Information Security Group

Review 15/16

ROYAL HOLLOWAY UNIVERSITY OF LONDON

WELCOME FROM THE DIRECTOR OF THE INFORMATION SECURITY GROUP (ISG)

Prof Keith Mayes

It is my pleasure to introduce the latest in a long line of ISG Newsletters, and to inform you of our recent activities in information /cyber security education and research. If you are a potential student then it should provide compelling evidence that this is absolutely the place to study, and your ticket to a very interesting and rewarding career. If on the other hand you are from industry or government then you should see that we produce many expert/skilled future employees and that we offer cutting edge ethical research and expert advisory services.

With the ISG I cannot talk about the present without mentioning the past. Firstly, I must thank my predecessor Professor Keith Martin for his huge contribution to ISG leadership over recent years, however, for the ISG origins I must venture much further back in time.

The ISG formed in 1990 with Professor Fred Piper as the first Director; beginning a quarter of a century of pioneering work. Cyber security is a hot topic today, but how many institutions recognised this 25 + years ago? The ISG launched the first specialist MSc around the same time; however, the seeds of ISG activity are even older. As a young engineer, the first book I read on information security was called "Cipher Systems", by Fred Piper and Henry Beker, and published in 1982!

In a quarter of a century, the ISG has trained many post-graduate students. Our alumni number well over 3,000, including senior figures in industry and government. This explains why our employability is so outstanding, having hit 100% in several recent years. Our alumni numbers will be swelled by our current 200+ students on the campus MSc, 250+ on the Distance Learning MSc (both GCHQ certified), and our 90+ registered PhD students. The PhD numbers are boosted by our EPSRC/GCHQ supported cyber security Centre for Doctorial Training (CDT), one of only two in the UK, which offers 10 funded PhD places each year. The MSc is now available with a year in industry option and we also offer cyber/information security specialisms within Computer Science undergraduate and MSci courses.

ISG teaching is underpinned by excellent research. The ISG is well known for its cryptography/protocol work, but our research is enormously diverse and spans from human factors, critical infrastructure, network security, mobile devices, Internet of Things (IoT), clouds and embedded systems. For example, the ISG Smart Card and IoT Security Centre, looks at embedded systems and implementation security, including payments, mobile, IoT and transport security. Another example is the ISG System Security Research Laboratory that focusses on software security, including botnets and malware.

We believe in the excellence of the ISG, but never rest on our laurels. Our courses are continually evolving with the help of our industry and government contacts. We note the growing importance of our multi-disciplinary research and this newsletter includes articles from colleagues in Mathematics, Law/Criminology and Geography/ICT4D; as well as the Royal Holloway Capture-the-Flag team ("Phish&Chips"). Collaboration beyond the University, either directly or via our Institute for Cyber Security Innovation, enables even more impact and we are actively pursuing this agenda.

I hope that you find this newsletter interesting, and please do not hesitate to contact us if you require further information.

INDEX

A BRIEF HISTORY OF THE MSC IN INFORMATION SECURITY

Dr Chez Ciechanowicz

> MSc Information Security Programme Director

In 1987 a number of companies came to Royal Holloway to discuss the possibility of introducing an MSc in Cryptography. Fortunately (with hindsight!) it was felt that this would be too 'narrow', and that a degree in the wider area of Information Security would be more beneficial to industry, and produce more students for Royal Holloway. After considerable consultation with our (ever increasing number of) industrial partners, the MSc in Information Security was launched in October 1992.

Developing this MSc is certainly the greatest single achievement of the ISG, and we are enormously proud of the achievements of its many graduates. The MSc was the first of its kind anywhere in the world. From its inception it has always been aimed at meeting the needs of the real world, and the ISG has continued to maintain and develop its strong links with industry and commerce. One indication of these links with the 'outside world' is the fact that the MSc has always relied on 'outside' lecturers to cover areas where we had no expertise, and to ensure industrial relevance. This was particularly true in the early years of the MSc when one quarter of the MSc was taught by industry experts.

In the first year the MSc had 7 full-time students and 3 part-timers. Student numbers grew rapidly, and at the height of the dotcom era we had over 250 MSc students. Luckily for project supervisors and exam markers, numbers later stabilized at about 150 – 180. Staff numbers had to increase correspondingly! The original ISG had 5 full-time academics; we currently have 17.

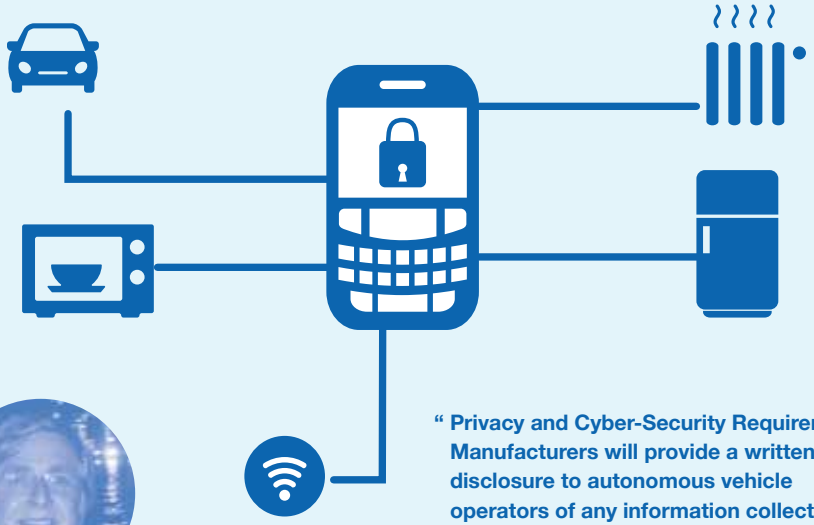
As the MSc grew in the mid 1990s, the ISG's theme of Academia and Industry in Harmony was developing. One of our main partners was Zergo, founded by Henry Beker, who introduced a structured Information Security training programme on which members of the ISG lectured. This led in 1994 to the Introduction of the Postgraduate Diploma in Information Security, based on courses offered by Zergo and an MSc level dissertation supervised by Royal Holloway academics.

