# Information Security Group

Review 16/17

ROYAL HOLLOWAY UNIVERSITY OF LONDON

## WELCOME
## Prof. Keith Mayes

> Director of the Information Security Group (ISG), Head Of The School Of Mathematics and Information Security at Royal Holloway University of London

It is difficult to believe that a year has passed since my last newsletter welcome; until I recall some momentous events. The international political landscape has shifted with Brexit, the USA elections and rumblings of changes in other countries. In the world of cyber security, the stories are hitting the headlines like never before, with massive data losses, state sponsored eavesdropping and hacking, political pressure on encrypted communications and social media services, as well as the rise of fake news. In response, the UK government had created the National Cyber Security Centre (NCSC) and strategies to make the UK the "hardest target". Well, I am very pleased to say that against this backdrop of change and many portents of doom, the ISG is doing extremely well on all fronts!

A notable highlight from the last year, was the renewal of EPSRC/GCHQ funding for our Centre for Doctoral Training (CDT) in Cyber Security, which with College support means we can attract/fund, 10 top quality PhD students each year, complementing the outstanding students already within the CDT. We also extended (+ five years) our status as a GCHQ/NCSC recognised, Academic Centre of Excellence in Cyber Security Research (ACE-CSR), and our funded research exceeded targets, making us one of the best performing departments within the College.

Student numbers for our campus MSc in Information Security have grown for the past two years in a row and seem likely to increase again for next year, with 200+ students on campus and even more on our Distance Learning programme. We are also teaching a lot of Computer Science undergraduates who have opted for specialist ISG modules in information/cyber security. Our alumni now numbers around 4,000 and industry engagement and employability remain excellent. New for the coming year is a module on human factors and privacy, research methods training, plus a security management module that will be offered to undergraduates in the School of Management.

We added to our government engagements by being instrumental in the creation and operation of the All Party Parliamentary group in Cyber Security. I was also privileged to be an invited guest speaker at the Commonwealth Parliamentary Association Cyber Security Day, and attended the royal opening of the NCSC.

Our research profile continues to expand with growing emphasis on human factors, critical infrastructure, data privacy, software security and of course the Internet of Things (IoT). The security of IoT (or lack of it) is extremely worrying, so several ISG experts are supporting the work of the IoT Security Foundation; which is chaired by our very own Professor Paul Dorey.

Not surprisingly, we have expanded to cope with the research, teaching and external engagement demands on the ISG, and welcomed three new staff members, with another two vacancies to be filled this year. We are also working closely with experts in other departments/disciplines at RHUL.

I predict another challenging, but exciting year for the ISG, and please do not hesitate to contact us if you require further information.

INDEX



## MSC UPDATE
## Dr Chez Ciechanowicz

> MSc Information Security Programme Director

At the start of term in September 2015, we had a 30% increase in new student intake as compared with September 2014. A year later we had another increase in numbers; this time it was 15%. At the start of April 2017, the total number of applications for the 17-18 year is 15% up on the corresponding figures for April 2016. Adding these figures to the Distance Learning MSc intake, by September 2017 we are very likely to have more than 600 registered MSc students. In addition to this we now have approximately 4000 alumni. This must surely make our MSc the largest such programme in the world – something that we are hugely proud of! Given the current shortage of well-qualified cyber security professionals, we hope that in a small way we are helping to improve the situation.

Recently, there has been a surge of interest related to the human aspects of cyber security – this is perhaps not surprising! In the "2015 Information Security Breaches Survey", commissioned by the UK Government, it states that 50% of the worst breaches suffered by UK companies were caused by avoidable human factors. Despite these figures, higher education programs on information security do not provide specific training to address the relations between individuals and the technical and managerial aspects of security. Having acknowledged this shortcoming, we are putting the finishing touches to a new module on "Human Aspects of Security and Privacy". The purpose of this module is to provide candidates with the knowledge and the methods to design security systems, protocols and procedures taking into account how individuals interact with them. Students of this module will be able to envision systems that are secure, not only because of the technical foundations of the system itself, but also because the interactions with individuals are also designed to enforce security. The module will cover the psychological, ethical, societal and legal dimensions of information security and privacy.

Each year there are two £500 prizes that are awarded during our December graduation ceremony. The first of these is awarded to the most outstanding MSc student of the year. This year the prize was awarded to Minerva Hoessl who achieved an overall average approaching 90% – a truly outstanding performance. The second prize is awarded to the student that achieved the highest mark for the MSc dissertation. The prize was awarded to Max Kington who obtained a mark again approaching 90%. Needless to say, both these students obtained an overall Distinction grade for the MSc – truly deserved!!

## DEVELOPMENTS IN DISTANCE LEARNING MSC

Prof. Peter Komisarczuk

**> Programme Director of Distance Learning**

The academic year 2016-17 has seen a number of changes in our distance learning provision: new teaching team members, Department of Culture Media & Sport cyber security scholarships, a new MOOC and updates to course content and materials.

We welcomed Dr Jorge Blasco Alis in September as a new member of the ISG and module leader for Security Management where he has led the team of three tutors to deliver the module. He has worked on the campus module and is revising the content to harmonise distance learning and campus provision for delivery in September 2017. In addition Jorge has been working with industry to develop a new module on human factors in security which we plan to have in place for September 2018.

Dr Guillermo Suarez-Tangil became module leader for Digital Forensics and the tutor team was extended with the addition of Martin Warren (Module Leader for Cybercrime) to enhance the natural synergy between the two modules. The extension of the team was required as we now have over 40 students registered on the module.

In October we welcomed Dr Daniele Sgandurra to the ISG and with the increase in student numbers he has taken on responsibility as deputy programme director for the distance learning degree. In addition he has responsibility for the campus Computer Security module and he and Geraint Price will revamp the distance-learning version of the module for delivery in September 2017.

The distance learning degree was awarded four full fee cyber security scholarships from the Department of Culture Media & Sport last summer. These were aimed particularly at increasing participation of women, minorities, ex military personnel and mid career changers who want to enter a career in cyber security. Nearly 70 applications were made in just 3 weeks and the four scholarships were awarded. This helped the distance learning degree to exceed 300 registered students for the start of teaching. Our increase in numbers is also exciting in terms of our graduating students with over 30 students expected to graduate this year on completion of their projects. Next year we should see circa 40 students completing the MSc.

////////////////////////////////////////////////////////

**New MOOC "Information Security: Context and Introduction"**

When we consider distance learning we should include a consideration of Massive Open Online Courses (MOOCs). The MOOC concept originated around 2007-8 and developed from a cooperative learning concept to a significant learning outreach with over a dozen significant providers of online open/semi-open teaching materials. The content is developed by a wide range of universities, colleges and groups or individuals to engage a wide range of learners, from school children to professionals. Additionally over the last decade the focus has moved from the provision of open education to more of a marketing tool as the business model has developed.

Dr Lorenzo Cavallaro developed the first ISG MOOC in 2013-4, which was provided through Coursera, entitled Malicious Software and its Underground Economy: two sides to every story . This was developed for delivery occasionally in specified periods on the original Coursera platform. Today the Coursera platform provides for continuous delivery of courses with content improvements that can be pushed in an ad hoc fashion as required. Lorenzo's MOOC has been very successful which inspired us to consider developing further open learning material.

Our second MOOC, Information Security: Context and Introduction , is delivered on the new Coursera continuous delivery platform and launched in February 2017. The focus of the MOOC is to provide an introduction to Information Security and provide a discussion of the scope of the curriculum in information security by introducing the discipline, outlining the Cyber Security Body of Knowledge (BoK) based on a draft of the Knowledge Areas identified by the ACM led Joint Task Force on Cybersecurity Education, coverage of some fundamental areas and concludes with an introduction to security careers, the industry and professional aspects. The focus on careers was seen as a particularly useful angle that we hope will engage new graduates and mid-career professionals to consider studying our discipline and making their career in our fast paced industry.

////////////////////////////////////////////////////////

**The Cyber Security Body of Knowledge and Knowledge Areas**

The Cyber Security curriculum has been developing over a number of years, with the ACM Joint Task Force (JTF) on Cybersecurity Education aiming to publish their version in December 2017. Such developments have led to a UK based project to develop an open Cyber Security Body of Knowledge (CySec BOK) funded by GCHQ who launched a call to create a UK consortium to develop the CySec BOK. A consortium led by Professor Awais Rashid will develop this resource over the next few years.

One perspective on the CySec BOK is to consider the cyber security knowledge areas (KAs) being defined by the JTF, although the ACM JTF constitute a largely US centric viewpoint of cyber security education for undergraduate and graduate studies. They are seen to be producing a useful resource that could be widely applicable, although requiring some modification for the education systems in different countries. The MOOC uses an early draft of their work which identified the following nine KAs:

1. Cyber Defence, such as cryptography, data security, network security, information assurance.
2. Cyber Operations, such as cyber attack, penetration testing, cyber intelligence, reverse engineering, cryptanalysis.
3. Digital Forensics, such as hardware and software forensics, incident response, cybercrime, cyber law enforcement.
4. Cyber Physical Systems, such as Supervisory Control and Data Acquisition (SCADA) systems, internet-of-things (IOT), industrial control systems.
5. Secure Software Development, such as secure systems design, secure coding, deployability, maintainability, usability of secure information systems.
6. Cyber Ethics, such as ethical use of information systems, privacy and anonymity, intellectual property rights, professional responsibility, global societal impact of information systems.
7. Cyber Policy, Governance, and Law, such as government and institutional cyber policy and practices, regulatory authorities for cyber systems and operations, cyber law.
8. Cyber Risk Management, such as cyber resilience, mission assurance, disaster recovery, business continuity, security evaluation, cyber economics.
9. Human Behavioural Relating to Cyber Systems and Operations, such as social engineering, social networks, user experience, and organizational behaviour.

These KAs map well onto our MSc, both campus and distance learning. As the JTF develop their KAs and the curriculum, we will be able to update the MOOC content and push it onto the delivery platform to give students a steer on what they should expect to find in a cyber security degree.



## BLOCKCHAIN: BEYOND BITCOIN

Dr Elizabeth Quaglia

**> Lecturer, ISG**

Blockchain has recently emerged as a promising technology, and in the last couple of years the name has vigorously buzzed in academic papers as well as industrial promotional material.

The excitement started back in 2008, when Satoshi Nakamoto shook the world with the paper "Bitcoin: A Peer-to-Peer Electronic Cash System", and gave us a glimpse of what a blockchain could do in the context of Bitcoin, the newly proposed cryptocurrency. What Nakamoto achieved was complete decentralization through technical methods and smart incentives, and blockchain was the key technology behind Bitcoin's success.
At the moment, the majority of papers discussing blockchain are still Bitcoin-related, but current trends suggest the balance is about to change.

In this article, we will give a brief overview of what a blockchain is and then explore some of the applications of this technology that go beyond Bitcoin.

////////////////////////////////////////////////////////

What Is A Blockchain?

A blockchain is, simply put, a distributed database, in the form of a list, with the following two features: 1) data is added in blocks; 2) each new block is linked (or chained) to the previous block. More specifically, each block contains data as well as a hash pointer to the previous block. (A hash pointer is defined as a pointer to where data is stored together with a cryptographic hash of that data.) This means that each block contains, in particular, a digest of the data of the previous block, which allows us to verify that the data in that block has not been changed. Indeed, if it had, the hash value would not match up due to the collision resistance property of the cryptographic hash. This feature of tamper-evidence is what justifies the appealing idea that a blockchain is an immutable record of stored data.

This simple data structure has enabled the much talked-about notion of distributed ledger, i.e., a decentralized platform to which data can be added.

But, in this distributed setting, how does one decide which block gets added to the chain? This is done by achieving a distributed consensus. Doing so is a well-known problem in distributed systems, and several consensus protocols exist allowing entities in the system to agree on a decision. (A popular example is the Practical Byzantine Fault Tolerance (PBFT) algorithm.) But again Nakamoto spiced things up by proposing a new consensus protocol, inclusive of proofs of work and incentives. Nakamoto's protocol, presented in the context of Bitcoin, works roughly as follows.

1 A node in the peer-to-peer network broadcasts its data (in the original context, Bitcoin transactions) and each node collects broadcast data into a block;
2 Each node works on finding a difficult proof of work for its block, and then broadcasts the block;
3 Nodes accept the block only if "valid" (in Bitcoin this means that the transactions are valid and not already spent) and express this by working on creating the next block in the chain.

Nodes whose blocks get added to the blockchain are rewarded with money, which is an incentive for participating in this protocol. And this is how the chain grows.

Now that we have a basic idea of what a blockchain is, let us take a look at the different types of blockchains and at what they can be used for.

////////////////////////////////////////////////////////

Permissionless Vs Permissioned Blockchains

The Bitcoin blockchain, which by many is considered to be the blockchain, was born in the context of peer-to-peer networks and in the spirit of pure de-centralization. Indeed, anyone can potentially contribute to its growth and, in some way, write history. Blockchains that operate in this model are defined permissionless, and many of the existing blockchains belong to this type.
Besides the aforementioned example of Bitcoin, all the applications that use Bitcoin as a platform rely on a permissionless blockchain. One such application is that of secure timestamping (useful to patent ideas, for instance). If you think of a blockchain as a data structure to which we can add new data, which is tamper evident and available forever once added, and to which we can associate a notion of ordering (thanks to the hash pointers), then it is straightforward to see that this can be used to build a secure timestamping system. One could also use this traceability-in-time feature as a way to prove ownership of some property, such as a stock in a company, a car or a house, without relying on a central authority.
Perhaps one of the most exciting applications of permissionless blockchains is the recent development of Ethereum, an alternative cryptocurrency that allows users to add, for a small fee, "special" data to the blockchain, i.e., a smart contract. Once the program code of the contract is uploaded, it lives and it is enforced on the blockchain. Smart contracts range from establishing a reward for the winner of a game of chess, to running an auction or performing escrowed payments. The Ethereum project can already technically allow any user to run such contracts, but it is only in its beginning, experimental phase: it promises a fruitful growth of interesting usecases.

In contrast, a permissioned blockchain is a closed ecosystem where the access of each participant is well defined and differentiated based on role. A prominent example of this can be found within Hyperledger, an open source project aiming at advancing blockchain technologies through the global collaboration of leaders in technology, finance, banking and IoT. Dr. Angelo De Caro, researcher at IBM Zurich, describes one of Hyperledger's projects, Fabric, as "blockchain for enterprise" and explains the different roles of nodes in the closed, trusted network it provides: the endorsers run the chaincodes, a generalization of the smart contracts, and the orderers run a traditional consensus protocol (e.g., the PBFT algorithm). Clearly this model departs from the original vision of complete decentralization, but the approach does enable a variety of applications, fueling the enthusiasm for it especially in the business world.

An interesting application of permissioned blockchains was presented at the 27th HP Colloquium on Information Security, held at RHUL last December, by Leanne Kemp. The founder and CEO of Everledger described how this new technology is being used to register and track ownership of valuable assets such as diamonds and artwork by collecting the asset's defining characteristics and creating a permanent record on the blockchain.

