCrae, R. R., & Costa Jr, P. T. (1994). *The stability of personality: Observations and evaluations. Current directions in psychological science,* 3(6), 173-175.
[5] McCrae, R. R., & Costa, P. T. (1987). *Validation of the five-factor model of personality across instruments and observers. Journal of personality and social psychology*, 52(1), 81.
[6] Suler, J. (2005). *The online disinhibition effect. International Journal of Applied Psychoanalytic Studies,* 2(2), 184-188.
[7] Halpern, D. (2015). *Inside the nudge unit: How small changes can make a big difference.* Random House.



DIGITAL IDENTITY – A CASE STUDY FOR ACCESSIBLE AND INCLUSIVE DIGITAL SECURITY

Lizzie Coles-Kemp

> Professor ISG

In March 2020, Lizzie Coles-Kemp (ISG) and Claude Heath (Media Arts) were commissioned to run a short consultation programme on behalf of the Department for Digital, Culture, Media and Sport (DCMS) on the topic of digital identity. DCMS commissioned a programme of four consultations to be undertaken with groups who are dependent on digital identities for use of essential services such as finance, welfare, health, housing and education. The purpose of the consultation was to provide a snapshot of how digital identities are part of everyday lived experiences and to provide input on the design of a future digital identity framework. These consultations are part of DCMS's wider call for evidence on the topic of digital identity.

Working together since 2012, Lizzie and Claude developed new ways to engage with individuals and groups on topics related to information security and privacy - pioneering the use of LEGO kits to encourage multi-stakeholder engagement in risk assessment. However, in a departure from this approach, the consultation programme for DCMS over the summer of 2020 was conducted via online meetings held on Zoom, as face-to-face engagement was ruled out due to the pandemic. In order to retain the details emerging during each session about the complexity of digital identity set-up and use in everyday life, Claude drew visual notes to supplement our written notes.

The consultation themes showed that digital identity is something that people encounter in their everyday lives and that the more dependent people are on essential services, the more likely they are to routinely use digital identities. Data from the consultations also revealed that it was not uncommon for people to need help to manage their digital identities; help might come from professionals working in support services or from friends and family providing more informal help. From an identity service perspective, such third-party support might be regarded as a form of social proxy.

Claude's illustrations depicted the many frustrations and exasperations with the design and use of digital identity verification tools and systems that the participants encountered. In particular there were frustrations over what was required in terms of proof of identity: how often they had to prove their identity, in what format they had to provide that proof, and the variability in what constitutes proof. Some also found the language used in digital identity tools too difficult and technical. The cost of providing physical proof was too high for some: for example, the cost of a passport or of a provisional driving licence, the cost of having documents printed, and the cost of accessing copies of documentation such as birth certificates. Equally, the technological costs of accessing digital identity services were also too high for some: the cost of acquiring technology and connectivity.

The need for informal assistance was a topic that participants raised themselves and discussed in great detail during each session. The digitalisation of services has left many feeling both unsure of how to access essential services and annoyed at the lack of help and support on offer from the service providers. This lack of support coupled with the poor design of many digitalised essential services left some participants describing the digital services as adversarial and a cause of stress. Digital identity systems could also be too rigid and not recognise the status and roles of individuals. For example, individuals who are caring for a sibling do not often have their caring role reflected in the set-up of their sibling's digital identity.

Despite these challenges and frustrations, participants recognised the value of a digital identity scheme that could be used across all essential services. However, such a scheme, it was felt, would only be successful if it was designed so as to not disbenefit people with limited capabilities and resources. Each participant group, in different ways, reflected on their hopes and aspirations for future digital identity programmes. All groups coalesced around the following hopes:

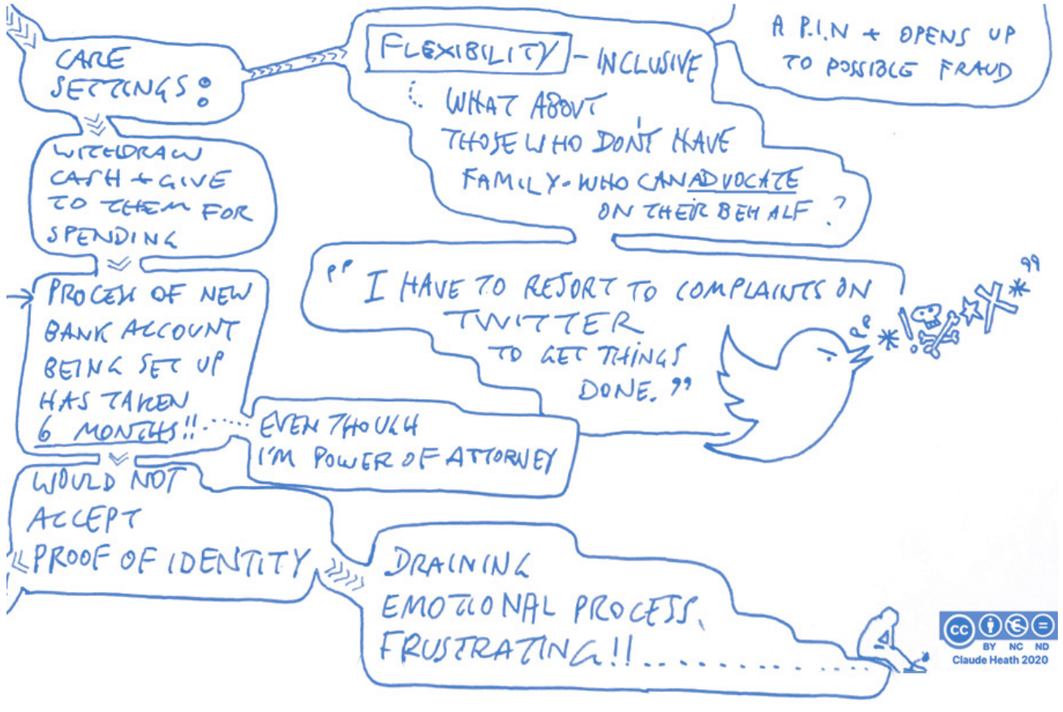
- An identity system that works for the people, rather than people having to accommodate to the identity system.
- An identity system that respects a person's rights and that is accessible to all.
- An identity system that enables a person to have autonomy and control over their own digital identity.

Realising such hopes requires that we ground the design of technology and systems in the principles of accessibility and inclusion. To make digital identity universally accessible means that we no longer think of a single individual technology but, instead, a collection of identity tools and processes embedded within the naturally occurring support structures in people's everyday lives. Such a collection of tools enables people experiencing differing levels of economic and other constraints to benefit from digital identity technologies. It also requires that we have processes and techniques that can be used to identify where a technology might exclude people, whom it might exclude, and why. Coupled with this, processes and techniques are needed to identify where such technologies might harm the security of an individual. Above all, it requires that technology is designed and deployed in such a way that it is usable for those who need it; this means a usability that is not simply confined to interface design but that also ensures that the underlying identity and access processes and policies that the technology supports are usable. This is not only a question of technology design, but also a question of how we regulate the digital identity market to ensure that its offerings are inclusive and accessible. Regulation is typically needed in areas of technology use where values and goals are contested and the data from these consultations indicate that the question of inclusive and accessible digital identity is one such area.

The ISG has worked for over ten years on topics related to digital inclusion and the security issues that arise from digital marginalisation. It is encouraging that central government is giving focus to the topic of digital inclusion as it moves forward with digital infrastructure programmes.

(The views expressed in this article are those of the author. The original consultation report is available: https://pure.royalholloway.ac.uk/portal/files/39967033/Digital_Identity_Ground_up_Perspectives_DCMSRHUL_2020.pdf)

Figure caption: "This is a snippet from one of Claude's illustrations. It shows some of the frustrations one group of participants experiences with current digital identity tools and processes."



COUNTRY-2-COUNTRY 2020 - CELEBRATING CYBER SECURITY INTERNATIONAL COLLABORATION AND SUCCESS

Keith Mayes

> Professor ISG

Royal Holloway, University of London, via its Information Security Group (ISG), is one of the six Founder Members of the International Cyber Security Center of Excellence (INCS-CoE). The mission of this organisation is to facilitate collaboration between academia, industry and government for education, research and data sharing, in the field of cyber security. The other Founder Members are Imperial College London (UK), Keio University (Japan), Kyushu University (Japan), UMBC (USA) and Northeastern University (USA). I am the Royal Holloway board member, and current Vice-Chairman of INCS-CoE.