A major landmark was the award to the College of The Queen's Anniversary Prize for Higher and Further Education of 1998. This prestigious award was given in recognition of the work of the ISG.

Certainly, the success of the MSc and the subsequent expansion of the group have provided the resources to enable the ISG to make a contribution to the field of information security. But perhaps its greatest asset consists of its students and alumni. Students from a wide variety of backgrounds have brought their different experiences and insights to the MSc to enhance the learning experience for all. And our alumni (more than 3000), now spread throughout the world and in many different companies and enterprises, have continued to support the ISG and contribute to its work.

Changes and developments have multiplied rapidly since 2000, and we conclude by listing the most important of these:

- The range of MSc courses has continued to expand. In 1992 there were 3 options modules. During the period 1996 to 2014 an additional 11 modules were developed and taught.
- In order to accommodate the need of students with interests focused on e-commerce, an MSc in Secure Electronic Commerce was introduced in 1999. This MSc ran for five years, and was then restructured to become the "Secure Digital Business" pathway through the Information Security MSc.
- In 2003 a Distance Learning version of the MSc was launched through the External Programme of the University of London, thereby opening up a totally new market for the ISG. There are currently more than 300 registered students.
- In 2008 as a response to industry demands, ISG introduced Block Mode delivery for a substantial proportion of the MSc. With all the various delivery modes now available, we have developed a totally flexible way of studying the MSc over an extended period.
- The MSc was taught in Rome between 2011 and 2013 for GCSEC (Global Cyber Security Center).
- In 2012 six specialist "MSc tracks" were introduced. Completion of an MSc track will indicate that the student has achieved a degree in a specialist sub-area.
- In 2014 the campus MSc was one of only four Master's programmes to achieve full GCHQ certification. In the following year the Distance Learning MSc also achieved full certification.
- In 2015 we launched a Year in Industry option for the MSc
- We now have the support of a large and impressive group of distinguished Visiting Professors.
- Laboratory facilities for the students have improved dramatically since the early days, and the ISG now has its own highly complex computing environment.



THE INTERNET OF THINGS – SOME SHAPES FORMING IN THE MIST

Prof. Paul Dorey

> ISG Visiting Professor

A world of physical objects instrumented with sensors, communicating data and acting on their environment is a mind boggling thought. In fact, the Internet of Things (IoT) has been called the Internet of Everything which is exciting technically but completely overwhelming when we try to think about the security. The good news is that some areas of focus are starting to emerge on a sector by sector basis and it's a story of both data and devices.

Driving Ahead

The several years of focus on 'research hacking' of a range of automobile makes, that in July 2015 got a lot of unwanted attention for the Jeep Cherokee, has created a corresponding response from the industry. Security standards and information exchange groups have formed, and an industry of security consultancy, assessment and even OEM devices such as car firewalls and Intrusion Protection are on offer. First Tesla, and now GM have created bug bounty and responsible disclosure programmes and we have seen entertainment system company Harman acquire Towersec (known for its on-board security systems to protect Electronic Control Units (ECUs) and Telematics control systems (TCUs).

Where there are risks there are also regulators, with a proposal from US Senators Ed Markey and Richard Blumenthal for the US Security and Privacy in your Car (SPY) Act 2015-2016 which would regulate vehicle privacy and security. In California, December 2015 saw the publication of draft regulations for autonomous vehicles that also look at both privacy and security – to quote the summary:

> " Privacy and Cyber-Security Requirements: Manufacturers will provide a written disclosure to autonomous vehicle operators of any information collected by the autonomous technology that is not necessary for the safe operation of the vehicle, and will be required to obtain written approval to collect this information. Autonomous vehicles will be equipped with self-diagnostic capabilities that meet industry best practices and are capable of detecting, responding, and alerting the operator to cyber-attacks or other unauthorized intrusions. In the event of such an alert, the autonomous vehicle operator will have the capability to override the autonomous technology."

This all shows a significant advance in thinking and we should expect a lot more leading work to happen around automotive security, plus a growing support industry to back it up.

Back at the Home

Unlike the more closed development environment of the car, the chaotic situation of the Internet of Things in the home is still showing the challenge of open systems and diversity. In the home there are multiple vendors and use cases, and system integration is in the hands of the end user. Default passwords and poor security management (such as missing patching) is still too common, but the worst part of home IoT security and privacy can be the attitude of the product vendors who are not used to running services. Towards the end of last year we saw reports that technology toy manufacturer VTech had been hacked, with a disclosure of 6 million records which included children's names, dates of birth and gender. The hackers also stole photos and chat logs from VTech's Kid Connect service, which allows adults to use their smartphones to chat with kids using a VTech tablet. VTech notified customers by letter but then quickly changed their terms and conditions to read:

> " You acknowledge and agree that you assume full responsibility for your use of the site and any software or firmware downloaded there from. You acknowledge and agree that any information you send or receive during your use of the site may not be secure and may be intercepted or later acquired by unauthorized parties".