This and previous examples briefly show how blockchain technology is growing and permeating a variety of research and business areas. While blockchain is not the answer to all our problems, it has sparked some very interesting lines of work, and talented researchers keep being attracted by both the theoretical and practical challenges its numerous applications pose.

# A SURFEIT OF SSH CIPHER SUITES: AWARD-WINNING RESEARCH FROM THE ISG

Prof. Kenny Paterson

**> Professor, ISG**

Surfeit (noun): an excess of something; King Henry I of England is reputed to have died from eating a surfeit of lampreys.

SSH is a Swiss army knife for security-conscious system administrators, enabling them to remotely administer servers, perform secure file transfers, and achieve low-cost Virtual Private Networking without leaving the comfort of their desks.

The SSH protocol uses cryptography - both public-key and symmetric-key - to build a secure channel between two SSH-aware devices. The actual mechanisms to be used is negotiated by the two parties during the protocol. But how good is that cryptography? A team of ISG researchers -- Martin Albrecht, Jean Paul Degabriele, Torben Hansen, and Kenny Paterson -- recently decided to find out.

Our study led to a research paper published at the ACM Conference on Communication and Computer Security (ACM-CCS) in October 2016. The paper was one of three to receive a best paper award, from amongst more than 800 submissions. Our study also led directly to improvements in the security of the OpenSSH implementation of the protocol.

We began our work with a measurement study, scanning the entire IPv4 address space to find SSH servers, grabbing their banners and preferred algorithms. Perhaps surprisingly, roughly 1 in every 256 IP addresses on the Internet was found to host an SSH server - roughly 16 million in total. Even more surprisingly to us, OpenSSH (37%) was no longer the most popular server software, but had been overtaken by Dropbear (58%), a low-footprint, open-source implementation that is popular in embedded systems and home routers. Other implementations accounted for less than 5% of all servers we found in our scan.

Digging deeper into the data, we looked at the servers' preferred encryption modes. Looking at the number of preferences across all the servers, we found 199 different modes. While Dropbear did not exhibit much diversity -- mostly a mix of CBC mode and CTR mode encryption in combination with HMAC-SHA1 -- OpenSSH did, with a mix of old and new encryption schemes, including a smattering of AES-GCM, a small amount of ChaCha20-Poly1305 (the default algorithm since version 6.9), and various instantiations of an "Encrypt-then-MAC" construction of whose existence we were not previously aware (but which was introduced to OpenSSH in version 6.2, released in 2013).

Having sampled this landscape, we decided to try to evaluate the security of the most popular encryption options for SSH.

We began by looking more closely at CBC mode. As early as 2008, two of us (Martin and Kenny) working with Gaven Watson had discovered a vulnerability in the CBC mode specification in SSH which would allow a determined attacker to carry out a plaintext recovery attack. We knew that a patch had been put in place in the OpenSSH implementation to prevent our 2008 attack, but we did not know how widely it had been taken up, and we did not know whether other implementations had adopted it or implemented their own countermeasures.

When we started to look more closely at the source code, we found a number of problems with the patch, leading to new timing attacks on the OpenSSH implementation: the patch prevented our original 2008 attack, but not variants of it. Here we were informed by all the work we had done in the intervening years on finding vulnerabilities in the SSL/TLS protocol. Fortunately, CBC mode has been disabled by default for some time in OpenSSH, though we found a long tail of older versions in our scan that were potentially vulnerable to attack. Worse, we found that Dropbear had done nothing to prevent the 2008 attack except for implementing CTR mode and making it the default algorithm, leaving users who continued to use CBC mode open to attack.
We responsibly disclosed the issues that we had found in OpenSSH to the development team, and they patched against our new attacks in OpenSSH versions 7.3 and 7.5. The reason that two sets of patches were needed is complex, and points to the extreme fragility of CBC mode in the context of the SSH protocol.

In parallel with developing new attacks, we tried to provide formal security proofs for the other encryption modes commonly available in SSH. To do this, we started with a security model that was developed in a 2012 paper by Jean Paul and Kenny, working with Sasha Boldyreva and Martijn Stam (BDPS). This model was built for the specific purpose of analysing protocols like SSH that handle decryption in a "fragmented" manner: pieces of a longer ciphertext can arrive in small fragments, one per TCP segment, and are decrypted in an online fashion as they arrive. Such processing opens up new attack opportunities, as exploited in our 2008 paper in which we analysed CBC mode.

The BDPS model only considers confidentiality, so we extended it to also handle integrity. In making this extension, we found a bug in the original BDPS model: because of a subtle definitional issue, the model would declare *all* encryption schemes to be insecure! Needless to say, this made the definition quite useless, but also highlights the complexity and subtlety involved in getting to the right definitions for encryption notions when going beyond the standard ones.

Armed with repaired and extended definitions, we then set about proving the security of AES-GCM, ChaCha20-Poly1305, and the Encrypt-then-MAC construction that we found in OpenSSH. (CTR mode was already treated in a 2010 paper by Kenny and Gaven Watson.) These modes are all quite easy to analyse in the "standard" setting for symmetric encryption using Authenticated Encryption security notions, but the fragmented setting presented by SSH makes the proofs much more challenging to construct.

Along the way, we found a subtle bug in the OpenSSH implementation of the decryption step for Encrypt-then-MAC: although the MAC was properly computed on the received ciphertext, the computed MAC value was not compared to the received MAC value until after decryption had been performed. This meant that decryption was being carried out on unauthenticated data, partly negating the protection afforded by the MAC.
Fortunately, this did not lead to any concrete attack, and was swiftly patched by the OpenSSH team after we disclosed the bug to them.

At the end of our work, we drew the following key conclusions:

-- The SSH deployment landscape is complex and diverse.
-- CBC mode encryption in SSH is dangerous and should be avoided.
-- With this exception, the encryption modes used in SSH are sound, assuming the underlying cryptographic components (such as block ciphers and pseudorandom functions) are secure.
-- The "surfeit" of SSH cipher suites is probably excessive, taking the idea of achieving robustness through cryptographic algorithm diversity too far.

Looking ahead, we are now examining the performance impact of more advanced encryption modes for SSH. These offer even stronger security properties, like prevention of certain types of Denial-of-Service and traffic analysis attacks. Our early results suggest that these stronger properties can be achieved at modest cost in terms of computation and bandwidth overhead. We are currently working on a robust performance study and the integration of our prototypes with the OpenSSH codebase.

In closing, it's worth noting that our research was sparked by the impact agenda promoted by HEFCE, the Higher Education Funding Council for England (aka, our academic paymasters). In 2021, HEFCE will run an exercise to evaluate all the research being carried out in UK universities, with research impact being a significant factor in the evaluation. As preparation for that exercise, we wanted to find out if our 2008 attack had had any real world impact. This was the reason for carrying out our initial measurement study: we wanted to find out if CBC mode was still popular or if it had been supplanted by other modes. We were surprised with what we found and quickly realised that more research could be done, and indeed was needed, to improve our confidence in SSH's use of cryptography.

Sometimes government policies concerning research do result in useful outcomes...

Read our research paper:
http://www.isg.rhul.ac.uk/~kp/surfeit.pdf

## THE WISDOM GROUP

**The WISDOM group was founded in 2016 by two PhD students – Sheila Cobourne and Thyla van der Merwe – with a vision to promote equality and diversity in the School of Mathematics and Information Security and to encourage more women into the field. WISDOM stands for Women in the Security Domain and / or Maths and was set up in response to the under-representation of females in the field - at all levels - from students to staff to professionals. Currently only 11% of professionals in Information Security are female (http://womenscyberjutsu.org/). Only 12.8% of the STEM workforce are women (WISE – Women in Science and Engineering). WISDOM seeks to address the balance and has a range of activities that help achieve the group's objectives. Regular meetings, conferences, and networking events are held to develop new staff and student networks but also to reach out across industry and academia. Younger students are encouraged to join and make new contacts with peers who are slightly further down the road than them. There are opportunities for WISDOM members to coach and mentor younger members and help them navigate their way through life. WISDOM educates on relevant subject areas including unconscious bias, imposter syndrome, promotes relevant training and runs leadership and development courses. The group aims to act as a safe space for people to speak out on equality and diversity issues and through awareness hopes to improve attitudes and organisational processes by being agents of positive change. Since creation, the group seems to be taking more ground, gaining more members and developing more momentum. Founder Sheila Cobourne comments: "Thyla and I were both involved with the Athena Swan committee, and regularly used to meet for coffee to talk about the issues that were raised in meetings. The idea for the WISDOM group grew out of this, and it has been inspiring to see how the group has gone from strength to strength since it started." Founder Thyla van der Merwe reports that: "In retrospect, it's surprising to me that a group like WISDOM didn't exist in the School of Mathematics and Information Security prior to 2016; raising the profile of women in the fields of Mathematics and Information Security is clearly something that a lot of people in the School care about. We've received a tremendous amount of support from the School leadership, as well as other School members - people of all genders seem to support our vision, showing that the apparent lack of diversity in our fields is indeed everybody's problem, and that many of us are open to tackling it." With the support of so many staff and students within the School it appears that WISDOM will continue to grow and help shape the context in which we study and work. There is much activity planned for the future, the group is soon to release a film about their work so far and have a regular blog on their website, visit: wisdom.rhul.ac.uk for further details.**

# CYBER SECURITY: EVOLUTION OR REVOLUTION?

Dr Geraint Price

> Lecturer, ISG

A few years back I wrote a piece for the ISG Review Newsletter entitled "Cyber Security: Plus ça Change". At the time cyber security was a relatively new term, and while there were things to consider that were different, I set out the opinion that not much has changed in the move from "information security" to "cyber security".

However, I have recently begun to wonder: do we need a more radical rethink of what is required from our research agenda?

In this article, I will set out why, since that original piece, I have slowly moved my stance to one of "revolution, not evolution" – at least for some of the issues we seek solutions for.

## We Don't Know What's Broken Until It Goes Bang

My previous article was written shortly after the ISG had started running the "Cyber Security Club" whose goal was to shed some light on all that was cyber security (a relatively new term at the time). At one of our early meetings, in setting out his view on cyber security, one of our speakers used the example of the de Havilland Comet within the context of cyber security. For those not familiar with it, the Comet was the first commercial aeroplane to use jet engines. After an early successful start, a number of Comets suffered catastrophic failure during flight. Initially, the crash investigators could not figure out the cause of the crashes. After a team carried out a scientific study where they submerged a full aircraft in a water tank repeatedly to simulate the change in pressure it experienced in flight, what they saw was metal fatigue around the windows. This led to a change in design for airplane windows where the radius of the curve at the corners of the window were made larger to spread the load of the strain which was put on the metal across a greater arc.

My reading of this event in relevance to our discussion here is as follows. While there had been commercial flight for many decades prior to the introduction of the Comet, the application of a new technology in terms of the jet engine resulted in a change in context and experience for the technology which the designers had not foreseen (i.e. the increased strain on the metal around the fuselage window). In this example, the scientific understanding of the metallurgy at work was insufficient to deal with the changing context.

How does this relate to cyber security? In my opinion, the work of the early pioneers in information security (much of which has its home in the 1970s) is now being applied to scenarios where our scientific understanding is insufficiently advanced to accurately, and predictably, understand the risks we are taking. In other words, we will not be able to anticipate which parts of our system will break until they announce that to us themselves.

## Other Examples Where Science Has Needed To Adapt In The Past

I will now draw on two other examples from the field of medicine to elaborate on this theme.

Ignaz Semmelweis was a Hungarian physician in mid-19th century. He noticed that the delivery ward run by doctors had a much higher incidence of mortality than the delivery ward which was run by midwives. He hypothesised that there was some form of delivery mechanism at play, where doctors (who had been carrying out autopsies in the morgue) would transfer the cause of the illness from the morgue to the maternity ward. As a result of his observation, he proposed a routine of hand washing with chlorinated lime solution prior to working on the delivery ward. However, the medical community of his day were sufficiently aloof to pour scorn on his ideas, and eventually Semmelweis died in a lunatic asylum. In a cruel twist, he had been sent to the asylum for his progressively heated disagreement with the established medical community of the time. It wasn't until Luis Pasteur confirmed the "germ theory" of infection that Semmelweis's suggested practice was widely adopted.

Moving forward to the 20th century, we have the example of Barry Marshall. Marshall was a researcher who had started to doubt the conventional wisdom of the time that stomach ulcers were caused by stress, spicy food, etc. He hypothesised that the cause of many ulcers was actually a bacterial infection. Again, many of his peers at the time disagreed with his claim. How was he to put his theory to the test? He decided to take the rather "brave" decision to ingest the bacterium which he thought was the cause of the ulcer (while I'm not certain, I believe that he did this as he couldn't have got ethical approval to deliberately infect a healthy subject other than himself). Upon taking the bacteria he duly developed a stomach ulcer which he successfully treated via a short course of antibiotics. Ultimately Marshall (and his collaborator Robin Warren) were awarded the Nobel Prize in 2005 for their work.

## So Why Are These Examples Relevant To Us Here?

In the case of Semmelweis, while he had a hypothesis which he could back up with circumstantial evidence, he couldn't provide direct scientific proof to back up his claim. In this case, the science itself was too immature to help.

In the case of Marshall, while he had a hypothesis, many in the field strongly disagreed with him. Therefore he needed to provide them with that direct scientific proof to disprove their theories. While science as a discipline can provide us with many life-changing advancements, we have to be careful not to accept all "perceived wisdom" without clear and unambiguous evidence to support those claims.

## Where Do We Go From Here?

So how do I propose we use these examples to help guide our future research? Ultimately, for some aspects of our discipline (e.g. cryptography, analysis of security protocols, etc.) we already have a firm grounding in the science of these disciplines. As such, those aspects of "cyber security" can continue to develop in an evolutionary manner (albeit with the salutary lessons of the Comet, Sammelweis and Marshall to remind us to retain a healthy dose of humility).

However, there are large parts of cyber security which are still inadequately understood by us. In these cases I believe that we need a more revolutionary approach. Why so? When all is said and done, many of the concepts which we are dealing with are social constructs (e.g. privacy, trust, safety, etc.). As a discipline, many previous attempts have struggled to articulate them in the mathematical and logical models which have underpinned our previous work. As such, I argue for a more revolutionary approach, where we further explore the possible contribution of models and methods which have their roots in other disciplines, particularly those from the social sciences.

This isn't only my view, and the work that has been carried out by the Research Institute in the Science of Cyber Security (RISCS – www.riscs.org.uk) over the past four years has started us down this path. However, I would argue that we need to be more positive and proactive in this approach. While these are nothing more than analogies brought in from other disciplines, I am a firm believer in looking outside one's own sphere of expertise to learn what you can from others.

## The ISG's Role In Shaping This Landscape

While the ISG has long been recognised for its leadership in the more traditional, technical aspects of security, we have also been developing our capability in these new avenues of research.

