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 prizes 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.

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.
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.

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 methodological 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; and 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 on solving crossword puzzles. Did any of the same skills serve you well as an academic researcher?

I think they did. A more interesting question is now being an academic served me well as a crossword setter! I left academia to focus on my new interest – 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 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.

On to – 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 = ART]

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 degree. 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 has led to 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 those of 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 move 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.
The ISG has a long tradition in cybersecurity research. It is one of the largest academic departments working in the Defence Science and Technology Laboratory (DSTL), 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 broad tradition of information security education. Founded in 1992, the ISG’s flagship MSc Information Security masters programme has seen over 3,000 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 research and development in information security or dealing with a practical aspect of information security. Because our students come from a range of backgrounds, we want them to develop 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 Comerford prize. These MSc projects are re-written in accessible form and published online on the Computer Weekly website (https://www.computerweekly.com). They 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/).

Postgraduate research students, working on postgraduate research, also contribute to the security and safety 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

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 went 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 are not in the syllabus and which are not that of organisational (in)action but address in a timely manner. Reactive solutions have been effective but stressful. It is imperative that we develop community groups and toolkits to not only support rapid change, but also ensure that outstanding issues are addressed. Our image and the appropriate institutional use of research and of the evidence-based approach must be protected.

In contrast to the increased participation of students and better attendance of the online material, it is not clear that students and teachers adapted well to the change. The change in teaching style and delivery has forced us all to adopt new working styles and for those who are used to teaching face-to-face, it may be that they were not prepared to make the shift.

We as staff can draw on university resources 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 are reluctance to learn the technology placed in front of them.

The engagement, retention and performance of students have been excellent. The challenges are real, but they can be overcome. We as staff can draw on university resources to help us through this period and we must not allow this to remain out of sight.

As we return to campus, we will need to revisit the open problem of truly hybrid teaching. In contrast to the fully digital delivery which was nothing new, initially defined in the 1960’s, then revised in the 1990’s to the definition we now have today which may not be sustainable in the long term.

There have been clear benefits to digital delivery: student engagement increased, availability of information increased, and we can now have access to information from anywhere in the world. However, there are also clear disadvantages: the ability to scan the room and see whether students were present is not available in this new era of blended learning. As we return to campus, we will need to revisit the open problem of truly hybrid teaching.

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 went 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 are not in the syllabus and which are not that of organisational (in)action but address in a timely manner. Reactive solutions have been effective but stressful. It is imperative that we identify those who may be having trouble with the change and offer them additional support. As we return to campus, we will need to revisit the open problem of truly hybrid teaching.

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 went 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 are not in the syllabus and which are not that of organisational (in)action but address in a timely manner. Reactive solutions have been effective but stressful. It is imperative that we identify those who may be having trouble with the change and offer them additional support. As we return to campus, we will need to revisit the open problem of truly hybrid teaching.

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 went 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 are not in the syllabus and which are not that of organisational (in)action but address in a timely manner. Reactive solutions have been effective but stressful. It is imperative that we identify those who may be having trouble with the change and offer them additional support. As we return to campus, we will need to revisit the open problem of truly hybrid teaching.

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 went 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 are not in the syllabus and which are not that of organisational (in)action but address in a timely manner. Reactive solutions have been effective but stressful. It is imperative that we identify those who may be having trouble with the change and offer them additional support. As we return to campus, we will need to revisit the open problem of truly hybrid teaching.

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 went 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 are not in the syllabus and which are not that of organisational (in)action but address in a timely manner. Reactive solutions have been effective but stressful. It is imperative that we identify those who may be having trouble with the change and offer them additional support. As we return to campus, we will need to revisit the open problem of truly hybrid teaching.

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 went 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 are not in the syllabus and which are not that of organisational (in)action but address in a timely manner. Reactive solutions have been effective but stressful. It is imperative that we identify those who may be having trouble with the change and offer them additional support. As we return to campus, we will need to revisit the open problem of truly hybrid teaching.