The strong negative reaction to this by many commentators was also supported by regulators such as the UK's Information Commisioner's Office (ICO) who (in a press interview) have said that such terms are contrary to existing data protection regulation. But it is not all bad. Consumer product vendors such as Phillips (makers of the Hue light bulb) have dedicated security design teams, assurance processes and their own responsible disclosure process. The home IoT device market is also generating commercial interest for new security services, including start-up Dojo Labs, with a home network integrity and intrusion monitor which they are developing through crowdfunding, and also established security company F-Secure with their 'Sense' network security hub planned for release in late 2016.

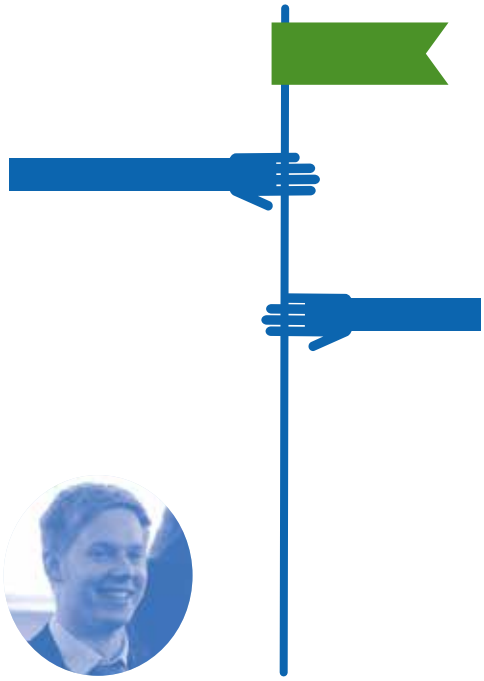
However, as the majority of home applications are unlikely to be of interest to regulators, so self-policing and standards setting are particularly important. Examples include the Allseen Alliance who focus on interoperability and so (to quote the Alljoyn Standard)

> "...have security at the application level; there is no trust at the device level. Each interface can optionally require security. If required, authentication occurs on demand between the two apps when a method is invoked or to receive a signal".

It's a start, but as any security professional will tell you, true security of a system cannot be determined without reference to the trust levels of the components. For example, at the time of writing NIST have just put a paper (Draft NISTIR 8063) out for comment that defines a set of five Internet of Things primitives (from 'sensor' to 'decision trigger') to help in the analysis of trust requirements.

Perhaps some of the standards from the industrial sector, who can draw on their experience of security in the SCADA/ Industrial Control Systems world, can provide greater depth. A good example is shown by the Industrial Internet Consortium (IIC) Reference architecture. Secure design requires attention to the security concerns for endpoints, the communication between them, and for security of the processing and storing data. With a similar breadth, the mobile operators GSM Association (GSMA) has just (February 2016) published some guidelines on IoT security where they explore use cases such as wearable devices and mobile drones. These address services and endpoints as well as network operator concerns.

So, the Internet of Things may be big, but sector by sector we are getting to grips with security.



RHUL LAUNCHES NEW CTF TEAM

Dusan Repel

> CDT PhD Student

Recently, a handful of computer science and information security enthusiasts have assembled to form RHUL's new and official Capture the Flag (CTF) team. Over the next action-filled days, the team swiftly broke a polyalphabetic substitution cipher, authored custom shellcode for a buffer overflow exploit, uncovered embedded steganographic data and factored a weak RSA key. Their raison d'être was clear: to exercise their information security skills in a legal, challenging and extra-curricular environment, with the ambitious objective of becoming world-class.

The CTF principium brings to the discipline of computer security a competitive sharp-edge, wherein a developed understanding of cyber security is effectively wielded in a time-sensitive context, and the motto "knowledge is power" is routinely materialized. The objective of CTF competitions is to distill the present-day wide-spectrum computer security work, involving vulnerability discovery, exploit synthesis, cryptanalysis and tool tradecraft into short and objectively measurable exercises.

Hence, in the spirit of offensive cyber security, an official RHUL team of hackers, code breakers (and of course, coffee makers), collectively referring to themselves by the UK-oriented name "phish'n'chips", was born. The CTF team has grown considerably since its inception and sports a diverse range of multi-skilled attendees, sourced from many corners of RHUL's undergraduate and research community, including BSc, MSc, PhD and post-doctoral levels. Regardless of academic rank, participants are warmly invited to contribute in-depth knowledge and security experience gleaned from the cyber domain, and apply it in a unit-esque manner to solve technical problems in real-time.

RHUL's CTF team is administered and jointly run by postgraduate members of the Information Security Group (ISG) and Computer Science departments. Structurally, a CTF team requires both a degree of central organization, and pro-active voluntary participation from the student community. The team is therefore logically divided into a large majority of players, who primarily join to explore personally uncharted territory and experiment at practise sessions. This majority is necessarily complemented by a dedicated set of committee members from Systems Security Lab (S2Lab), who direct the CTF practice sessions and make executive decisions during live competitions.

In the recent months, the CTF team has made its debut on multiple computer security scenes: RHUL's team achieved the spot of "top UK team" (and top 1% globally) at a 2-day CTF competition hosted in Beijing, China, which attracted thousands of security-savvy whitehats. The RHUL team also recently came 2nd out of all participating UK teams in a 36-hour Swiss-based CTF event. Teams from nation states of geopolitical interest to the UK, which are thought to be actively, but silently pursuing cyber-warfare capabilities, including the United States, China and Russia, are routinely present and often top ranking.