In particular, Prof Lizzie Coles-Kemp has cultivated an international reputation for leading innovative and ground-breaking projects in this arena.
There are also others across the college more broadly (from psychology, law and geography) which have been contributing to novel research in this area – some of whom have already written for the ISG's Newsletter in previous years.

I, along with others in the ISG, was involved in the CySeCa (Cyber Security Cartographies) project, led by Lizzie Coles-Kemp, which was part of the first wave of projects in the RISCS community. I am also chairing a Practitioner Panel for the second phase of work within the RISCS community. Our goal there is to collate the experience and requirements of those who face these problems as part of their work. This will then allow us to influence and tailor our research agenda to provide direct, relevant and usable research outputs.

Ultimately, I believe that the ISG is ideally placed to continue providing innovative and applicable research – of both the evolutionary and revolutionary varieties.

# CDT UPDATE

Prof. Carlos Cid

> Director of the CDT in Cyber Security

November 2016 saw the launch of the new National Cyber Security Strategy, which was announced by the Chancellor of the Exchequer, Philip Hammond MP, during the Future Decoded conference in London. The five-year strategy will see an investment of £1.9 billion into defending UK cyber systems and infrastructure, deterring adversaries, and developing national cyber security capacity. One of the highlights of the new strategy was the creation of the National Cyber Security Centre (NCSC) as the single, central body for cyber security at a national level.

The strategy also brought excellent news for Royal Holloway's CDT in Cyber Security: it confirmed the renewal of funding for our CDT, with a new grant of £3.45M to provide funding for three further cohorts of PhD students in cyber security. The new strategy also carried several other initiatives for promoting cyber security science and technology in the UK, such as the continuing funding of the Centres of Excellence in Cyber Security Research (ACE-CSR) and Cyber Security Research Institutes, confirming the long-term commitment of the government to supporting the UK's cyber security academic sector.

The renewal of the CDT in Cyber Security also reaffirms Royal Holloway's pivotal position as a national centre for cyber security education and research. The Information Security Group is one of the largest academic cyber security research groups in the world. Royal Holloway was one of the first academic institutions in the country to be recognised as an ACE-CSR. Its highly successful MSc in Information Security programme was one of only four to gain full GCHQ certification in 2014, and now has well over 4,000 alumni around the world.

The CDT is now in its fourth year, and we have for the first time a full house: 37 CDT students divided into four cohorts, working on topics ranging from embedded security to cybercrime, from cryptography to geopolitics of security, from software security to cyber economics.
In September 2016, we welcomed eight new students as part of the 2016 CDT cohort. They are approaching the end of the first-year CDT training programme, and getting ready for their summer projects.
Students from the first three cohorts are likewise busy with their research, industrial placements and extra-curricular activities.
The research output produced by the CDT continues to be outstanding, both in quality and volume. CDT students had in the past year a number of peer-reviewed articles published and presented in international events, including a best paper award at CCS 2016, one of the world's top-ranked annual security conferences.

Engagement with industry is a key component of the CDT programme, and our students have spent time during their summer internships visiting CDT industrial partners in the UK and overseas, including NXP Semiconductors, Vasco Data Security, Cloudflare and L-3 TRL. Finally, students have shown their initiative and leadership in a number of extra-curricular activities: CDT students have been playing an active role in the formation and running of the WISDOM group, which aims to encourage diversity in the department; and together with students from Oxford's CDT, they are organising the third inter-CDT workshop, with the theme "Crypto Wars 2.0", to explore the ongoing public debate around encryption and secure communication.

Royal Holloway has been producing PhDs in cyber security for over 30 years, with many of its PhD graduates occupying senior cyber security roles in academia and industry.
The launch of the CDT in 2013 has however provided a significant boost to our doctoral-level training and research programmes. It has given us the opportunity to attract and recruit excellent students to join our annual cohorts of PhD students, to work on a wide range of cyber security topics. As anyone attending one of our CDT events can attest, Royal Holloway has today one of the most vibrant and productive post-graduate environments in cyber security in the UK, and this is something that we all – CDT/ISG students and staff – can be very proud of.

# THE ALL PARTY PARLIAMENTARY GROUP IN CYBER SECURITY

**Dear Readers,**

**As a Member of Parliament, I am acutely aware of the importance of Cyber Security to the safety and security of UK citizens and the nation as a whole. When I first became enthusiastic about the proposed APPG in Cyber Security, I was motivated to help inform busy parliamentarians about vital cyber security issues and to stimulate cross party debate in this area. The need for this is all too evident with a plethora of incidents and news stories attributed to criminals, terrorist and nation states. The formally stated objectives of the APPG are as follows:**

**"The purpose of the All-Party Parliamentary Group (APPG) on Cyber Security is to raise awareness in Parliament of issues relating to Cyber Security by providing a forum for briefings, debate and discussion. The group will address developments in Cyber Security systems and techniques affecting consumers, businesses (including small business) and the role of cyber security in the smooth working of Defence, the UK economy and society as well as the Critical National Infrastructure. The group activity will be applicable to, security, identity, regulation and fraud, and it will provide information that promotes inclusion and understanding for non-specialists."**

**My fellow officers of the APPG include, the Secretary, Steven Paterson MP, Admiral the Rt Hon Lord West of Spithead GCB DSC PC ADC DUniv, the Rt Hon Lord Arbuthnot of Edrom; with Professor Keith Mayes and Andrew Henderson representing the ISG as secretariat.**

**Our discussions so far have been extremely stimulating and centred on the security of the Internet of Things, critical infrastructure security, and how hackers can stalk individuals. At the time of writing there are scheduled events to discuss fake news and transport system security.**

**Government clearly has a role in tackling cyber security threats and plain speaking explanations of the technical issues are of great help to non-specialist parliamentarians when considering how to shape future policies in this area.**

**As Chairman of the APPG I am grateful to the ISG for its on-going expert input and support for the secretariat, and I wish the ISG well for the coming year.**

**Yours Sincerely**
**Flick Drummond MP**
**APPG chair and Member of Parliament for Portsmouth South**

# ANOTHER EXCITING YEAR FOR THE SMART CARD CENTRE (SCC)

## Prof. Konstantinos Markantonakis

**> Director of the ISG Smart Card and Internet of Things Security Centre (SCC)**

The ISG SCC continues to push the boundaries of research and teaching in the fields of smart cards, tokens, Internet-of-Things and their associated application and security challenges. In the last academic year, we supervised more than 20 MSc projects in related topics. In fact, the MSc project "Evaluation of Apple iDevice Sensors as a Potential Relay Attack Countermeasure for Apple Pay" by Gareth Haken and supervised by the SCC won the David Lindsay Prize, awarded every year by the British Computer Society's Information Security Specialist Group to the project that best addresses innovative applications of Information Security. This project also resulted in a conference publication in the 3rd ACM Cyber-Physical System Security Workshop (ACM CPSS'17)[1]. This project adds to the relatively long list of MSc projects supervised by the SCC resulting in conference papers, which demonstrates the hard work of our MSc students. On the teaching front, our campus and distance-learning versions of the optional MSc module of "Smart cards, tokens, security and applications" have been updated to reflect recent advances in IoTs security. Our teaching efforts continue to cover information security undergraduate modules in the Computer Science department.

In July 2016, we reached the end of the 30 months of the Secure Avionic Wireless Networks (SHAWN) project funded by the Technology Strategy Board (TSB) and EPSRC. The project partners included General Electric (GE) Avionics, Critical Software, HW Communications and the University of Strathclyde. The ISG SCC acted as the information security authority responsible for providing a secure and reliable security assessment on the various project proposals. Dr Raja Naeem Akram's contribution in the project resulted, among others, in five papers being published in international conferences.

This research thread has also strengthened our existing collaboration and publication efforts with past visiting researchers of the SCC, including Damien Sauveron from the University of Limoges, and with the University of Bordeaux, leading to further papers, in key avionics conferences, on Drone security and Unmanned Aerial Vehicle (UAV) platforms. This resulted in two accepted papers in the 2017 Integrated Communications Navigation and Surveillance (ICNS) conference. Two more collaborative papers are currently under review.

In September 2016, we started a new three-year EPSRC project on "Improving customer experience while ensuring data privacy for intelligent mobility", referred to as DICE. This is a joint effort between the Universities of Surrey, Southampton, Loughborough and ourselves. Dr Raja Naeem Akram is the named RA and he will be providing his expertise on data provenance and anonymity.

We also celebrated the successful completion of two PhD students supervised by Prof Markantonakis in the SCC. Dr Sarah Abu Ghazalah completed her PhD viva in October 2016. In the course of her PhD studies, Sarah extended the expertise of the SCC in the fields of low-cost authentication protocols for RFID tokens by identifying weaknesses and improvements in existing protocols, implementing her proposals in real RFID tokens and verifying the correctness of the proposed protocols using automated verification tools. Sarah's contribution resulted in eight papers in international conferences and journals. Dr Hafizah Bin Mansor completed her PhD viva in March 2017. Hafizah's work on automotive security and firmware updates for automotive sensors has helped the SCC to expand our activities in a domain with real world significance, where information security is of paramount importance. Hafizah's work resulted in five papers published in international conferences and journals. She went a step further by implementing her proposals in real sensors used by the automotive industry and experimenting with performance measurements in her own build CANBUS network prior to also verifying her proposals using automated verification tools. Both colleagues worked very hard in completing their studies, and taking into account that they also had a family to care for, they deserve plenty of congratulations. Well done!

Our research on investigating the effectiveness and reliability of ambient sensors as anti-relay mechanisms for mobile phone-based point-of-sales payments was mainly through the work

of our PhD students Iakovos Gurulian, Carlton Shepherd (funded by the CDT) and Dr Raja Naeem Akram. This is accepted for publication in the Mobile Security Technologies (MoST) 2017 which is held in conjunction with the IEEE Symposium on Security and Privacy[2]. This work has also enabled us to collaborate with colleagues from the University Waikato in New Zealand, for the analysis of the results using their well-established WEKA tool. There are two more related papers under conference review.

Our PhD students are also busy, with at least 12 papers being published in well-respected international conferences and journals. We have to congratulate all the ISG SCC PhD students not only for their hard work in research areas with real world practical significance, commitment and professionalism, but also for their team spirit and companionship. The ISG SCC is constantly looking for strong PhD students, so if you are interested to discuss PhD opportunities please do not hesitate to get in touch.

The SCC staff/PhD research activity has generated more than 160 published papers in international conferences and journals with more than 15 papers in 2016 (www.scc.rhul.ac.uk/publications.php). It is worth noting that the second edition of our "Smart Cards, Tokens, Security and Applications" book is due to be published by Springer in the summer of 2017.

The ISG SCC welcomes Dr Daniele Sgandurra, our newly appointed lecturer in the ISG, affiliated with the SCC, currently located in the refurbished SCC equipment lab in the founders building. Dr Sgandurra's expertise will strengthen further the SCC's strategic research and teaching expansion in the fields of IoTs.

It is well known that the ISG SCC's activities would not have been possible without the endorsement and membership of our sponsors. In recognition of our long-standing links with the transport industry, the SCC is delighted to announce that Transport for London and ITSO have extended their support to the SCC. Furthermore, the UK Cards Association has also extended their support for another year. However, we look forward in establishing further collaborations with additional partners, in order to expand the real world significance of the SCC's research. We welcome any such opportunities for collaboration and memberships so please feel free to contact me.

In June 2016, the SCC led the organisation of our 5th Information Security Group (ISG) Alumni Conference and the 1st ISG Open Day. These events highlighted the breadth of the ISG research and teaching activities, along with highlighting the interdisciplinary information security research of the ISG.

On 30th August 2017, we will be celebrating our 15th anniversary by hosting the well-established ISG SCC Open Day with the usual mixture of industrial exhibitors, MSc and PhD students demonstrating the results of their MSc projects and research respectively. Note this date in your calendars, as we look forward to welcome you at this event.

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

References


[1] Gareth Haken, Konstantinos Markantonakis, Iakovos Gurulian, Raja Naeem Akram and Carlton Shepherd, " Evaluation of Apple iDevice Sensors as a Potential Relay Attack Countermeasure for Apple Pay", ACM CPSS'17 Program, 3nd ACM Cyber-Physical System Security Workshop, Abu Dhabi, UAE, April 2, 2017: (in conjunction with ACM AsiaCCS'17)

[2] Shepherd, C., Gurulian, I., Frank, E., Markantonakis, K., Akram, R., Mayes, K. & Panaousis, E. 25 May 2017, "The Applicability of Ambient Sensors as Proximity Evidence for NFC Transactions", IEEE Mobile Security Technologies (MOST) 2017 - San Jose, United States

## WHY DIVERSITY MATTERS IN INFORMATION SECURITY

Prof. Lizzie Coles-Kemp

**> Professor, ISG**

Diversity across science, technology, engineering and mathematics (STEM) subjects is regarded as an important topic not only by those who are dis-benefited by the current STEM career and education programmes but also by policy makers, industrialists and educationalists. Its importance is reflected in its prominence in education policies across the entire education sector. The ISG is often drawn into this debate partly because information security is often regarded as a STEM subject and also because of its role in supplying graduates to join the STEM workforce.

The School of Mathematics and Information Security is home to the WISDOM (Women In the Security Domain and/or Mathematics) group. This group provides an important platform through which the diversity initiatives can be discussed and developed. The group also helps us to respond to the fact that the Information Security MSc has a minority of female students that consistently represents only 20% of each student cohort.

However, when discussed at national policy level, diversity is a term that not only relates to gender but also embraces ethnic, ability and socio-economic diversity. I would argue that to respond to real-world security problems, we need to broaden this conceptualization still further. For example, let's consider my own minority status. Superficially, as we can see from the figures above, it could be argued that I am in a minority being a female. However, I would argue that is only part of what makes me a minority in information security. I am a female who completed her education with almost no mathematics in her background, who spent part of her tertiary education in the Scandinavian system with a focus on consensus and collaborative working and whose upbringing and formative experiences engendered a strong belief in the importance of social justice and equality for the economic well-being of a society. By not having a background in mathematics or the mathematical sciences has always put me in a minority whether in practice or in academia because my thinking and my methods of abstraction are different to the majority in the domain who have an engineering or mathematical science background.
By being exposed to different ways of thinking about social strength and societal well-being, my understanding of security is perhaps a little different to the more traditional Anglo-Saxon focus on individualism and the power of the economic markets. This difference in perspective has often helped to make a positive contribution to finding creative responses to real-world security problems.

This position augments the more typical argument for diversity in STEM. In 2014 The Campaign for Science and Engineering (CaSE) published a report titled "Improving Diversity in STEM". The report featured with the statement that "A more diverse science, technology, engineering and mathematics (STEM) workforce is not simply desirable in terms of equality, but necessary if we are to maximise individual opportunity and meet economic need."
The report presents a number of barriers to diversity in STEM. These barriers range from challenges in promoting diversity in STEM at school age to managing the gap between supply and demand of skilled STEM workers. In the ISG's case support for and the promotion of the WISDOM group as well as the on-going contribution that the ISG makes towards the gaining of the Athena SWAN equality award are direct responses to these barriers.