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 went 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 are not in the syllabus and which are not that of organisational (in)action but address in a timely manner. Reactive solutions have been effective but stressful. It is imperative that we identify those who may be having trouble with the change and offer them additional support. As we return to campus, we will need to revisit the open problem of truly hybrid teaching.
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 December 2019 cohort’s first-year teaching 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 lab sessions 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 shared experience. 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 managed to run 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 students who have been exposed to more than just the technical elements of cybersecurity. The autonomous aspects of a PhD can also be challenging and can be particularly hard during the last twelve months, especially those that did not have scholarships and deadlines which helped throughout the challenge, including trying to reduce pre-preparation nerves by keeping us distracted with some great conversations.

There has been much discussion about the digital divide and the Year 1 CDT students from the Centre for Doctoral Training (CDT) in Cyber Security for the Everyday (CSCED) have been able to make a contribution to reducing this by teaching cyber security training to refugees and help throughout the challenge, including trying to reduce pre-preparation nerves by keeping us distracted with some great conversations.

The next round was all a blur. We had to digest the lack of preparation time compared to the previous one, as now serious cyber incidents had occurred. In the scenario, the ICU Oxygen scenario was centred around threats relating to the team in order for us to conduct further research into the impacts of the threats, and help throughout the challenge, including trying to reduce pre-preparation nerves by keeping us distracted with some great conversations.

We were ecstatic at the end of the first day. It had been a tough challenge, but we had also advanced to the semi-finals. As we watched back, we felt we had put together a well-deserved bake and made pancakes (it was Shrove Tuesday), before settling in for a well-deserved break and made pancakes (it was Shrove Tuesday), before settling in for a well-deserved break and made pancakes (it was Shrove Tuesday), before settling in for a well-deserved break and made pancakes (it was Shrove Tuesday), before settling in for a well-deserved break.
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 that has begun to rise to public awareness with reports of internet shut-downs among protests across the world, starting in Hong Kong with the anti-extradition law bill amendments protests (though an internet shutdown did not take place there) and later spreading to protests in India, Iran, ISIS, 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 full attackers with their social graphs just by passively observing them overnight (without unlocking the phone). We verified the attacks in practice on Android devices using an attacker’s device and later spreading to protests in India, Iran, Hong Kong protesters’ playbook”. Bridgefy was not envisioned as a “protest app”, its use was not intended for such a use case. The use of PKCS#1 v1.5 was also problematic – thanks to competition with Gzip and then encrypted block-by-block using RSA with the decrypted 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 reused the Wi-Fi 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 Denial of Service attack with any two users in range, without the users noticing that their messages are no longer private or public.

In Bridgefy as analysed, messages send to the Bluetooth running network first compressed with Gzip and then encrypted block-by-block using RSA with the decrypted 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 reused the Wi-Fi 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 Denial of Service attack with any two users in range, without the users noticing that their messages are no longer private or public.

By using the Bluetooth mesh network were first compartmentalized as privacy and authenticity as well as security goals that cater to these needs. We note, though, this requires understanding “these things are not done in isolation”. The use of PKCS#1 v1.5 was also problematic – thanks to competition with Gzip and then encrypted block-by-block using RSA with the decrypted 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 reused the Wi-Fi 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 Denial of Service attack with any two users in range, without the users noticing that their messages are no longer private or public.

In Bridgefy as analysed, messages sent to the Bluetooth running network first compressed with Gzip and then encrypted block-by-block using RSA with the decrypted 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 reused the Wi-Fi 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 Denial of Service attack with any two users in range, without the users noticing that their messages are no longer private or public.
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 test the 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 it brought by official standards recognition, albeit predominantly within the UK. The second part BS 7792-1:1999, 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 over 7009 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 Procedure" in October 1999, resulting in its publication, with minor amendments, as ISO/IEC 17799:2000 on 1st December 2000. Whether 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 standards 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 the protection which was the primary focus of ISO/IEC 27002:2013. The fact that ISO/IEC 27002 was increasingly seen as outdated relative to current cyber threats, and some of their incorporation into the new 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 7792-2:2002, was officially launched on 9th 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.gamma.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 Appropriateness (SoA). Organizations 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 27001, must indicate whether or not it has been implemented and in either case why. That is, while standard conformity does not require implementation of any of the controls in ISO/IEC 27002 (it is, and always has been, a code of practice rather than anything more), 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 27001 to a single 27001 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 27001, was published in 2006, 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, five further standards have been added to the 27001 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 the controls in ISO/IEC 27001 has been updated at intervals (including in ISO/IEC 27001:2013, 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 relatively unsupportable) standards within the 27001 series rather than incorporating them into the base 27001 standard. The 2013 revision is intended to suffer through the international standards agreement process and started to lag behind current practice, quite a contrast to 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 control) rather than the 14 categories of ISO/IEC 27002:2013. This avoids some of the awkward shoe-horning of controls into categories in the current standard, as well as enabling some of the obvious controls to be removed. Even more importantly, new controls have been added and redundant ones removed.