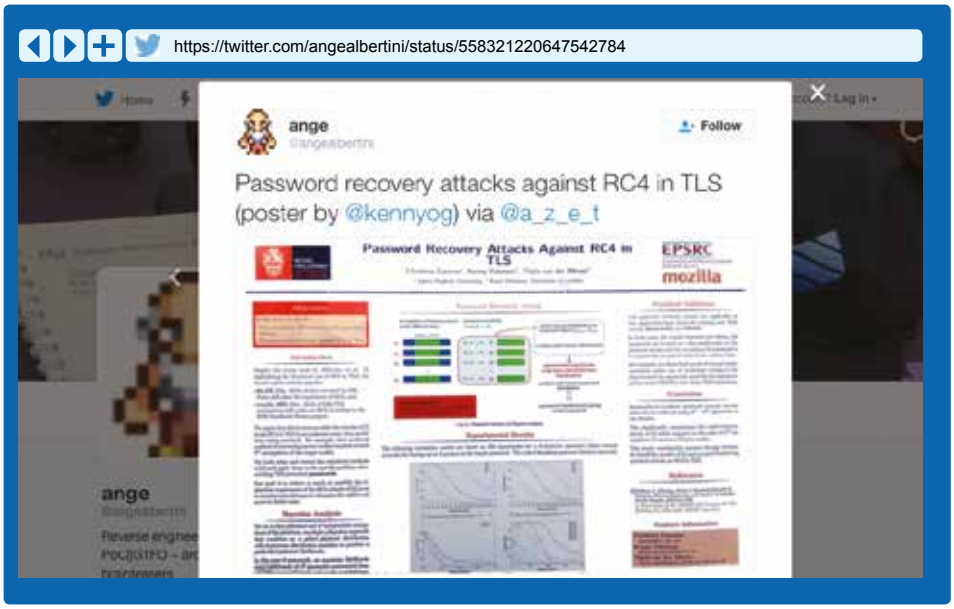
The format and technical nature of CTF jeopardy challenges (as opposed to an attack/defense model) bears a strong resemblance to puzzles that the 1st generation of RHUL's Centre for Doctoral Training (CDT) students produced for the UK-wide Universally Challenged competition. The CDT's entrant team, namely "Alice in Wonderland", won 2nd prize for designing a multi-layered set of program analysis and cryptography puzzles, closely following the theme of Lewis Carroll's famous book. It required opponent teams to conduct steganalysis, crack substitution and stream ciphers, and overcome a program's obfuscation and anti-debugging tricks.

A delegation from RHUL's CTF team has also recently competed in a one-day cyber security event run by Deloitte in London, UK. After fierce rounds of mixed challenges from the forensics, crypto, binary reverse engineering and web-security categories, the team successfully claimed overall 2nd place, beating several other of the UK's ACE-CSR universities in the process. RHUL is one of 13 currently accredited Academic Centres of Excellence in Cyber Security Research (ACE-CSR) and has a GCHQ-certified Cyber Security MSc.

Apart from the archetypal CTF examples of exploiting buffer overflows under relaxed security conditions, the team on occasion leads detailed discussions of more real-world hands-on attacks. The subject matter may focus on both close-access and computer network-based methods, such as using magnetic-strip access devices, establishing rogue GSM (2G) mobile networks, lifting password hashes from physically-insecure machines, accessing IP-enabled camera systems for reconnaissance purposes, improving the stealth of command & control (C&C) techniques for software implants, delivering spear-phishing e-mails via SMTP spoofing or assessing the security of an organization's LDAP servers.

The likely future of CTF, however, lies not in the speed-typing of its human components (its hackers), but in their ability to formalize and mechanize an attack methodology, to scale it and operate successfully at computer speeds. The currently human-dominated CTF domain, perhaps reflecting the evolution of other real-world areas of computing, is becoming increasingly automated and less human-directed. DARPA has in the recent past invited the US academic community to engage in a machine-vs-machine CTF-like competition, depending solely upon automated program comprehension and its ability to generate proofs of program vulnerability. The Systems Security Lab (S2Lab) at RHUL actively conducts research into automated program analysis and exploitation.

The CTF team routinely publishes a schedule of planned events, which includes upcoming participation in local face-to-face or world-wide online competitions, with the latter commonly taking place on weekends on a bi-weekly or monthly basis. In the temporary absence of global competitions, team members present walkthroughs of intriguing and previously-solved challenges that captured their attention in particular. Members of the team currently meet in McCrea 128 (the CDT "clubhouse") every Tuesday at 6pm. There is an existing pool of volunteer speakers lined up from RHUL's student and research community, standing by to give 20-30min theoretical, but practically-applicable talks on CTF-relevant topics. We look forward to seeing you there!



Poster appears on Twitter

RC4 IN TLS – SO WHAT HAPPENED NEXT?

Prof. Kenny Paterson

> Professor of Information Security, ISG

Back in the 2013/14 edition of the ISG newsletter, Jacob Schuldt gave a comprehensive account of our 2013 research into the insecurity of the RC4 encryption algorithm when used in the TLS protocol (details here: http://isg.rhul.ac.uk/tls/). Curious readers may be wondering: so what happened next? Did the world pay attention? Did anything change?

Two years later, things have changed -- and quite dramatically.