The ISG's focus on interdisciplinary working that embraces the social sciences and the humanities offers an important route to improving the diversity of information security. In gender terms alone, interdisciplinary working is an important route to diversifying the information security population. The majority of UK-based information security academics will apply for funding to the Engineering and Physical Sciences Research Council.
The Research Councils reported in 2016 using their own data and data from the Higher Education Statistics Agency (HESA) that the academic population of the engineering and physical sciences is circa 17,000 comprising 16% women and 84% men. In the student population, the number of female students is circa 25% with 75% male. This contrasts with the picture reported for the Economic and Social Research Council (ESRC). Here the data currently show that the academic population is somewhat larger – circa 30,000 but the gender composition is strikingly different with females being the larger group in some measurements, for example studentships. Studies in the sociology of technology have shown that the focus of study and analysis is closely linked to the diversity of the communities working in a particular domain. In the engineering and physical science approach, the focus of analysis in an information security problem is typically information or the technical infrastructure related to the generation, circulation or curation of that information. In contrast, following a social science or humanities approach the focus of analysis would often be the individual, the state or society. With the diversification in focus of analysis, multiple perspectives are introduced, a richer range of problem solving techniques is developed and the resonance with a wider student population encouraged. Promoting diversity at such a fundamental level is essential for the continuing relevance of our field both as a practice and as an area of study. Our goal, in my view, therefore must be a research and practice community that can be regarded as multi-cultural by a broad range of measures and that is comfortable in its own diversity.

Biog: Lizzie Coles-Kemp is a Professor of Information Security who worked in information security practice for 18 years prior to joining the ISG to teach and research social and organisational aspects of information security.

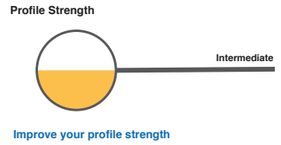


## GAMING... SERIOUSLY?

Andreas Haggman

**> Third-year PhD student in the CDT in Cyber Security**

**The idea of play is something many people abandon after childhood. If the word "sandbox" conjures up images of virtual machines you are probably one of these people (and should therefore read on!). Beginning with Johan Huizinga's 1938 treatise Homo Ludens, much research has demonstrated the power of playing and games beyond the playground, leading to a meteoric rise of the concepts of gamification and serious games.**




### Gamification

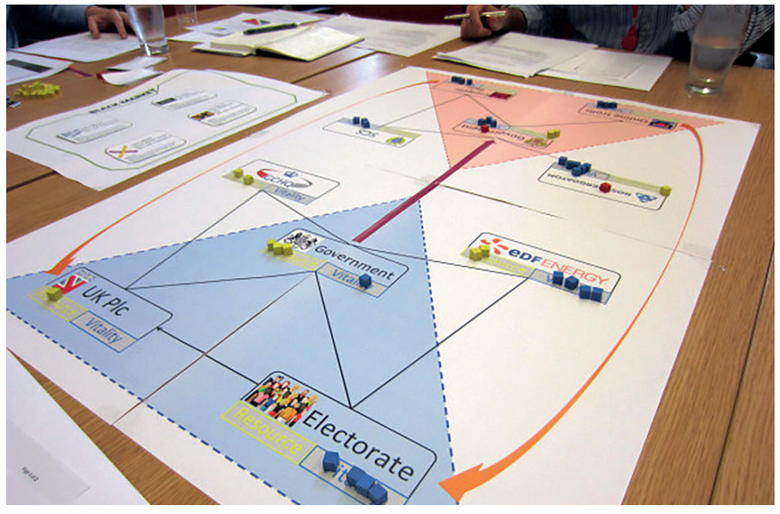
**If you have ever restocked your fridge, flown overseas, or created a social media profile chances are you will have experienced gamification. Tesco, and other supermarkets, offer shoppers Points (all of which, we are told, "add up!") just for completing the mundane weekly shop. Airlines dish out Frequent Flier miles which customers can spend on future flights. LinkedIn assesses how complete your online profile is and gives you a ranking from Beginner to All-Star. These are but a few examples of the myriad organisations that have implemented gamification for marketing and customer retention.**

**The basic idea is to set targets for customers to strive towards and administer rewards for successfully reaching milestones. The gratifying nature of this system will be readily identifiable by any videogame player who has received an "Achievement Unlocked" or "Trophy Earned" notification. If implemented subtly, these gratification systems are potentially even more powerful as people do not consciously recognise their presence, but simply feed into the playful human nature. At its core, gamification is a method of positive reinforcement that shapes "player" behaviour in a desired way. The key difference, of course, is that in partaking in these activities (shopping, flying etc.) we are not consciously playing games, but merely going about our lives.**

### Serious games

**In much less nefarious ways, the serious games initiative seeks to harness many of these same concepts but for overt training and education purposes. Serious games are either adapted from existing games or built from scratch to address some pedagogical need. The games may forego the gratification mechanisms described above in favour of high-fidelity simulations where players can experience an activity in a way that closely resembles real life and thereby derive explicit lessons for real-life behaviour. Technology has played a particularly important role in serious games, because the higher fidelity a simulation achieves the more direct the lessons are that can be learnt. Developments like virtual and augmented reality will prove pivotal in coming years, providing users with extremely engaging and interactive experiences.**

**Although the military has been particularly pioneering of such simulations, serious games have been made for a whole gamut of military and civilian uses, including urban infantry combat tactics, treatment for sufferers of post-traumatic stress disorder, repairing industrial equipment, predicting financial markets, and any number of cockpit-type experiences from piloting fighter jets to driving ambulances. The list goes on.**



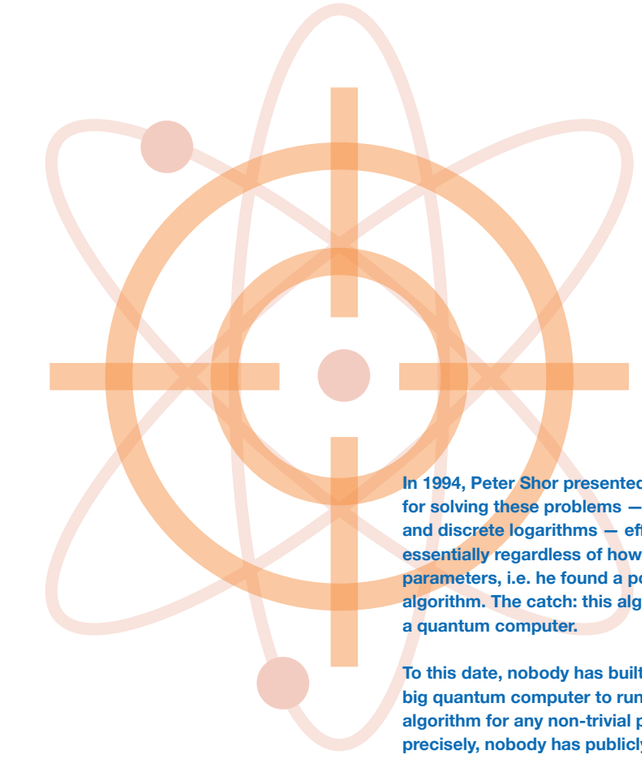

### Wargaming

**That the military led the way in the use of games is perhaps less surprising when we consider that a particular subset of games had been used for centuries to shape minds and behaviours. The roots of wargaming can be traced back some 5000 years to ancient games like Wei Hai (literally "encirclement", a precursor to Go) in China and Chaturanga (a precursor to chess) in India, which were used to teach aspiring military commanders about strategy and tactics. Modern wargaming, however, was really pioneered in 18th and 19th century pre-unification Germany, where it was wholeheartedly adopted by the general staff. The success of the German military in ensuing conflicts can be partly attributed to this.**

**Simply defined, wargaming is an activity that at some level of abstraction seeks to model and simulate conflict. Over the past 200 years wargaming has been used by militaries around the globe to understand events of the past, plan operations and organisations, and explore envisaged futures. In the past few decades, wargaming has also entered the civilian commercial world, with companies recognising the potential of using these tools and methods to achieve cost savings and realise business growth. However, despite this widespread popularity, few serious, and even fewer good, attempts have been made to apply these ideas to the cyber domain. The importance of cyberspace as a communications and commerce medium is firmly entrenched, and concepts around cyber warfare feature heavily in modern military thinking, yet little work has been done (at least in the public domain) to wargame cyber.**

**My own work in the Centre for Doctoral Training in Cyber Security in the ISG seeks to ameliorate this situation. I have developed a wargame based on the UK National Cyber Security Strategy for the purpose of cyber security education and awareness training, primarily for senior policy- and decision-makers. The game is currently being deployed to as many organisations as possible to ascertain its pedagogic value.**

**With games and gamification now being widely appreciated for serious uses beyond jovial childhood pastimes there is great appetite to explore these methods in a variety of settings. Just as building sandcastles can be formative to early personal development, so can applications of playful ideas be leveraged to grow knowledge and foster understanding in more adult environments, including cyber security. "Games," said Benjamin Franklin, "lubricate the body and mind." He was definitely on to something.**



## POST-QUANTUM
Dr Martin R. Albrecht

> Lecturer, ISG

Typically, secure electronic communication involves the following steps. Alice and Bob use a cryptographic key-exchange protocol like Diffie-Hellman (or a key encapsulation mechanism based on RSA) to agree on a common encryption key and then use this shared key to encrypt and authenticate their messages. To secure this sort of scheme against person-in-the-middle attacks, they would use digital signatures like ECDSA or RSA-PSS. This sort of approach is used in TLS, SSH, IPsec, Signal, etc.

The key exchange, key encapsulation and digital signature parts of these schemes rely on the difficulty of either factoring — given $N=p.q$ for $p$ and $q$ prime, it is hard to find $p$ or $q$ — or on the difficulty of computing discrete logarithms in some finite group, e.g. modulo a large prime $p$ – given $g^a$ and $g$ it is hard to find $a$.
By "difficult" or "hard" we mean that the cost for an attacker grows much more than the cost of a user, as we increase parameter sizes.

In 1994, Peter Shor presented an algorithm for solving these problems — factoring and discrete logarithms — efficiently, essentially regardless of how big we choose parameters, i.e. he found a polynomial-time algorithm. The catch: this algorithm runs on a quantum computer.

To this date, nobody has built a sufficiently big quantum computer to run Shor's algorithm for any non-trivial problem (more precisely, nobody has publicly announced it) and it remains unclear if it is at all possible. Note that D-Wave's machines are not quantum computers in the sense required here. Still, recent theoretical and practical progress in the area of quantum computing has many people worried. One motivation is the following scenario: an attacker could collect encrypted traffic now and store it until sufficiently big quantum computers are available. Once this is the case, it can use their capabilities to decrypt the stored ciphertexts. Thus, if encryption ought to provide security well into the future, it might be under threat already by quantum computers… even if they do not exist yet.

From ETSI to NIST and throughout the cryptographic community efforts are underway to design, analyse and standardise algorithms which are secure in the post-quantum era, i.e. post-quantum cryptography (PQC) also known as quantum-safe cryptography (QSC). At its heart, this is a quest for mathematical problems which allows similar functionality to discrete logarithms or factoring, while still being secure against quantum computers.

An example of such a problem is the approximate GCD problem. Consider the factoring problem mentioned above: given $N=p.q$ find $p$ or $q$. Now, assume we are given many $N_i = q_i . p$ where $p$ stays the same but $q_i$ changes each time. In this setting, finding $p$ is easy, i.e. there is a polynomial-time algorithm even on classical computers: $\gcd (N_1, N_2)$ is efficient and will return $p$ with good probability. This fact has indeed been exploited in attacks against RSA implementations which use bad randomness to sample their $p$ and $q$. For example, embedded devices that create keys when booting up for the first time might have limited entropy available.

However, if we just modify the problem slightly to obtain $N_i = q_i . p + r_i$ where $r_i < p$ are small-ish integers, then this problem can be shown to be as hard as solving the Shortest Vector Problem (SVP) on arbitrary lattices. This is a roundabout way of saying that it is believed to be hard even on a quantum computer. If we pick parameters right, that is.

However, picking parameters right is not so easy. Just as we base the recommended size of RSA keys on the best known attacks, we would pick parameters for post-quantum algorithms on the best attacks against post-quantum schemes. Yet, post-quantum algorithms such as the approximate GCD problem have not been studied for as long as, say, RSA. As a consequence, researchers in the Information Security Group and elsewhere are investigating algorithms for breaking these post-quantum schemes to guide us towards secure parameter choices which resist all known attacks.

In terms of performance, post-quantum cryptography is not doing too badly. Many proposed schemes are faster than RSA or even elliptic curve cryptography for similar security levels. On the other hand, post-quantum schemes tend to require larger public keys and larger ciphertexts, i.e. to send a short message securely more bytes need to be sent on the wire. Reducing these sizes is hence another focus area for post-quantum cryptographic research.

PS: Post-quantum cryptography is something rather different to quantum cryptography such as quantum key distribution (QKD), which uses quantum mechanics to establish secure keying material between two parties. However, firstly, QKD only covers short distances so that trusted relays are needed to bridge larger distances, invalidating end-to-end security claims. Secondly, QKD, too, is subject to person-in-the-middle attacks. To prevent such attacks (in the absence of digital signature algorithms), the two parties need to have some common secret to authenticate the data they are sending. But if we have a common secret, we can use symmetric cryptography. Thus, in practice, QKD is much closer to a short-distance symmetric encryption scheme where a common key is used to encrypt and authenticate messages between parties than to public-key cryptography. However, symmetric cryptography such as hash functions or AES are currently not threatened by quantum computers (but we will need to increase parameters somewhat).



## CYBER SECURITY DEMANDS MORE THAN BLAMING THE VICTIM
Robert Carolina

> Senior Visiting Fellow, ISG

Cyber security professionals are increasingly interested in end users, and understandably so. Decades of investment in security technologies often leads us to perceive the end user as the weakest link in the security chain.

While this renewed focus on the human element is generally positive, it can sometimes lead to something negative: blaming the end user. Placing 100% of blame for security failure, and by extension 100% of responsibility, on the end user could subvert the cause of security and reduce or destroy trust in cyber infrastructure.

I've recently noticed a growing trend where people in positions of influence and authority asked about security failings answer with special scrutiny to poor end user behaviour. Their comments often start with a true technological observation. For example, many security incidents and attendant frauds could be avoided if only consumer end users would take a better approach to updating and patching their software.

The frustration expressed by the professionals making these observations is palpable. And the harm caused is real. Consider a 2016 report from the UK Office for National Statistics. The ONS estimated that during a single 12-month period in England and Wales there were approximately 1 million incidents of cyber-enabled fraud that caused a loss between £1 and £1,000. While additional incidents produced larger losses, it is staggering to see how cyber-enabled criminals have been harvesting money from the "long tail" of small cons that have become cost-effective using the Internet.

Many security failures could be avoided if end users behaved differently.

The problem, however, arises when deciding how to encourage "better" cyber behaviour.