Such a radical change will no doubt require many security industry and user groups to re-approach 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 logic is not so earth-shattering, as the new version of ISO/IEC 27002 provides a helpful annex giving guidance on the new and revised 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

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.

NIST plans to make a draft standard available between 2022 and 2024.

The sense of “we are getting close to the deliverable of this standard” is reinforced by the NIST process coming to a close is mirrored in the “UK Cyber Security Sectoral Analysis 2022”, 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; and 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 mechanisms and digital signatures. On the other hand, lattices have underperformed 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 “quantum-safe world” lays a wealth of constructions where the viability of lattice-based schemes – or, indeed, any post-quantum scheme – 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 Privacy-Pass, 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, MSL, 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.


2 Technically, digital signatures are not an “asymmetric primitive”, they exist in “Mimicrypt”. But in practice we tend to build from them 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.
WHY ETHNOGRAPHY MATTERS TO INFORMATION SECURITY
Rikke Bjerg Jensen
Nicola Wendt

An emerging body of information security scholarship has explored the security needs and practices of select 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 always explicitly stated, is the understanding that 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, who defines ethnography as “the world of difference between a commitment to long-term 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 security needs and practices and need to be interviewed. 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 organise action and interaction in the settings they inhabit” (emphasis in original). Ethnographic work is thus capable of unveiling ‘social facts’ about the groups we study and go beyond rhetoric, cultural interpretation or critical discourse found elsewhere [2,5].

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 five weeks onboard two container ships in Nuuk and two weeks in Copenhagen, Rikke spent five weeks onboard two container ships in Greenland [6]. We 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 due to 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 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 rationalised 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 the ship’s 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 needs and 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.

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

"There is a world of difference between a commitment to long-term 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]
things in motion that was to change I practice research. However, it also put Freya fundamentally changed the way that recruited clown and artist Freya Stang to be by the communities that VOME worked with engagement were not always well received communities who had been swept up in funding for a project called Visualisation I joined the ISG in 2008 and in that first

ONLINE

OF CLOWNING AROUND

noses and come out of clown character. secure means for the clowns to rest and Access was further complicated because security goals.

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 their tribulations and difficulties they face on a daily basis. This perimeter is achieved by creating a silent studio environment with patient visitors and meant that the digital clowning programme could be built on top of a robust and secure digital infrastructure. It also meant that the hospital had to comply with stringent hospital information security policies and procedures. However, from her work with us, Freya knew that a secure and non-invasive platform was not enough to provide the kind of safety, privacy and security that was needed. So she now developed a form of digital clowning that fuses technology with policy, process and performance 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 platforms, spaces to be trusted, separate sessions, and a secure process for the closing and opening of platform spaces. As my role in further complicating Sykehusklownene’s clowns work in clown duos and this meant that these digital spaces had to come together and form a shared space in which the personal information generated during a session was protected. Access controls and policies needed to regulate access between patient sessions. For example, there had to be a secure means for the clowns to test and prepare without coming in contact with the platform, while having the option to remove their nose and come out of clown character. Patient privacy was paramount, particularly with the clowns worked with families isolating at home. Privacy controls also became part of the clown practice and it developed to quickly determine who was in the room with a patient at the start of a clowning session, somethat will always easy to see on screen. Clown, as well as patient, privacy was also important since, in the COVID lockdowns, they 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 breach the multi-layered privacy and security of the clown-patient interaction.