In early 2013, figures from the ICSI Certificate Notary (https://notary.icsi.berkeley.edu/) indicated that roughly 50% of TLS connections were using the RC4 algorithm. This figure is suspected to have actually increased after the 2011 BEAST attacks on the alternative CBC-mode ciphersuites in SSL 3.0 and TLS 1.0, which were the most widely deployed protocol versions at the time. Today, in March 2016, the corresponding figure from the ICSI Certificate Notary is 2.4%, representing a substantial improvement in the security of TLS in practice.

So how did we get from there to here? It didn't happen purely by accident.

What follows is a timeline explaining the major influences along the way; after this, we'll reflect on what we've seen during this process.

August 2013: Andrei Popov of Microsoft produced the first draft of an Internet document deprecating the use of RC4 in TLS (see https://tools.ietf.org/html/draft-popov-tls-prohibiting-rc4-00)

October 2013: The influential SSL Pulse website (https://www.trustworthyinternet.org/ssl-pulse/) started to track RC4 support on servers, reporting that 93% of the roughly 150k sites surveyed supported the RC4 algorithm. SSL Pulse chose not to penalise sites for supporting RC4 at this stage, due to the poor availability of better options (at this time, mainstream browsers did not yet support TLS 1.2 with its AES-GCM algorithm).

Summer 2014: After the initial publicity surrounding our 2013 paper, the figure for RC4 traffic had dropped, reaching about 35%. We started work on a follow-up paper focussing on the recovery of passwords encrypted under RC4 in TLS. "We" here included Christina Garman, a visiting PhD student from Johns Hopkins University in the US with sponsorship from Mozilla, and Thyla van der Merwe, a PhD student with Royal Holloway's Centre for Doctoral Training in Cyber Security. Our aim in this follow-up work was to illustrate the truism that "attacks only get better", and to push RC4 further towards being obsolete in an effort to reduce the 35% figure. We combined some statistical tricks, several thousand core-hours of computation (donated by our sponsors WhiteOps and Google), and the exploitation of peculiarities of Internet protocols like BasicAuth and IMAP that repeatedly transmit user passwords. The end result: by the end of the year, we were able to reduce the number of encryptions needed to recover useful plaintext from the 2^34 initially needed down to about 2^26, and the running time of the attack from an estimated 2000 hours down to a couple of hundred hours. We argued that this brought the attacks to the verge of being practical.

December 2014: SSL Pulse started to cap servers supporting RC4 at a grade of "B".

January 2015: Social media then played a starring role. Thyla presented a poster on our recently-completed work at the Real World Crypto conference in London in early January; a blurry photo of this poster made its way onto Twitter (see Figure 1); then the rumours started to fly. In mid-January, Itsik Mantin, who had studied RC4 closely in the early 2000's along with Adi Shamir, brushed off one of his old research ideas and announced the "Bar Mitzvah" attack, so-called because it relied on a "13 year old weakness in RC4". This attack turned out, when finally published in March, to be less powerful than the 2013 attacks. However it received a lot of press attention, further increasing the pressure on RC4.

February 2015: The Twitter photo from Thyla's poster was used in a blogpost from CloudFlare, a major Content Delivery Network (CDN) and website hosting provider, explaining that they were rapidly retiring RC4 because of "whispers of another, easier attack on RC4 in the academic community" (see https://blog.cloudflare.com/end-of-the-road-for-rc4/). Also in this month, the IETF finally published RFC 7465 ("Prohibiting RC4 ciphersuites"), containing the stark message "RC4 can no longer be seen as providing a sufficient level of security for TLS sessions" and citing our 2013 research paper to back this up.

March 2015: We made our new research paper available (see http://www.isg.rhul.ac.uk/tls/RC4mustdie.html), just ahead of Mantin's BlackHat Asia presentation of his Bar Mitzvah attack. Cue more coverage in the technical press, reporting that RC4 was past due for retirement.

April 2015: SSL pulse announced plans to more harshly penalise servers supporting RC4 (see https://blog.ivanristic.com/2015/04/ssl-labs-rc4-deprecaton-plan.html).

July 2015: Another blow for RC4 came in new research from Mathy Vanhoef and Frank Piessens from KU Leuven. Their work exploited a different set of biases in RC4 compared to our work, the Mantin biases. These had been discovered by Itsik Mantin in the mid-2000s, and had been used by researchers previously in attacks on RC4. However, using these in a more systematic way, Vanhoef and Piessens were able to mount an HTTPS cookie recovery attack requiring around 2^30 encryptions and needing roughly 75 hours to mount the attack (see http://www.rc4nomore.com). Their attack needed more encryptions than our latest attack, because of the weaker biases being used. But the new attack was faster to execute,

since it was able to run in a single TLS connection and therefore did not incur the connection establishment cost of our attack. Crucially, Vanhoef and Piessens built a working demo of their attack, showing that it was no longer a theoretical possibility but now a realistic prospect.

August 2015: The Vanhoef-Piessens work and our paper were presented back-to-back at the USENIX Security Symposium. A video of Thyla's talk is available here: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/garman . At the very end of the video, Ron Rivest, the designer of RC4, can be heard saying "I support your call to stop its use. It's about time. It's an old cipher now". By this time, with all the publicity and the IETF deprecation, RC4 usage had dropped to around 13% of all TLS connections.

September 2015: Google, Microsoft, and Mozilla, in a coordinated series of press releases, announced that they would be completely removing support for RC4 in their web browsers in early 2016.