Last year Sir Bernard Hogan-Howe, the then-head of the Metropolitan Police, suggested in an interview that banks should limit or eliminate compensation to customers when poor cyber hygiene was a cause of the financial loss. Although Sir Bernard's comments drew an immediate firestorm of protest from consumer protection groups, he is not alone. I continue to hear suggestions that end users who fail to follow what technology experts believe is good practice should have compensation for incidents reduced or eliminated.

Unfortunately, evidence suggests that these sorts of proposals, presumably intended to frighten people into better behaviour, are unlikely to achieve that result. End users continue to make security mistakes, even when they are threatened with financial or other punishments for poor behaviours.

The evidence from behavioural science suggests that fear and pejorative approaches to changing end user behaviour are only useful when people feel fully in control of their behaviours and fully understand exactly how to stay safe and protect themselves. Unfortunately, this is precisely the opposite of how most users feel when they engage with online systems. As businesses and governments have responded to demand for online services, and then encouraged or demanded that customers move their interactions online, we face a growing universe of people who use online systems without any significant appreciation of the risks produced by their behaviour. These users do not naturally sense the effect that their behaviour may cause.

An audience member at the NCSC's CYBERUK17 event in March brought the problem into focus with an intriguing question. Four decades ago a simple public awareness campaign increased automobile safety behaviour by encouraging drivers to wear seat belts. The audience member asked what similarly simple message can we give to end users today that will make them safer online?

Although the expert panel provided a variety of interesting responses, I believe that the larger truth is also a sadder truth – no such simple message exists today. Forty years ago, drivers were told that wearing a single piece of reinforced nylon could save their lives. The device was simple. It had only one button. That button had only one function. Drivers could take control of their personal safety by clicking the belt. They could exercise control over their environment by buckling up. This is the type of simplicity that empowers users and changes behaviours. It is the type of simplicity that currently does not exist in cyber environments. One panel member seemed to acknowledge this as he observed that end users do not have sufficiently simple choices because using an online environment is still far too complicated a series of tasks.

Arguing that banks should reduce or eliminate compensation for many victims of cyber enabled fraud merely compounds this problem in two ways.

First, any effort to use the new policy to create a fear-based message is unlikely to produce better behaviour for the reasons outlined above. Second, and in my opinion equally troubling, consider for a moment what causes most consumers today to have faith in ecommerce as we know it. The average consumer has no significant understanding of cryptography or PKI. They don't understand the role of a certificate and when it is appropriate to trust one. They don't know the difference between a buffer overflow and a man-in-the-middle attack.

Why do consumers continue to offer up their credit card details to web sites using a complex online infrastructure that they barely comprehend? I suggest the simple answer is the implicit or explicit financial guarantee provided by today's credit card system. For many decades, the card industry has provided assurance to buyers and sellers that neither side would lose out significantly due to card fraud. This insurance model created the trust that all parties needed to conduct business with strangers at a distance. The model also puts the responsibility for many fraud losses on the party with the most cyber expertise who is normally the least cost avoider: the banks.

Of course, banks have a perfectly justifiable expectation that end users should act "reasonably" with their identity credentials. But the complexity of today's online environment challenges most end users to understand what they should do. There is no single "keep me safe" button on their computer that will reduce risk of fraud by 95%.

If banks eliminate compensation for fraud where end user behaviours are deemed somehow "less than good", but not so bad as to be "obviously negligent", it could undermine one of the foundations of trust that makes ecommerce today a success.

People who are not technology specialists remain broadly confused by a blinding array of cyber security measures and countermeasures. The rapid pace of change in our cyber environment adds to the confusion. Placing significantly more responsibility onto the end users of this system diverts our attention from the accompanying solution that can enhance security – the cyber equivalent of an end user "seat belt".

# HOW RATIONAL ARE INFORMATION SECURITY PROFESSIONALS AS DECISION-MAKERS?


Prof. Keith Martin &
Dr Konstantinos Mersinas

> Professor, ISG
> Distance Learning Tutor, ISG


It is well-known that, as decision-makers, none of us are perfect. Behavioural economics research provides numerous examples which show people systematically deviate from the model of the "rational decision maker". Cognitive limitations, subjectivity and biases are three of the most important factors for this deviation. For example, we all tend to be loss averse, meaning that the fear of losing something is almost twice as powerful as the attraction of gaining something of similar value.

As human beings, it is thus unlikely that the decision making of information security professionals is free from bias. However, it is possible that information security professionals consider certain types of decision in a slightly different way to the general population. After all, information security professionals are trained to think about "bad things" happening and how to try to allay them. Might this make them better decision makers? Or might this in fact lead them to exaggerate certain risks and turn them into worse decision makers? We decided to investigate this issue.

## Why it matters

Decision making is an important aspect of many information security professional roles, particularly those relating to risk management. Traditionally, information security risk management methodologies, both qualitative and quantitative, have been developed under the assumption that decision makers have the cognitive capacity and appropriate risk attitude in order to make "optimal" decisions based on available data. It has also been assumed that decision makers approach problems objectively and that their decisions are not influenced by the way a problem is presented.

In a common and simplified setting for security investment, professionals have to assess risk and consequently decide on protective and corrective measures for treating this risk. Inevitably, judgement and subjective perceptions are to some extent inherent in this type of decision making. However, it is crucial to support such decision making in a way that, as best possible, "objectifies" the process. The goal of our research was thus to identify what biases were demonstrated by information security professionals when faced with certain types of decision, and whether these deviated from those of the general population.

## What we did

We recruited a group of information security professionals engaged in a range of different information security roles. We also recruited a group of Royal Holloway students not studying information security as a sample of the general population.

We then conducted a series of online experiments based on lotteries which required participants to indicate decision preferences. These lotteries typically featured a set of options which indicated amounts a participant could pay in order to avoid certain types of loss. These lotteries were in some sense a simulation of the types of decision an information security professional might have to make when considering a particular security investment in order to counter the risk of the occurrence of a security incident.

## What we found

Not surprisingly, information security professionals were shown to exhibit many of the same decision making biases as the general population. Perhaps this is a positive finding, since it shows that information security professionals are human! However there were several interesting findings which indicated that information security professionals do approach decision making in a slightly different way.

One was that information security professionals were shown to be better at minimizing expected losses. In other words, they were shown to be more adept than the general population at reducing overall risk. This is perhaps to be expected, as the consideration of what could be lost, and how to prevent loss, is very much ingrained in "security thinking".

However, information security professionals were also shown to be more ambiguity averse than the general population. In other words, professionals were inclined to become risk averse when faced with decisions about less clearly specified threats. Perhaps this is because of the responsibility felt by information security professionals for their role in protecting an organisation. They may be more willing than the average person to invest in protection against unknown threats just to "be on the safe side", and because they may themselves be blamed when unexpected bad things happen.

A number of other findings amongst the information professional participants are worthy of comment:

- Professionals reveal preferences over risk treatment actions: they prefer to reduce risk compared to transferring it or eliminating it.
- Professionals favour reduction of losses compared to reduction of the probabilities associated with these losses.
- Risk attitude of professionals significantly changed across experimental conditions which presented the same security investment problems in different ways, showing that information security professionals are subject to biases of framing.
- Professionals' preferences between security and operability are influenced by their specific job role. Interestingly those in management roles tended to prioritize security over operability, while those in more technical roles favoured operability over security.

## Implications

So how can the findings of this research be directed towards better support for information security professionals involved in decision-making, particularly about security investment decisions? We have the following recommendations.

Bias awareness. The first step towards objectifying decisions is to be aware of the existence of such biases. This aligns with the recommendation of ISO 27001 that "risk perception and risk attitude of involved parties, should be taken into consideration". Establishing awareness of how potential biases in decision making might arise is an important contribution towards this goal.

Expected value maximisation. We recommend that decision-makers could minimise unnecessary spending or avoid the insecurity of underspending if they use both maximisation of expected profits as well as minimization of expected losses as measures for evaluating risk-related investment choices. This approach might contain the tendencies of professionals towards loss-making ambiguity aversion. Note that these two approaches appear to have different effects on security spending. For example, our findings indicate that viewing information security as a positive contributor to the business appears (perhaps naturally) to increase willingness to invest in security measures.

Role-dependence. The role-dependent perception of security professionals in combination with insufficient communication during the decision-making process can lead to a misalignment of priorities and inevitably to disagreement over how to manage risk. Decision-makers and managers need to be able to identify these differences of perception when discussing security investments.

Framing considerations. Security problems, when examined in isolation, are likely to be subject to framing effects, which can distort issues and lead to subjective decision making. Diversification of security investment decisions due to framing effects is likely to be fairly common. Approaching decision making by considering a range of potential framing options might help to reduce this type of effect.

## Conclusion

Decision making in information security is not fundamentally different to decision making in any other area. It is thus subject to the normal biases exhibited by human beings in all walks of life. Nonetheless, our research has highlighted some aspects of information security professional decision making which seem to stray slightly from the norm. We have also highlighted aspects of such decision making which should be recognised and taken into consideration by organisations when making security investment decisions.

Full details about this research and its findings can be found in:


- Experimental Elicitation of Risk Behaviour amongst Information Security Professionals http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_mersinas.pdf
- Measuring Attitude towards Risk Treatment Actions amongst Information Security Professionals: an Experimental Approachhttp://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_22-5.pdf
- Are Information Security Professionals Expected Value Maximisers?: An Experimental and Survey-based Test J Cyber Secur (2016) 2 (1): 57-70. https://doi.org/10.1093/cybsec/tyw009



# ELECTRONIC ENGINEERING AT ROYAL HOLLOWAY


Prof. David M Howard

> Head of the Department of Electronic Engineering Royal Holloway


Royal Holloway, University of London, is opening a new Electronic Engineering Department which will admit its first students in September 2017. The key driver behind this initiative is the desire to encourage more women into engineering following in the footsteps of the College's founders, Thomas and Jane Holloway. The core ethos of the new department is the necessary role of creativity in modern engineering in the context of group working; students will engage in group project from the outset through years 1, 2 and 4, with their individual project being in year 3.

In today's world, the products of engineering are everywhere around us. The huge increase in data being recorded, stored both locally and remotely, accessed from (almost) anywhere on the planet raises all sorts of issues relating to, for example: privacy; security of access; security of integrity; ease of accessibility; protection of accessibility; compatibility with tomorrow's software developments; devices used to record the data and devices used to replay the data. The traditional boundaries between electronic engineering, computer science and information security have to be at least lowered and at best broken down such that these and other issues in relation to data can be studied "in the round".

Within the new syllabus for Electronic Engineering there is a module taught by the Information Security Group on information security which will provide a heads-up start within the field of data security for final year students. Since much of current electronic engineering practice involves the use of embedded systems that rely on software and data gathering for their control and operation, all issues in relation to how data is handled and how the code itself is protected become an essential part of the engineering specification that must be met for a successful product. Within the department of Electronic engineering there are also data security issues emerging within the research groups. One is concerned with the data available when Smart Meters are commonplace; potentially the information they capture could indicate when we are at home or using particular electrical appliances; in the wrong hands such knowledge could be used for inappropriate purposes. Within the music and audio group, the use of speech as a means of recognising the identity of someone is of interest in the context of natural developments in speech synthesis.

The world is a data driven place in which to live.

# VULNERABILITIES OF IOT DEVICES

Dr Daniele Sgandurra

> Lecturer, ISG

The Internet of Things (IoT) is one of the most used buzzwords in information technology. So, what is exactly the IoT? In broad terms, we can think of it as being composed of any physical device embedded with electronics, software, sensors, that is connected directly to the Internet, with the ultimate goal of providing users with additional “smart” features. Examples span from smart-TVs, baby monitors, smart-watches, to those devices controlling larger environments, such as smart cities (as in smart-parking devices, or smart-farming), and critical infrastructures (e.g., programmable logic controllers for water control). It also includes security systems (e.g., smoke detectors), thermostats, ventilation and air conditioning systems (HVAC), as well as smart-washers, smart-kettles and the likes. Finally, it also includes autonomous vehicles and implantable medical devices. In a well-known report[1], Gartner forecasts that 20.8 billion connected IoT devices will be in use worldwide in 2020. Indeed, the IoT promises economic growth as well as convenience for users: it is estimated to have a potential economic impact of $2.7-$6.2 trillion by 2025[2] and to create more than 4 million developer jobs by 2020[3].

## Vulnerabilities Of IoT Devices

While this is all excellent news for consumers, businesses and governments, the security (and safety) implications of the IoT are equally significant. This is because attacks targeting our online space may also put our physical security at risk[4]. This is mostly due to the increasing number of vulnerabilities in IoT devices found on a daily basis[5]: as an example, in October 2016, the distributed denial of service attack on Dyn, a company controlling and managing several DNS services, has brought down most of America’s Internet, and was caused by an IoT botnet (Mirai)[6]. These attacks, as well as several other ones[7], have been possible due to basic security vulnerabilities on IoT devices, such as digital video recorders, IP cameras, and routers. It is worth noting that some IoT vulnerabilities do not require advanced skills by attackers to be exploited as they usually come from very poor security design choices. For example, most of these vulnerabilities are due to insecure communications with the cloud backend (e.g., unencrypted traffic), weak identification (using the MAC address for identification), poor management of the security of the devices (e.g., hardcoded password), easily bypassable security controls, or insufficient security of the update mechanisms (e.g., private keys shared on all devices).

## IoT Threats

The impact of these vulnerabilities varies greatly, from enabling an attacker to remotely perpetrate a car, to unlock doors to let intruders in our house, or request a sharp increase of water temperature during our shower, or simply retrieve our camera feeds from a remote location. Attackers could remotely shut-down systems (e.g., HVAC), or install a stealthy malware onto all our smart-home devices to slowly take control of our home. In a hypothetical scenario, researchers have shown how it could be possible to create a black-out in an entire city using drones to hijack smart-bulbs, and replicating the attack using a worm[8].

## Issues With Securing Iot Devices

So why do vulnerabilities still plague new devices, after so many years of security principles learnt from past mistakes? Of course, the best defense would simply be for IoT devices to run only secure software (but what is “secure” software?). Unfortunately, this does not seem to be very likely to happen anytime soon, as, firstly, IoT vendors seem to be more interested in delivering a new "smart" feature baked into an existing device, maybe by packing together components from different manufacturers, than actually thinking of possible security/safety consequences this new feature may introduce. Secondly, security has also an additional cost (e.g., training developers, providing updates and patches) that maybe is not marginal for some IoT (cheap) devices. Thirdly, vulnerabilities on IoT devices are often very difficult to update, due to hardcoded firmware, or to small interfaces or to unawareness of users. Finally, some IoT devices are meant to stay with us for a long time (think about a smart-fridge), so their insecure life may span more than 10 years.