The ISG Smart Card and Iot Security Centre (Scc) was founded in 2002 and is 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.ruthealco.ac.uk/).

Firstly, the SCC would like to thank Dr Raja Naeman 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 postdoctoral researcher on the EPSRC-funded project “DICE and H2020 EXFILES”. He also supported other researchers including the wireless avionics ‘SHAWN’ project. Raja led numerous other initiatives including our summer internship programme and some event organisation. Raja has now been awarded a Senior Lectureship at the University of Greenwich. 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, Seclia, led by Raja, is a cross-disciplinary solution for transparent, accountable, and auditable machine learning. This project was also accepted on to the government-funded and secured commercialisation funding from Innovate UK. It is testament to the hard work of the Seclia 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, PrimeSec, led by Konstantonas, generates real-time analysis of an organisation’s security and privacy concerns using causalities. 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 strategy of teaching expansion into hardware security, side-channel analysis, ransomware mitigation, and the legal and organisational aspects of this number generators. He currently teaches Security Testing as part of the MSc in Information Security.

The SCC recently received a £177,000 grant as part of the UKRI World Laboratory initiative. Darren helped to lead this bid, which resulted in the acquisition of state-of-the-art GPUs and Snaphdragon mobile development boards, unmanned aerial vehicles (UAV) equipment, and a high-speed UAV camera array for digital signal processing and prototyping hardware-implemented cryptography. The SCC now possesses an autonomous vehicle prototype platform (PIXIT). 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 SCC and other researchers to re-purpose their work and spearhead commercialisation activities in an open-use environment. This is part of the ongoing growth within the ISG and the wider research community on multi-disciplinary, collaborative research.

Darren and Konstantonas are currently involved in the final stages of an Innovative UK Smart Grant proposal to develop a secure communications module for heterogenous networks of robots, focusing on agile wireless communications. Raja has also helped to secure a £1M grant for the SCC secured a three-year H2020 project (EXFILES) to develop new digital forensic tools for mobile devices. This project uniteles European law enforcement agencies, universities and the private sector. It is a great honour to welcome back Dr Carlton Shepherd to the SCC as our new Research Director on Cyber Security Environments (TEEs). To lead our contributions, we collaborated with Rebecca Roache and Dr Jonathan Seglow from the Department of Computer Science, Imperial College, London, in the areas of 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, the SCC 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 lightweight remote attestation system without traditonal root of trust using new RISC-V CPU features. This work was recently accepted at the IEEE Design-on-Chip (DoC) conference. We also collaborated with Dr Jan Kalfant recently published a report on decentralising national-scale energy distribution, allowing for energy participants to be compensated when the grid can be created, renegated, and ended more quickly than present [3]. PhD research on digital signal processing and TEEs 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.

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, grooming, child sexual exploitation, sexual coercion and extortion and live direct child abuse.

They also include obscene and indecent content, hate speech, radicalisation, extreme pornography, revenge pornography, "whoring" (tricking people into buying stolen personal data), child sexual abuse materials, misinformation and disinformation.

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.

Understanding these three components means understanding the phenomenological online misbehaviours, 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 correlated 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 profiling, 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 ///

[3] Of course, there are limits 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.
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 not to disbenefit people with limited capabilities and resources. Each participant group, in different ways, reflected on their hopes and aspirations for future digital identity programmes. 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 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 not to disbenefit people with limited capabilities and resources. Each participant group, in different ways, reflected on their hopes and aspirations for future digital identity programmes. 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 not to disbenefit people with limited capabilities and resources. Each participant group, in different ways, reflected on their hopes and aspirations for future digital identity programmes. 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 not to disbenefit people with limited capabilities and resources. Each participant group, in different ways, reflected on their hopes and aspirations for future digital identity programmes. 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 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!
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

CONTACT INFORMATION:

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

Twitter: twitter.com/isgnews
@ISGnews

LinkedIn: linkedin.com/groups?gid=3859497

YouTube: youtube.com/isgofficial