January 2015: Google removed RC4 from the Chrome browser in version 48. More than 1 billion users are then fully protected. Mozilla removed RC4 from Firefox in version 44 and another few hundred million users are fully protected. Recent versions of Microsoft Internet Explorer and Edge now only use RC4 in fallback connections (and support will be removed even there from April 2016). Apple's Safari browser still uses RC4, but only with the lowest priority. We (Remi Bricout, Sean Murphy, Kenny Paterson and Thyla van der Merwe) released a research paper, independently confirming the results of the Vanhoef-Piessens work and providing a firm theoretical foundation for the cryptanalysis of RC4 using the Mantin biases (see http://eprint.iacr.org/2016/063).

This brings us almost to today. Our initial work in 2013, combined with the follow-up work by us and others, spurred the community to make a major change in the way TLS is deployed on the Internet. Today, the ICSI Certificate Notary reports that just 2.4% of TLS connections are protected using RC4, while SSL Pulse shows only 8.5% of the servers surveyed still offer RC4 for TLS 1.2, where better encryption options are available.

Because of the prevalence of legacy browsers and badly configured websites, getting rid of the last 2.4% of RC4-protected TLS connections may still take years. For example, theSSL Pulse survey shows that a few dozen of the surveyed websites still support only RC4 ciphersuites. And beyond the web environment, there is evidence that RC4 is still a popular choice when configuring TLS clients and servers, for example protecting e-mail traffic.

As part of the shift away from RC4 in TLS, TLS 1.2 has become much more widely deployed. TLS 1.2 has been supported in all the mainstream browsers since early 2014, the number of websites supporting TLS 1.2 rose from 11% in 2013 to 74% today, and more than half of TLS traffic is now protected using AES-GCM and TLS 1.2 (with AES in CBC mode being the second most popular choice). Another major development is the decision of the IETF to start work on TLS 1.3. Amongst many other improvements, this new version removes support for RC4 and CBC-mode ciphersuites from TLS altogether. RHUL Centre for Doctoral Training in Cyber Security PhD students Sam Scott and Thyla van der Merwe have played a critical role in the development process for TLS 1.3, working with Cas Cremers and Marko Horvat from the University of Oxford to produce a detailed security analysis of the draft TLS 1.3 protocol (you can read about their work here: http://tls13tamarin.github.io/TLS13Tamarin/).

We are very proud of our work analysing the security of RC4 in TLS. By breaking the algorithm once, then breaking it again (and more severely than before), we gave a clear illustration that the algorithm's days in TLS were numbered. Coupled with careful communication of the results to key players in the industry, this helped create the momentum the industry needed to move away from the algorithm. Our approach has ensured that the research has had a huge positive impact on the security of communications on the Internet: literally billions of users are now using stronger cryptography because of it.

THE FIRST ISG OPEN DAY: JUNE 16

We are proud to announce that on Wednesday 22nd June 2016 we will be holding our first ISG Open Day.

The Open Day is designed to showcase all that we do here in our world leading Information Security department. The day will consist of various activities including presentations from current research students, exhibitions and demos, talks from ISG staff and keynote lectures from exciting guest speakers.

Tickets are free but registration is essential via Eventbrite eventbrite.co.uk/e/isg-open-day-2016-tickets-21258962128

The programme for the day will be interesting and varied. There will be three keynote speakers, short "soundbite" presentations and a talk from a representative of CrossFyre about "Women in Crypto". Each room will have its own individual theme such as cryptography, the Smart Card Centre, the Systems Security Lab, "vintage" computers, PhD poster presentations, and "creative securities". Information about the Information Security MSc and MSc Alumni activities will be on display, along with content from our multidisciplinary partners within the college.

The day will finish with a panel discussion about security issues in the Internet of Things, to be chaired by Robert Carolina.

The three distinguished keynote speakers are:

Keynote Speaker 1:
Professor Mike Edmunds
(Cardiff University)
Title: *Unlocking Aphrodite's Secrets: The Antikythera Mechanism and its legacy*

Keynote Speaker 2:
Dr Joel Greenberg
Title: *Bletchley Park and the Industrialisation of Signals Intelligence*

Keynote Speaker 3:
Ken Munro: (PenTest Partners)
Title: *The IoT. Your very own Wi-Fi controlled and App enabled Armageddon*

We are very grateful to our sponsors – GSK, KPMG, Royal Holloway Enterprise and Thales - who help to make this day possible.

The Open Day webpage will be updated with further information as it becomes available https://www.royalholloway.ac.uk/isg/open-day-2016/open-day-2016.aspx

For more information contact:
Prof. Konstantinos Markantonakis
k.markantonakis@rhul.ac.uk
Michelle Gates
michelle.gates@rhul.ac.uk

CENTRE FOR DOCTORAL TRAINING IN CYBER SECURITY

Prof. Carlos Cid

> Director of Royal Holloway's Centre for Doctoral Training in Cyber Security

It is hard to believe, but Royal Holloway's CDT in Cyber Security is celebrating three years! Since its launch in April 2013, we have recruited 30 students, who are now working on a wide range of research topics, including software security, cybercrime, cryptography and geopolitics of security. Setting up and running the CDT in these past three years have been demanding tasks, but also truly rewarding. The CDT has been a huge success! It has without doubt greatly enhanced the research environment at Royal Holloway. It has also opened several new opportunities for business engagement, and feedback from our external partners in industry and government indicates the great value of the CDT to them.

The establishment of the Centres for Doctoral Training in Cyber Security was one of a number of initiatives supported by the UK Government as part of the National Cyber Security Strategy, published in November 2011, which had as one of its fundamental goals to develop in the UK the "cross-cutting knowledge, skills and capability" required to support all other cyber security objectives. The UK has been a leader in engaging players from industry, government and academia to create a vibrant and innovative cyber security sector. We are confident that, despite its early age, our CDT has been making a small but noteworthy contribution to this effort.