## The Future Of IoT Security

A recent report[9] by the Department of Homeland Security highlights some approaches and suggested practices to strenghten the security of the IoT. The principles focus on these key areas: incorporating security at the design phase; advancing security updates and vulnerability management; building on proven security practices; prioritizing security based on potential impacts; promoting transparency across the IoT ecosystem; and connecting carefully and deliberately. Some security experts, such as Bruce Schneier[10], advocate the introduction of government policies to regulate IoT. This could mean the introduction of measures such as regulations, fines, ratings, certifications, legal liability, and forensic investigations to help reduce the number and severity of IoT vulnerabilities. This could set a path for the near future to enable these “smart” devices to really improve our lives in a secure way. Unfortunately, the best way to understand the current status of security for the IoT can be summarized using this quote: the “S” in “IoT” stands for Security.

## References

[1] Gartner, “Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015”. 10 November 2015. Available at: https://www.gartner.com/newsroom/id/3165317

[2] McKinsey & Co, Disruptive technologies: Advances that will transform life, business, and the global economy. Available at: http://www.mckinsey.com/business-functions/business-technology/our-insights/disruptive-technologies

[3] VisionMobile, IoT report series: The Industrial IoT Landscape. June 2015.

[4] Camara, Carmen, Pedro Peris-Lopez, and Juan E. Tapiador. "Security and privacy issues in implantable medical devices: A comprehensive survey." Journal of biomedical informatics 55 (2015): 272-289.

[5] ComputerWorld, “Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON”. 13 September 2016. Available at: http://www.computerworld.com/article/3119766/security/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html

[6] The Guardian, “DDoS attack that disrupted internet was largest of its kind in history, experts say”, 26 October 2016. Available at: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[7] Brian Krebs, “KrebsOnSecurity Hit With Record DDoS”. 16 September 2016. Available at: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[8] Ronen, E., O'Flynn, C., Shamir, A., & Weingarten, A. O. (2016). IoT Goes Nuclear: Creating a ZigBee Chain Reaction. Available at: http://iotworm.eyalro.net/iotworm.pdf

[9] Tim Greene, “Bruce Schneier: Public-service technologists are needed to tame the IoT”. 15 February 2017. Available at: http://www.networkworld.com/article/3170825/security/bruce-schneier-public-service-technologists-are-needed-to-tame-the-iot.html

[10] U.S. Department of Homeland Security, “Strategic Principles for Securing the Internet of Things (IoT)”. November 2016. Available at: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf



# THE PRIVACY DEBATE

Anne Onymous

> Actually Dr Allan Tomlinson, ISG

We all thought that the Crypto Wars ended inthe 1990s, but some battles linger on. The details may have changed but the principles under debate remain the same: should security technologies be freely available, or should use of these technologies be controlled by the state? In the 90s the issues were primarily about encryption and secure communications. In the new millennium, particularly following the Snowden revelations, the debate has widened to encompass the more subtle issues of privacy.

## Nothing to Hide

The advent of "Web 2.0" and social media allowed us to publish our own content on-line. Many new services emerged to facilitate this and inevitably these service providers quickly saw how to profit from the data they were collecting.

Some users of these new services expressed concerns about privacy. However, in 2009 Google CEO Eric Schmidt pointed out that "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." This is the same Eric Schmidt who blacklisted journalists after they published personal information about him obtained through Google searches.

The argument that if you have nothing to hide, you have nothing to fear is rather naive. How many of you would allow a camera in your living room to broadcast images over the Internet? In 2013 LG televisions were discovered to be collecting personal information including "Voice Information captured through your use of voice recognition features" and sending this, unencrypted, over the Internet. In this case voice information was collected, however it's well known that webcams can be hacked to be switched on remotely and collect images. But, hey, we've got nothing to hide, right?

Many people do post images, videos, and all sorts of personal information on social media sites. Indeed, Facebook founder Mark Zuckerberg stated in 2010 that privacy is no longer a social norm". Since then, Facebook have continued to add privacy features to their service including private messaging and "Anonymous Login". When they updated their WhatsApp messenger with end-to-end encryption Zuckerberg praised it as an "important milestone for the WhatsApp community." Perhaps in 2017 privacy has become a social norm again. The notion of having nothing to hide is often used to support arguments against providing privacy. A similar argument is that "the ends justify the means". In other words, we can all give up a degree of privacy if it allows law enforcement agencies to catch the bad guys. On the face of it, this seems like a reasonable argument, but let's look a little deeper.

This is a dangerous argument. If accepted, it allows any action to be justified in the hope that eventually things will be better.

Another problem with this argument is that we can never know in advance what the "ends" will be. Giving up our privacy might help law enforcement agents to catch the bad guys -- but equally so, it might not. If the badguys know their communications are being monitored they will use single-use disposable "burn phones" as the Paris attackers did in2015. And everyone's privacy is forfeit for nothing.

The alternative approach to the "ends justify the means" argument above is to base our actions on an ethical code. We agree on what is ethical in advance of any action. We can then use this code of ethics to guide our actions, rather than act as we wish and hope that things will work out in the end. Most professions have a code of ethical conduct, and on a wider level the notion of Human Rights is a code of ethics. The European Convention on Human Rights is a code of ethics. And in Article 8 we find the right to privacy. Article 12 of the 1948 Universal declaration of human rights states that "No one shall be subjected to arbitrary interference with his privacy, family, home correspondence, nor to attacks upon his honor and reputation". So if we base our actions on such a code of ethics then it is clear that not only is privacy a social norm, but it is also a fundamental human right.

## How to maintain privacy

There can be no doubt that banning encryption and mass surveillance undermines our privacy. In some cases we may have recourse to the courts when our human rights are broken; but only after the damage has been done. Moreover, the real difficulty arises when it is the state who is undermining our privacy. Is there anything we can do to defend our right to privacy? Are there security technologies we could use? Or should use of these technologies be controlled by the state? Indeed, the Crypto Wars continue.

Well, encryption is not illegal yet, and there is an abundance of technologies that can be used to enhance our privacy with regular surveys of such tools published regularly. The details of the tools available change quickly, but there are a few standard techniques that remain fairly constant.

Let's begin with email. Many professionals exchange email during the course of their employment whose content may be sensitive: health, financial, or legal information for example. In a corporate environment S/MIME may be used to protect sensitive data; outside this environment GPG provides an alternative. Both tools provide plug-ins to email clients that can make signing and encrypting email almost transparent. These tools do require some initial configuration which may be just enough to put them out of reach of the general public. But service providers exist who offer the same functionality via a simple web interface. Moreover, some service providers offer a service where, even if GPG is not used, all messages stored on their servers are encrypted under a key only known to the user.

Internet search engines are well known for storing personal information. Of course we can clear our caches when we close the browser and enable tracking protection, but it may be simpler just to use a search engine that doesn't track us in the first place. Again, there are several search engine providers to choose from.

If further web browsing privacy is required we can consider using a VPN. Using a VPN from an overseas service provider frees us from ISPs who may be tracking our online communications. Taking this one step further brings us to the realm of mixnets, onion routing, and the "Dark Web". Scary stuff, but if our communications are so sensitive that we can't even risk using a VPN outside the state's jurisdiction then we need to consider these options. The Onion Router (TOR) is a good starting point, although it does have some limitations which are mitigated by the Tails or Whonix linux distributions. And, of course, the Achilles heel of mixnets and onion routers is the exit node.

Most services like those mentioned above don't provide absolute privacy or anonymity. The devil is in the detail and for extremely sensitive communications great care has to be taken. For example, who has access to the exit nodes? Can the state order VPN providers to disclose information? What network layer is protected and are there any leaks via other layers and protocols.

Ultimately if we use a service provider that requires payment we can be identified by our credit card details. Bitcoin is also vulnerable to linking unless the wallet is only used for a single transaction. Pre-paid credit cards or gift cards may provide a solution depending on how and where they are purchased.

But although there are some limitations to these privacy services, they are probably good enough for most of us. Simple measures like judicious use of search engines, GPG, and using a VPN will greatly enhance our privacy. For the real whistleblowers there are ways to do this safely, this is something we are currently looking at in one of our MSc projects.

## SHOULD I REALLY HAVE JUST CLICKED ON THAT?

Dr Marco Cinnirella

**> Senior lecturer, Department of Psychology**

On 15th March this year I stood on stage at the Institute of Engineering and Technology in London with two Royal Holloway colleagues from the Information Security Group (Lorenzo Cavallaro and Stephen Wolthusen). Our task was to deliver the College's annual Stevenson public science lecture. This was a pivotal moment for me, and I believe it signifies a wider shift in the Information Security (IS) space. It was the first time I had shared a stage with academics who work on the technical side of IS, and indeed the first time in my academic career I had engaged in any kind of academic dialogue with computer scientists.

The path that led to the delivery of this public lecture, and which ultimately got computer scientists talking to social scientists like myself, started some twenty months earlier. At that time I, together with colleagues David Denney and Rikke Jensen (Law, Royal Holloway), were approached by a CISO who had the vision to recognise that the landscape of IS could be better charted if a technical approach found synergy with a human factors one. Professor Robert Coles, CISO at GSK, commissioned the three of us to develop a new multi-disciplinary approach to understanding the human factors behind employee information security beliefs and behaviours within large multi-nationals like GSK. I headed up the psychological arm of this work.

When an organization thinks about Information Security, there is a natural tendency to see this as a technological issue, both in terms of problems and solutions. This technological framing is understandable, given that many CISOs and their teams have a background in computer science. However, despite automation encroaching further into the workplace, humans remain an integral component, at least for now, in most work environments, and there is one certainty that is irrefutable – when humans interact with technology, one can expect the unexpected. Plugging security vulnerabilities and fixing the mess caused by human error absolutely requires technological solutions, however there comes a point when an organization may want to go beyond reactive firefighting, and instead seek to be proactive and to understand why those fires are lighting in the first place. This is where technology alone can no longer provide an answer, and the different lens offered by social science has something to offer.

As employees grapple with day-to-day work tasks, under increasing pressure to hit ever tighter deadlines, to multi-task their way through the use of different systems, to navigate a sea of emails, and to abide by regularly changing and expanding regulations, they cope as best they can. One way in which our brains assist with such challenges is to help us learn mental short-cuts that generally serve us well, even if at times they can leave us vulnerable. By deploying these short-cuts - what psychologists call heuristics – we conserve our cognitive processing power in the same way that mobile devices save power and energy by throttling CPU clock speeds. Ellen Langer was one of the first social psychologists to demonstrate how these mental heuristics can sometimes leave us vulnerable. In what is now regarded as a classic experiment demonstrating what she calls "mindlessness", she took down all photocopiers in a US college library apart from one, with the result being that a long queue formed at the one functioning machine. At various points in time a confederate working with Langer would approach the person at the front of the queue and recite one of three pre-prepared requests aimed at being allowed to push in. In the first variant, a request was given without any justification, in the second a reasonable justification followed the request ("because I am in a rush"), and in the final variation, the justification given was facile ("because I need to make copies"). Langer postulated that when we hear a request followed by the start of a justification ("because…") our minds switch into a mental autopilot which she calls mindlessness and many psychologists today called heuristic processing. According to Langer, this mental shortcut tells us that usually the request is genuine, and its effect is to reduce the attentional resources we devote to properly processing the reason – this means that even an illegitimate or facile reason can sometimes generate the desired response. Indeed, the experiment showed that the illegitimate/facile reason condition generated 93% compliance with the request, compared to 94% compliance when a genuine reason was given.

Heuristic or "mindless" processing occurs more often than we like to admit. In terms of IS behaviours, the only way employees can navigate their work challenges is through the regular deployment of a whole army of such mental heuristics. What does a genuine email look like, what does a phishing email look like, what is a safe link to click on, which senders are usually or always safe? Answers to these kinds of question are provided by heuristics, which equip us with stereotypical knowledge in such a way that our perception is guided and targeted to pay more attention to some cues in the environment than others. Of course for the social engineer aware of such heuristics, they provide an opportunity to exploit everyday mental shortcuts to their advantage, by tailoring threats in such a way that they "fly under the radar" of what heuristics lead us to expect threats to look like. Only in the last two to three years have social scientists began to apply these insights to Information Security, and as yet organizations are unsure quite how to leverage such insights to their advantage.

Part of the challenge facing organizations is to therefore better predict the interaction between humans and technology. This is by no means a new problem. The need to understand it was brought home very painfully via accidents in the civil aviation and nuclear industries, yet such lessons are seldom seen as relevant to Information Security, which is regrettable. What they tell us, is that employees dynamically make judgements about the costs versus benefits of doing what management expect them to do, and balance risk against convenience. When employees judge that a policy or procedure is an unwelcome impediment to their productivity, they may seek (sometimes creative) means to subvert the policy, whether it be by, for example, using public wi-fi in nearby cafes to usurp restrictions on the company network, through to using unsecured personal mobile devices to complete work that is otherwise hampered (in their eyes) by the restrictions imposed on company devices.

The determinants of such judgements are not mathematical decision schemes (as per behavioural economics models) but instead a complex interaction of individual level factors (e.g. personality dimensions such as "sensation-seeking"), work environment factors (such as peer pressure, "psychological work contract" and management style) together with broader cultural factors such as the degree to which a national culture fosters what psychologists call uncertainty avoidance, which reflects a society's general orientation to accepting or minimising risk.

This complex mix of individual, work and societal/cultural factors together help determine an employee's response to both Information Security threats and the organization's Information Security policies/procedures. Understanding this complex puzzle is the only way to properly predict how employees will interact with technology, and seeking to do so will provide organizations with a degree of resilience that technological solutions alone can not provide. Ignoring such human factors is, I predict, something that organizations will not be able to sustain for much longer.