On the 6th December 2020, the ISG was proud to host Country-2-Country 2020 (C2C2020). This was the inaugural capture the flag competition of INCS-CoE, and was an online, 24-hour marathon competition between 31 teams of five players. Each team was mixed by nation and institution in the INCS-CoE spirit of promoting international collaboration and friendship within cyber security education and taking inspiration from previous Cambridge-2-Cambridge competitions. The event was only possible thanks to support and sponsorship from the UK National Cyber Security Centre, the UK government Department for Digital, Culture, Media and Sport, Gemserv, RSA, INCS-CoE and Royal Holloway, and using systems and challenges from Fifth Domain.

The ISG's Daniele Sgandurra was chair of the international organising committee, which included representatives from University of Cambridge (UK), MIT (USA), George Mason University (USA), Edith Cowan University (Australia), Technion (Israel), Keio University (Japan) and UMBC (USA). The next four C2Cs will be hosted by Technion (10th August 2021), MIT, Keio University and Edith Cowan University.

The competition was closely fought to the end, with impressive individual and team performances. Everyone was kept in suspense about the winners until the prize-giving awards on 10th December. I was delighted to preside over the award ceremony, which included a welcome from Royal Holloway Principal Paul Layzell. Prizes were awarded for the top three teams and we were thrilled to discover a Royal Holloway competitor, Marcel Armour, in the winning team, and another, James Whaley, in the runners up. To have Royal Holloway competitors in the top two teams was the icing on the cake. However, there is not much time for us to rest on our laurels as C2C2021 is rapidly approaching!

THE ALL PARTY PARLIAMENTARY GROUP IN CYBER SECURITY

Dear Readers

When I was elected as the MP for Barrow and Furness in 2019, I was determined to do my part in ensuring a safe and prosperous future for all the citizens of this great United Kingdom. Little did I suspect the threat of a global pandemic, but I was very concerned about the growing threats to cyber security, especially from nation states. When the former Chair of the Cyber Security APPG, Alex Chalk MP stepped down due to added government responsibilities, I was only too delighted to take his place.

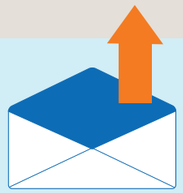
My fellow officers of the APPG now include the following MPs: the Rt Hon George Howarth, Khalid Mahmood and Owen Thompson; and from the Lords: Viscount Waverly, Admiral the Rt Hon Lord West of Spithead GCB DSC PC ADC DUniv, the Rt Hon Lord Arbuthnot of Edrom, the Rt Hon Baroness Neville-Jones, Baroness Neville-Rolfe and Lord Mackenzie of Framwellgate OBE; with Professor Keith Mayes and Andrew Henderson representing the ISG as secretariat.

Our last physical meeting was on the 3rd March 2020 and concerned aviation security, with speakers from the CAA, NCSC and industry. Thereafter we had to adapt to on-line meetings, which thankfully have proved quite popular. The meeting of the 3rd November 2020 was about the US Department of Defense's cyber security programme, whether it should be adopted in the UK and the impact on UK firms supplying the DoD. On the 25th November we welcomed Matt Warman, Parliamentary Under Secretary of State and Professor Charles Burton of the Canadian Macdonald Laurier Institute; in a discussion around High Risk Vendors in the supply chain and how they may apply soft influence on industry and academia. On 18th January 2021 we discussed the need for reform of the Computer Misuse Act, with Robert Carolina from Royal Holloway, University of London and Ollie Whitehouse from the NCC group.

In the near future, we are planning meetings on "Artificial Intelligence and Cyber Security" and "online harms"; and soon after we hope to have a joint meeting with the APPG for Energy Security. I am convinced of the valuable role of the APPG in informing parliamentarians of important issues, and I will ensure that insights and findings are fed into appropriate channels for influencing policy. In this endeavour I greatly appreciate the assistance of the ISG, for supporting the secretariat, and for the extensive cyber security expertise that it brings to the APPG discussions.

Yours Sincerely

Simon Fell MP
APPG Chair and Member of Parliament for Barrow and Furness



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

Twitter:
twitter.com/isgnews
@ISGnews

LinkedIn:
linkedin.com/groups?gid=3859497

You Tube
youtube.com/isgofficial

CONTACT INFORMATION:

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

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

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