If in 2011 it was already recognised the crucial importance of cyber security to modern society, this is even more pronounced today. Cyber Security is now frequently featured as front-page news, from reports about high-profile data breaches at UK businesses to the rise of economically-driven cybercrime to the essential debate on the use of encryption to protect digital communication. Citizens can no longer ignore cyber security in our ever-increasing networked world; it will remain a critical aspect of our society in the years to come, particularly with the expected adoption of ubiquitous computing and IoT devices. The need for professionals with leadership and critical thinking skills – in addition to the more conventional 'technical' skills – will be even more pronounced. We are convinced that our CDT students truly have the potential to become leaders in their fields.

In the past three years we have been working diligently with our partners in the industry and government to provide the students with a well-rounded education in cyber security, and develop their specialist skills in an area of the utmost importance to society. Students in all three cohorts have been kept very busy, and the results are exceptional.

We are expecting the new National Cyber Security Strategy to be published later this year, with cyber security remaining a top priority for the UK Government. With its many challenges and opportunities, cyber security continues to be a very exciting field to work on. The CDTs in Cyber Security present an exceptional opportunity for some of the country's best minds to be actively involved in cyber security academic research and education. We are looking forward to continuing to work with our partners in industry and government in training the next generation of leaders in cyber security.

CDT RESEARCH NEWSBITES

Conrad Williams was a co-author of *Obligations in PTaCL*, which was presented at the 11th International Workshop on Security and Trust Management, in Vienna, Austria, in September 2015.

Pip Thornton's paper *Diary of a Plastic Soldier* was published in the journal "Critical Military Studies" in March 2016.

Giovanni Cherubin was a co-author of the paper *Hidden Markov Models with Confidence*, which he presented at the 5th Symposium on Conformal and Probabilistic Prediction with Applications (COPA), in Madrid in April 2016.

Sam Scott and Thyla van der Merwe had their paper (co-authored with collaborators from the University of Oxford) *Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication accepted at the 2016 IEEE Symposium on Security and Privacy,* one of the world's top-ranked annual security conferences, which will be held in May 2016 in San Jose, USA.

Robert Lee and co-authors from RHUL had their paper *Binding Hardware and Software to Prevent Firmware Modification and Device Counterfeiting* accepted at the 2nd ACM Cyber-Physical System Security Workshop (CPSS 2016). Rob will present their work at the workshop in China in May 2016.

Suleman Ibrahim will be presenting his paper *Socioeconomic Cybercrime Theory of Nigerian Cybercriminals* at the 4th International Conference on Cybercrime and Computer Forensics (ICCCF 2016) in June 2016 in Vancouver, Canada.

THE SYSTEMS SECURITY RESEARCH LAB

Dr Lorenzo Cavallaro

> Reader in Information Security

The Systems Security Research Lab (S2Lab) was established in Sep 2014 within the Information Security Group at Royal Holloway, University of London. The lab focuses on devising novel techniques to protect systems from a broad range of threats, including those perpetrated by malicious software (malware) locally and over the Internet. Its ultimate aim is to build on machine learning and program analysis to consolidate understanding on well-established systems security research topics and explore novel directions to build practical tools and provide security services to the community at large.

Although we are still in a bootstrapping phase, this has been a very thriving period for the lab, and its members—one of which has successfully defended her PhD in Apr 2016—have been involved in a number of activities, including those aimed to promote and disseminate the lab's research outputs through presentations (e.g., keynote at OWASP AppSec EU 2014, several invited seminars at academic institutions and industry), publications in top computer security venues (e.g., NDSS 2015 and MoST 2016), program committee memberships for well-established forums (e.g., ACM CCS, ACSAC, DFRWS, USENIX WOOT), hosting conferences (e.g., DIMVA 2014 and ESSoS 2016), hosting visiting scholars (e.g., from TU Milan, University of Cagliari, University of Granada, and TU Munich), and foster further collaborations with industry (e.g., McAfee at Intel Security) and academic institutions (e.g., NUS, University of Luxembourg, University of Cagliari, University of Granada, TU Munich, UCL, TU Milan, and University of Milan).

We have been refining the line of research carried out in the lab and, although there is always appetite to broaden our scope, we have been primarily busy working on the following topics (up-to-date information is available at http://s2lab.isg.rhul.ac.uk).

Automatic generation of exploit for heap (memory corruption) vulnerabilities—the automatic generation of heap exploits lays its foundation in symbolic execution, which requires the ability to reason about a program's possible execution paths. The underlying technique builds on symbolic execution to automatically reason about heap managers' internal state and conditions necessary to successfully create a working exploit [1].

Machine learning for malware analysis, classification, and detection—new malware variants are engineered everyday to perform a number of potentially evasive malicious tasks. In this setting, there is a need for automated learning-based approaches that use machine learning (ML) to understand and classify the behaviour of malware. For instance, this enables classification of malware into families, which in turn ease mitigation by devising techniques that are robust against entire families with similar behaviour.

Classification of malware into families consists of extracting features and mapping them into feature vectors. For a given malware, we extract several features that we pre-process to have a suitable format that can be used in ML algorithms. We use several methods to reduce the dimensionality of the extracted features such as (but not limited to) Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and t-Distributed Stochastic Neighbour Embedding (t-SNE). Currently, in addition to these approaches, we are working on developing robust classification techniques that are resilient against proximity errors during classification. In particular, we have been working on conformal evaluator—a novel technique inspired by conformal predictors [2]—that quantifies common errors for machine learning algorithms, with (statistical) confidence [3]. The benefits of our approach lie in its application to detection and classification of botnets and Android malware. We already have an in-house framework for classifying botnets and a sandbox for extracting features for Android malware called CopperDroid. In particular, CopperDroid, has received significant recognition recently with the work being published at a premier venue, early on, this year [4] (preliminary results on Android malware classification are available in [5]).