The Stevenson Lecture 2017 can be viewed at: https://tv.theiet.org/?videoid=10011



## COMPUTER WEEKLY ISG MSC INFORMATION SECURITY THESIS SERIES 2017

Dr Siaw-Lynn Ng

**> Senior Lecturer, ISG**

**Founded in 1992, the ISG's flagship MSc Information Security masters degree programme has now produced over 4000 graduates from more than 100 countries in the world. The success of this MSc programme was recognised in 2014 when Royal Holloway became one of only four UK universities to gain full GCHQ certification of their Cyber Security Masters programmes.**

**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, the topics of our MSc projects are wide-ranging, from dealing with high-level subjects such as the provision of privacy in social networks, to detailed technical studies of Android malware.**

**Every year, a number of outstanding MSc projects are chosen to receive the Computer Weekly / Search Security awards. These awards are given to those projects which best present research in an area of information security of interest to information security managers and professionals. These projects are re-written, under the guidance of the individual ISG project supervisors, as accessible short articles for a general professional readership and published online at www.computerweekly.com. The result is a series of informative leading-edge articles which provide a useful, informed, non-technical yet expert insight into a number of important topics.**

**This year we have ten articles covering topics from cyber insurance to unified communication.**

**Online social networks have become extremely popular in recent years. However, their large user base makes them attractive to attackers. In the article "Safety meshing: Hybrid trust models in social networks for end-to-end encryption", Max Kington (supervised by Allan Tomlinson) considers an approach which is a combination of centralised and distributed trust systems, making use of the connectivity between users to enhance the trust we may place on central authorities.**

**The prevalence of social networks also causes concern over the privacy of users. The privacy policies of some of the main social network providers are analysed by Minerva Hoessl (supervised by John Austen) in the article "Are we trusting social networks too much?" so that users may understand their positions in the conflict between the convenience of these social media and the preservation of their privacy. Another potential incursion into individual privacy is examined in the article "The Investigatory Powers Act 2016 and Internet Connections Records: some surprising truths?" by Daniel Coats (supervised by Peter Komisarczuk). Internet Connection Records are one of the key aspects of the recent Investigatory Powers Act 2016, and this article considers how useful the Act might be in law enforcement and to what extent it intrudes upon individual privacy.**

**Social network is just an example of the increasing interconnectedness of the modern world. As networks become increasingly complex and dependent upon one another, we need a better way of modelling them and improving their resilience against failures and attacks. This is the subject of the article "Towards more robust internetworks: an application of graph theory" by Jamie Greenwood (supervised by Stephen Wolthusen), where graph theory is used to evaluate the robustness of various network configurations when subjected to targeted attacks.**

**A particular example of a complex modern network is the maritime container terminal, which is where containerised freight is transferred between ships and overland transport. They are a vital element of a country's transportation infrastructure. In his article "Cyber-risks in maritime container terminals: Analysis of threats and simulation of impacts" Peter Beaumont (supervised by Stephen Wolthusen) explains the dependence of modern container terminals on communications technology, and shows how the impact of cyber-attacks against them can be modelled using Discrete Event Simulation techniques. Cyber-attacks that adversely affect the physical domain is also the subject of the article "Cyber-physical attacks: Dawn of a new age in cyber-warfare?" by Christopher Cope (supervised by John Austen). Here the potential impact of cyber-physical attacks is examined, focusing particularly on the use of aggressive cyber activity in support of political objectives.**

**Communications networks are also very much a part of business and industry. In "Unified Communication: It should work as easily as a telephone call!", Thomas Reisinger (supervised by Peter Komisarczuk) explains various aspects of Unified Communication which enable people to collaborate seamlessly, using various real-time communcation methods integrated with business processes. The article examines the security problems faced by organisations and the possible solutions. While many security mechanisms aim to block attacks on computer networks, the article "Active defence through deceptive IPS" by Apostolis Machas (supervised by Peter Komisarczuk) proposes another approach to gather threat intelligence while defending networks, using honeypots to deceive an attacker. As well as prevention, much effort has also gone into the detection of attacks by malicious software. In "Hunting ELFs: An investigation into Android malware detection", Thomas Atkinson (supervised by Lorenzo Cavallaro) describes how malicious ELFs (Executable and Linkable Format) lying dormant in the depths of Android mobile applications awaiting activation by the malware that controls them may be detected.**

**The use of various tools from information and communications technology in commerce and industry brings with it associated risks. Businesses increasingly turn to specialist insurance in an attempt to cover a portion of their enterprise risk. In "Insuring the uninsurable: Is cyber insurance really worth its salt?", Michael Payne (supervised by Peter Kormisarczuk) outlines some steps which businesses can take in order to make better informed risk mitigation decisions.**

**These articles are written in a style making them accessible to everyone, and I would recommend them to anyone interested in various aspects of information security. As they are published by Computer Weekly we will announce them on our website (https://www.royalholloway.ac.uk/isg/informationfornewreturningstudents/mscproject/thesisprizes.aspx). Articles from past years are also listed on the website. Note that 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/isg/research/technicalreports/technicalreports.aspx).**

# RECONSTRUCTING BABBAGE

Prof. Adrian Johnstone

> **Professor, Department of Computer Science**

Charles Babbage has been called the "great-uncle" of modern computing, a claim that rests simultaneously on his clear understanding of most of the architectural principles which underpin the modern computer, and the almost universal ignorance of Babbage's work before 1970. There has since been an explosion of interest both in Babbage's devices and the impact they might have had in some parallel history, and in Babbage himself as a man of great originality who none the less had essentially no influence at all on subsequent technological development.

The CS department at Royal Holloway has funding from the Leverhulme Trust for a project which investigates Babbage's approach to machine design. Adrian Johnstone and Elizabeth Scott are focussing not on the objects themselves, but on the language that Babbage developed with which to design and reason about his machines. The key research question is: *how is it that one individual working alone could have synthesised a workable computer design over a short period, designing an object whose complexity of behaviour so far exceeded that of contemporary machines that it would not be matched for over one hundred years?*

We believe that the answer lies in the techniques Babbage developed to reason about complex systems. His Notations showing the geometry, the timing, the causal chains and the abstract components of his machines, have a direct parallel in the Hardware Description Languages developed since 1970 to aid the design of large scale electronics. These languages typically have a geometry facet in which the arrangement of electronic components in space is specified; a register transfer facet which emphasises the interconnection of functional units and registers; and a behavioural facet which describes sequences as state machines or in software-like notations. These interlaced facets present different abstractions to the design engineer: the separation of concerns underpins our ability to design complex systems.

Babbage was a fertile source of inventions throughout his life, but his most celebrated achievements are

- the first Difference Engine (DE 1) initially conceived in 1821, with a large fragment (now in the Science Museum) being completed by the end of 1832;
- the development of designs for an Analytical Engine (AE) (a programmable computer) starting in 1834 and continuing until Babbage's death in 1871;
- the second Difference Engine design (DE 2) started in October 1846 which was a re-implementation of the DE I architecture using the much more efficient mechanisms which Babbage had invented as part of the AE designs.

DE 2 requires only one third of the parts of DE 1; it includes the printer mechanism from the AEwhich itself displays more state-space complexity than all of the DE 1 architecture.

The first and second Difference Engines compute numerical approximations to polynomial functions using the method of finite differences - automating the technique used at the time by teams of humans to produce books of tables for navigation and other purposes. Both DE 1 and DE 2 comprise a large array of subtraction mechanisms which are sequenced in a straightforward, fixed manner under the control of a single stack of cams. The state space of the machines is straightforward; the complexity in the engines arises mostly from replication of function units rather than complicated control flow.

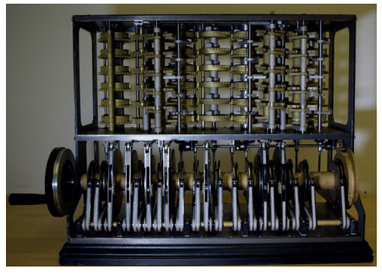
The Analytical Engine designs, for which three major phases of work can be discerned, comprise collections of function units specialised to particular purposes in a mill along with registers and a mechanical bus mechanism for transferring results back and forth. Some of Babbage's function units have complex state controlled by pins on a drum (effectively, a microcode controller) and the program itself can have branching flow control. The state space is thus vast, and the complexity of the hardware arises from both replication and from variation amongst function units.

Babbage's significance as the progenitor of modern computing has been both under- and over-estimated. Intellectually, the precedence case is clear: the Analytical Engine designs incorporate at an architectural level nearly all of the core concepts of a modern von Neumann style architecture - perhaps the only obvious exception is the notion of the virtual machine which was pioneered in the second generation of modern computers. However it is also clear that there are almost no direct lines of descent from Babbage's work to the mid-twentieth century development of electronic computers. Similarly, we believe that Babbage invented in the 1830's engineering methodologies that would only be universally adopted by professionals in the 1980's.

Babbage was very aware of the relative importance of objects and the meta-object; the design and the design discipline. He believed that his notation would become the standard design method taught in engineering schools. In that he was quite wrong; the notation was never widely appreciated. Most mechanical systems have very simple state spaces: it is only the introduction of memory that generates complex time-dependent behaviour, and that is exactly the point at which the geometry facet alone becomes inadequate to the task of specifying behaviour.

We are developing software tools to capture Babbage's designs from the surviving documentation, and to allow simulation of his Notation. Babbage used three kinds of documentation: form diagrams which are essentially un-dimensioned engineering part diagrams; *trains* diagrams which show the flow of cause and effect through a mechanism; and *cycle* diagrams which show timing relationships. Our modern reinterpretation of these notations is a language called FORTRAC (FORms, TRAins and Cycles – any resemblance to the names of pioneering software languages is accidental…). We are using the DE2 design as a sort-of Rosetta Stone, since we have the complete notations as well as the physical machine built by the Science Museum 25 years ago using only the engineering diagrams. So as to help ours and others understanding of the mechanisms, Dr Piers Plummer has designed and implemented a four column by six digit difference engine which uses Babbage's design principles for DE2, but opens up the mechanical structure so as to make it easier to see what is going on. The machine is built from laser cut steel and sintered-nylon 3D printed parts and will be offered as "open hardware", and Piers is currently completing a small steam engine to drive the difference engine.

Aspects of the project, including the steam driven Difference Engine will be on show in 18 months time in the new library bulding's exhibition space when the Holloway CS department celebrates its 50th anniversary.





# BREXIT: WHAT DOES IT MEAN FOR SECURITY AND PRIVACY IN EUROPE?

Prof. Chris Mitchell

> **Professor, ISG**

I am always rather dispirited by the standard media assumption that the most important aspect of any piece of news is whether it will make us, as individuals, a few quid better or worse off. Budget headlines are typically about how much more or less money we will have in our pocket because of the decisions made – not the larger impact of the decisions, many of which will almost certainly have a much greater effect on us, both as individuals and as a society, than minor changes to personal taxation or duty on fuel or beer. I believe this emphasis seriously underestimates the intelligence of the average newspaper reader or television watcher.

In the same way, almost daily articles in the mass media about Brexit focus on the direct financial consequences for the UK of the latest leaks, hints, or pronouncements. In much the same way, discussions of the Brexit impact on cyber security and privacy focus almost exclusively on how the UK will be directly affected by the Brexit process. Of course, this is an important matter and merits discussion, but it ignores a much more far-reaching effect, namely the likely loss of involvement of the UK and its experts in deciding the future of European regulations governing security and privacy. Given its much greater size and economic clout, the EU will likely dictate the UK rules for security and privacy, and so a loss of voice is a serious matter for all of us: the EU and the UK.

This is underlined by Peter Allison's recent Computer Weekly article, What happens to data protection when we leave the EU? As noted in his article, "no matter what the future legal relationship between the UK and Europe, personal information will need to flow". That is, if the post-Brexit UK significantly weakened the EU's General Data Projection Regulation (GDPR), due to come into force in the EU in May 2018, i.e. before Brexit occurs, then data flows between the UK and the EU will be adversely impacted, to the detriment of us all. As a result, this scenario is dismissed in Allison's article as most unlikely.

That is, whatever data protection regulations the EU enacts, not only at the time the UK exits the EU but at any later time, are almost certain to be adopted by the UK wholesale. The same is very likely to apply to EU directives and regulations governing cyber security; the UK simply cannot afford to be out of line with the continent in these matters. Of course, until now this has not been an issue, as the UK and its experts have played a major role in helping draft the EU documents. As Allison notes, the GDPR has been welcomed by UK industry; moreover, the UK has for many years exerted huge influence on EU security policy. This is supported, for example, by an article from 2012 in which Europol's director Rob Wainwright is quoted as saying that the "UK's contribution to policy-making in EU internal security is invaluable", and that it is "without doubt … one of the most influential Member States in shaping European internal security legislation". This influence has not always been in a direction favoured by all our European partners, but has been designed to reflect the UK's own policy and interests. For example, in the same article, Tony Bunyan (Statewatch Director) notes that "It is certainly true that the UK has been, and is, a major player on EU policing and internal security policies. However, there is little evidence that the UK's role has safeguarded civil liberties. On the contrary, the UK proposed that the Commission's EU PNR scheme be extended from just monitoring flights in and out of the EU to include internal flights between Member States … When it comes to internal security the UK is on the side of the hawks".

All this will change in the post-Brexit world. It seems very likely that the UK will cease to have direct input to the cyber security and privacy policy-making process in the EU. This is where I suggest the major long-term impact will lie – that is, in loss of influence rather than in any short-term adjustments in law. This is likely to have serious, and potentially damaging, consequences for two main reasons. Firstly, the UK will be obliged to adopt policies being formulated by the EU without any direct influence, and hence without the possibility of bending policy direction in the UK's favour; so much for taking back control! Secondly, and even more seriously, it is without doubt that the UK has significant expertise in the cyber security and privacy domain; after all it was the UK that led the world in developing data privacy legislation, and it was the UK that developed BS 7799, which eventually morphed into ISO/IEC 27002, a key component of the hugely influential ISO/IEC 27000 series of information security standards. Future EU policies may end up being less well-crafted, to the detriment of us all. It is interesting to note that many parties have made similar observations. In a Guardian article from February 2015, Norway's Minister for Europe is quoted as warning the UK of serious consequences for its security policy if it leaves the EU, primarily because of its loss of influence.

One other cyber aspect of Brexit merits attention. As others have noted (see, for example, Ghosh), restrictions on free movement may also exacerbate cybersecurity skills shortages in the UK. Given the dependence of the UK economy on the City of London, where such skills are in very high demand, an inability to recruit the best experts may itself damage the effectiveness of corporate security. Whatever happens, interesting times lie ahead for cyber security and privacy both in the UK and the EU. Finally, regardless of changes in the political environment, in the ISG we will continue to play our part in improving the supply of skilled cyber security experts through our long-standing commitment to cyber security education at both masters and doctoral level. We are also committed to continuing to expand our involvement in undergraduate teaching of cyber security. We will also continue our efforts to make a positive impact on the wider world, through our research, our involvement with industry and commerce, and our deep commitment to security standardisation.



# CREATIVE PRACTICES AND IMAGINED RISKS: IMPACTING ON CYBER SECURITY POLICY

Rikke Bjerg Jensen

> School of Law

Over the last four years, I have led and been involved in a number of inter-disciplinary research projects that have all orbited around questions relating to security and digital practices, and how academia can impact upon such practices; funded by government departments, research councils and industry partners. Ranging from exploring the use of social media technologies by military personnel and their families to understanding the meanings that people ascribe to their online behaviours – whether perceivably risky or not – these projects have facilitated new insights into wider human aspects of cyber security. More specifically, such projects have enabled an exploration into the relationship between digital practices and security through specific institutional cultures, examining how different members of those cultures conceptualise particularly risky spaces, objects, people, networks and structures.

This work has been driven by a growing interest in the ways in which people embedded within large organisations understand and experience risk primarily in relation to their own use of digital technologies and mobile devices in professional and personal capacities; practices that range from clicking on "dodgy" links in emails to circulating military orders through social media platforms. Whilst we might think of such practices as increasingly normalised everyday behaviours, as they have become largely habitual and engrained in our daily lives, they also exemplify a certain kind of creativity which is often used to negotiate creaking organisational infrastructures as they navigate particular articulations of risk and security. In many ways, these are approaches which have been employed to control, manage, or harness digital technologies, on the one hand, and circumvent established structures of connectivity, on the other, and are therefore constituted through or across a variety of spaces and networks.

Whilst digital technologies, and those who use them, have largely been perceived as potentially risky and worthy of practices that seek to securitise them, especially in organisational contexts, there is evidence to suggest that the measures and systems that have attempted to curtail digital risks and wider insecurities are potentially counter-productive. To this end, the work that I have been involved in over the last four years is illustrative of the erosion of information security behaviours and attitudes as well as the production of subversive practices that creatively find ways around the organisational measures that have been put in place to police them. It exemplifies the extent to which policy formulation in the context of cyber security and information protection is driven in part by a series of imagined risks, often based on perceived risky behaviours, spaces and objects. These imaginations have permeated organisational approaches to cyber security in ways that have shaped policy articulation and legal frameworks. It is therefore imperative that insights from research into actual digital practices, which we might call "creative" or "everyday", foster greater awareness of the need to move beyond perceptions and imagined practices.

But what do such practices tell us about cyber security and policy formulation? What constitutes risk in organisations with respect to online behaviour? And how might academic research impact upon the ways in which risks are conceived and imagined? Research in this area should of course engage with more critical work on notions of security by and through the digital. Perhaps the most obvious is the way that particular ideas about digital practices, behaviours and spaces are being developed and imagined by various actors as innately risky or threatening. Specifically, spatial and temporal demarcations are routinely invoked as threatened or put at risk by the digital and its inter-related human practices. At the same time, an emphasis on the everyday negotiations of connectivity and creative practices, within and beyond organisational settings, provides quite a different way-in to understanding policy development in the context of cyber security. Whilst many perspectives on cyber security have tended to operate on the level of technology and networks, less well understood are the more banal, but no less important, online social practices. Such a perspective, focused on the human-centred engagements with digital technologies in everyday contexts, is necessary if we are to broaden and deepen our understanding of wider security logics.

Against this backdrop, and with the aim of impacting upon the ways in which digital practices are conceptualised and framed by policymakers, my most recent project (with Professor David Denney, School of Law) has aimed to bridge the gap between academic research and policymaking within a cyber security framework. This is based on the growing need for understanding actual digital practices and behaviours in order to shape policy; and to counter the policy development based on imagined risks. Impactful research is particularly important in the context of cyber security given the speed with which social problems, driven in part by technological change, are being identified, defined and re-defined by policymakers. There are also particular security matters arising from such meta phenomena that require urgent change to the way in which research findings can be utilised in day-to-day policy and practice development. Similarly, there is a growing need to strengthen pathways to impact in the context of cyber security research and to develop a broader and deeper academic institutional strategy for policymaker and stakeholder engagement.

Instigating a dialogue between academic researchers and key stakeholders about how research into cyber security might impact on policy and practice is important. This is particularly significant as UK government funding bodies and university departments are placing growing importance on the need for research projects to demonstrate impact. Regardless of this increased focus on impact, academic institutions are often separated from the complex processes of policy implementation within organisations as my own research into different aspects of cyber security has demonstrated. This is despite the fact that such organisations are critical to ensuring that research findings have the intended impact with key stakeholders. Therefore, whilst academics face growing pressure to demonstrate that their research has an impact on wider societal and economic factors, and public knowledge more generally, how this impact is achieved is less clear.



# STAFF PROFILE: DR JORGE BLASCO ALIS

**> Lecturer, ISG**

**How did you become interested in Computer Science?**

**I think that it was mostly because of video games. When I was a kid my parents had an Amstrad PC at home. It was an amazing machine: It had no hard-drive, so every time we wanted to use it we had to insert a Floppy Disk with the Operating System (MS-DOS) to load our games. My brother and I used to play the Teenage Mutant Hero Turtles and other games for hours. One day, we discovered that if we randomly pressed all the keys on the keyboard long enough our turtles would become invincible for the rest of the game. I think that was my first brute force attack. Some years later, after Windows 95 was released, me and my friends bought a real-time strategy game called Age of Empires. At that time, not all of us had internet at our homes, so many weekends we would take our computers on the bus to play LAN parties throughout the night and trust me, computers at that time were not lightweight, you had to carry at least 10 kilos of hardware; the tower, the CRT monitor, keyboard, mouse and all the cables. Most of us decided we wanted to study Computer Science to build games like that.**

**How did you become interested in Information Security?**

**During my undergraduate degree, I took some optional courses on cryptography and information security. We studied classical and modern ciphers like Caesar, AES and RSA. I enjoyed studying the maths behind them, but what really grabbed my attention were the lab assignments of the information security courses. We learned how to encrypt files with OpenSSL and PGP, and we even had to implement a buffer overflow exploit to execute arbitrary code in an old Linux version. It was both very challenging and rewarding work. The exploit wasn't stable enough to work all the times so every time it was successful we went a bit crazy.**

**I enjoyed these courses a lot, so I signed up for the other optional courses on information security. My specialization was still artificial intelligence, but my interest in game development was slowly being replaced by information security. When I got to the end of my degree I wanted to do something related to information security as a project, so I talked with one of the lecturers within the department. I created a tool to hide C source code into text. I enjoyed this so much that I decided to put aside game development and embarked on a PhD focused on Steganography and Information Leakage. Games are still a part of my life, but just for fun!**

**What attracted you to come to Royal Holloway?**

**The Information Security Group with no doubt. The first I heard about the ISG was at Royal Holloway while I was studying for my PhD in Spain. I was in a conversation about the leading research groups on information security in Europe. One of the first groups that were mentioned during the conversation was the Information Security Group at Royal Holloway. During those years (and it still happens now), every prestigious conference had at least one paper from researchers in the ISG.**

**After my PhD I moved to the UK to work as a Postdoctoral Research Assistant on an EPSRC funded project. My project was related to Android Security and again, the research done within the Information Security Group, and more specifically in the System Security Research Lab (S2Lab) lead by Lorenzo Cavallaro came up. When I saw the opening on the website I thought the ISG would be a great opportunity for me to join a world-leading research group on information security with academics sharing a lot of their research interests with me.**

**What are your main research areas of interest?**

**My main research areas of interest are all related to system security. I have worked and still actively work on analysing Android malware. I work both on single and multi-app analysis. We analyse single apps looking for what is commonly known as mobile malware. In particular, I'm working on developing methods to quickly and accurately distinguish between benign apps and malware. The methods I'm developing are based on static analysis of apps through deep learning algorithms. When analysing multiple apps, my research focus on verifying that the communications between the different apps within a device are all related to the benign functionality of the app and are not used for malicious purposes.**

**More recently I have also focused on wearable based biometrics. New wearable devices like fitness bands are equipped with arrays of sensors that make them very suitable for biometric applications. Wearable biometrics have some advantages over traditional biometrics. They can be used for continuous authentication and allow the wearer to have full control over his biometric data. However, they also present challenges like the amount of noise present on the captured signals due to the highly dynamic environment and low cost of the sensors.**

**In addition, I am also interested in innovative methods to teach information security. In this regard, I recently developed, with Professors Peter Komisarczuk and Keith Martin, an introductory MOOC about information security that is now live on Coursera. I also plan to use my board-game addiction to develop a game that teaches non-technical people the security risks associated with information systems and how to mitigate them.**

**Could you tell us more about the possible security implications of malicious communications between Android apps?**

**Third-party apps installed in an Android system are considered non-trusted by default and are isolated from the rest of the system and apps through a sandbox and a permission system. Unfortunately, all apps, independently of their permissions, can communicate with other apps without any restrictions or user notification. At first this may not seem to be a big deal, but this allows apps to bypass the Android sandbox restrictions and opens the room for many malicious or, at least, unwanted behaviours.**

**For example, an app with access to the contact list (or any other permission-protected resource) could allow other apps to access this resource via inter-app communication. In the case of the contact list, a first app with access to the address book, could read all the contacts and send them to another app that was not granted access to them. Another possibility is information aggregation for aggressive advertisements. Apps embedding the same advertising library could share and correlate the behaviours of the users among different apps, violating their privacy. Colluding apps like these are very dangerous because most of the existing tools that are used to identify malicious apps are focused on analysing apps on their own without considering how they communicate with other apps.**

## STUDENT PROFILE: RACHEL PLAYER

**> PhD Student, ISG**

My first experience in research was during sixth form, when I was fortunate to be awarded a Nuffield Science Bursary (now named a Nuffield Research Placement). The Nuffield scheme enables students in year 12 to experience life as a scientist, by taking part in a short placement during the summer. My placement was in the maths department at the University of Liverpool, where I was introduced to the magic of linear algebra. I worked collaboratively with another Nuffield student, and the whole department was very welcoming and encouraging. I left with a sense of excitement about sharing knowledge, and keen to learn more maths.

Learning more maths had been my goal for as long as I could remember. I was frustrated with the pace of school maths lessons: in year 8 I asked my maths teacher what the square root of i was, and when he didn't answer I went away and supplied him with it in the following lesson. At that time, I was already excited about the prospect of studying lots more maths at A level and beyond. Studying maths at university was a clear option and this gave me a well defined "life goal".

In 2009 I duly arrived at the University of Warwick to begin my mathematics degree. Through a wide range of modules, I discovered that my interest was in number theory and algebra. Given my enjoyment of my Nuffield placement, this was perhaps not surprising. Four years passed quickly (as it has done now for the second time in my PhD studies!) and as I approached the end of my degree, I agonised about what to do next.

I had been fortunate again during my final year at Warwick to work with Prof. Samir Siksek, who supervised my MMath research project in number theory. Samir was extremely enthusiastic and helpful, and I enjoyed this project so much I began to think seriously about a career in research. At the same time, a sense of pragmatism kicked in, and I was wondering how best to use all this maths I was excited about. "Then it dawned on me: I should try the canonical application of number theory, cryptography! By a third stroke of good fortune, Samir had heard recently from colleagues at Royal Holloway of a PhD studentship in lattice-based cryptography that sounded ideal for me. Before I knew it, it was September 2013 and I had arrived in Egham to begin my PhD under the supervision of Prof. Carlos Cid and Prof. Sean Murphy.

Now I am coming to the end of my PhD, I can reflect on the innumerable benefits of studying here in the ISG. For example, from the many events the ISG holds with industry contacts, I have a sense of commercial awareness I was lacking at the end of my undergraduate studies. From the many opportunities to present my work at internal and external seminars, I have become a better communicator.

The department has a strong collaborative ethos, and this has been helpful to me through my PhD. As soon as I began my PhD, I began working closely with Dr. Martin Albrecht and fellow PhD student Sam Scott. As a result of this we published a paper in the Journal of Mathematical Cryptology.

Not only have I benefitted from the highly collaborative environment within the department, but I have also had the opportunity to work with external researchers. For example, in 2015 I was fortunate (we are now on the nth stroke of luck, I am sure) to spend a week visiting researchers in Prof. Buchmann's group at TU Darmstadt, which resulted in a paper published at Africacrypt 2016.

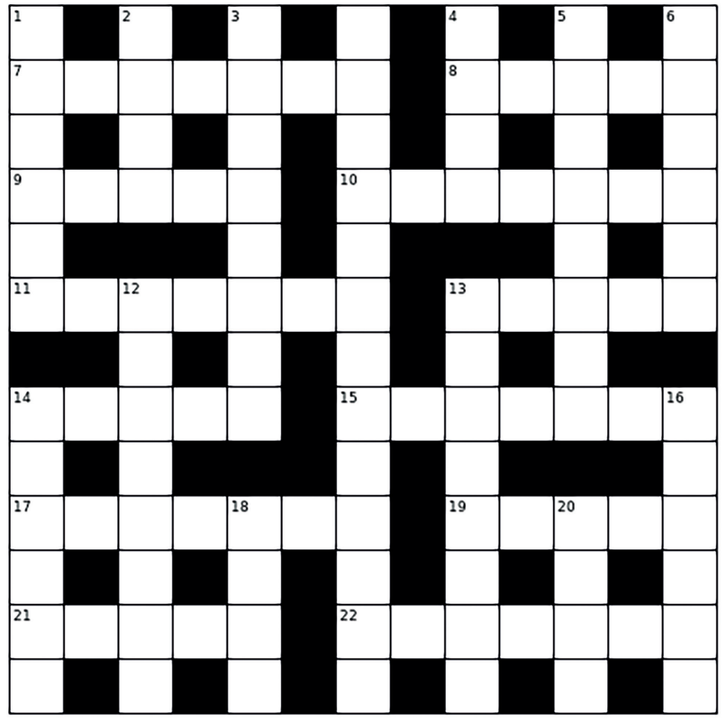
A highlight for me was undertaking an internship in spring 2016 in the Cryptography group at Microsoft Research in Redmond, USA, where my mentors were Dr. Kim Laine and Prof. Kristin Lauter. The group is developing a homomorphic encryption library called SEAL and I was implementing a new version of the library. The underlying encryption scheme implemented in SEAL is based on Ring LWE, which is a variant of LWE (Learning with Errors). LWE is a problem that is believed to be hard even when the adversary is equipped with a quantum computer. This is in contrast to some more traditional hard problems, such as factoring. Since I had previously worked on the cryptanalytic side (trying to determine how hard it is to solve LWE), I found it really interesting to be working on the construction side (trying to build exciting applications based on LWE), and this complemented my previous work well. In April 2017 I presented a paper based on our work on SEAL at the 5th Workshop on Encrypted Computing and Applied Homomorphic Cryptography in Sliema, Malta.

Since having role models has been so helpful to me, I strongly believe in trying to give the same access to others. To work towards this, I am really excited to be involved in the WISDOM (Women in the Security Domain or Mathematics) group in the department. I think this is a great way of forging networking and mentorship opportunities in order to encourage other young women to have successful careers in mathematics and information security. I am enjoying meeting groups with similar aims to WISDOM and learning what strategies they have found successful to this end.

Looking towards my own future career, once again I am agonising about what to do next, if not for any other reason than I feel like I have so many options! The path of a researcher seems as appealing as ever, but whether a researcher in industry or in academia is yet to be determined. In any case, I am yet again in a fortunate position, so I truly hope that in the near or distant future, I can return some of the many favours and help out others who hope to build a career in this area. Perhaps the ISG could welcome a Nuffield Research Placement student, and the cycle may continue!



## CROSSWORD
by Serpent



**A 1 down, 14 down has been used to encrypt the 6 down, 16 down.**
**The plaintext must be written beneath the grid.**

**Across**

7. **Angular measurement in a spherical co-ordinate system (7)**
8. **Cloth used for making uniforms (5)**
9. **Binge (5)**
10. **Windows text editor (7)**
11. **Nonsense (7)**
13. **Increase in salary (5)**
14. **Social class (5)**
15. **Terse (7)**
17. **Kneecap (7)**
19. **What protects the brain (5)**
21. **Showy splendour (5)**
22. **What protects the brain (7)**

**Down**

2. **Purveyor of pork pies? (4)**
3. **Body of a plane (8)**
4. **Satirical sketch (4)**
5. **Series of activities intended to achieve some goal (8)**
12. **Agitate (8)**
13. **Bicycle-powered carriage (8)**
18. **Old stringed instrument (4)**
20. **Single undivided entity (4)**

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: royalholloway.ac.uk/isg