Our experiments are becoming increasingly complex due to the polymorphic nature of malware that we are dealing with. ML algorithms are notoriously computationally intensive as they try out combinations of different features in order to test whether samples fit into a family. What further exacerbates the situation is that we are witnessing new variants of existing malware, which means either newer features or newer families altogether forcing existing classification techniques to retrain. This creates an unprecedented need for computing power and the need to parallelise the task of classification in order to speed it up.

We have already secured funding (EP/K033344/1 and EP/L022710/1) to support S2Lab's main research directions and an additional grant from GCHQ helped further in increasing our computational power. Our current results (luckily) outgrow our initial expectation and the additional equipment allows us to keep up with the pace of our analyses. Not only this plays a crucial role in proximity of deadlines (where we have to extensively time share our equipment across projects, with the risk of jeopardizing the submission if experimental results are late), but it also supports our capacity to further disseminate the output of our research, engage further with industry partners (McAfee Labs is project partner on EP/L022710/1, we have ongoing relationships with HP Enterprise and HP Inc., and we have started conversation with Google's Android security team, and Qualcomm Android security R&D), thus contributing to raise further the international profile of S2Lab's systems security research.

[1] http://s2lab.isg.rhul.ac.uk/c1f1455827d8384519e8ae065d31ad55/aeg.pdf

[2] Vovk, V.; Gammerman, A.; Shafter, G.; "Algorithmic Learning in a Random World", Book, 2005

[3] http://s2lab.isg.rhul.ac.uk/c1f1455827d8384519e8ae065d31ad55/ce.pdf

[4] http://s2lab.isg.rhul.ac.uk/papers/files/ndss2015.pdf

[5] http://s2lab.isg.rhul.ac.uk/c1f1455827d8384519e8ae065d31ad55/most16-droidscribe.pdf

AN UPDATE FROM THE ISG SMART CARD CENTRE

Prof. Konstantinos Markantonakis

> Director of the ISG Smart Card Centre

The year 2015 was a very eventful one for the ISG Smart Card Centre (SCC). Prof. Keith Mayes, the founding director of the SCC, became the new ISG Head of Department. Keith played an instrumental role in leading the development of the SCC as a worldwide centre of excellence in the fields of smart cards, tokens, security and applications. As a result this is the first, hopefully out of many more to follow, SCC update for the ISG Newsletter in my capacity as the new director of the SCC. I would like to congratulate Keith for his achievement and thank him for his continuing support. The task of ensuring the successful day-to-day operation of the SCC is demanding, but I am confident that capitalising further on our well established areas of research, along with expansion into related new areas, will make for an exciting future.

Anyone who has followed the history of the SCC will know that we have been very active in smart cards, SIMs, RFIDs, attacks, protocols, transport ticketing security and payment systems. However, we currently supervise 12 PhD students within the SCC with additional diverse research interests, including automotive security, secure software and hardware binding in embedded systems, refined mobile access control and ambient sensors, firmware updates for embedded devices, secure elements, location proximity, and Internet-of-Things (IoTs). The SCC continues to supervise 20 MSc students, in relevant topics, in any one academic year.

All these research activities justify further the expansion of the SCC activities into the wider spectrum of devices and embedded systems that might be considered the IoT. Therefore, there is a strategic intention to amend the external name of the SCC (with a subtitle - as the SCC is already well established) to become the Smart Card and IoT Security Centre.

In July 2016 we will reach the end of the 30 months of the Secure Avionic Wireless Networks (SHAWN) project funded by the Technology Strategy Board (TSB) and EPSRC. This is a collaborative project that includes General Electric (GE) Avionics, Critical Software, HW Communications and the University of Strathclyde. The ISG SCC is acting as the information security authority and is responsible for providing a secure and reliable security assessment of replacing wired avionics network with wireless alternatives. The project is very successful with GE leading the discussions with major players in the industry for follow up commercial initiatives. Much of the success of the SCC's involvement in the project can be attributed to Dr Raja Naeem Akram who was funded by the project. Raja's contributions surpassed expectations and he helped win the best paper award (for the security session) at a top avionics conference – 34th DASC 2015, as well as having two papers accepted for publication at IEEE I-CNS, and three in review for 35th DASC 2016. He is also leading the development of the SCC project demonstrator (in addition to the of the main project demonstrator) to be ready for our ISG Open Day on the 22nd of June 2016.

After the successful conclusion of the SHAWN project we will turn our attention to the newly funded three year EPSRC project on "Improving customer experience while ensuring data privacy for intelligent mobility", worth £280K to RHUL. This is a joint effort between the Universities of Surrey, Southampton, Loughborough and ourselves. Our PhD students are also busy, with a notable contribution from Danushka Jayasinghe, identifying a potential loophole in the online PIN verification process that was then published in IEEE TrustCom 2015. Further research work involved Raja Naeem Akram, Iakovos Gurulian and Carlton Shepherd investigating the effectiveness and reliability of ambient sensors as anti-relay mechanisms for mobile phone-based point-of-sales payments, currently under review in a major academic conference. Assad Umar published his work on the use of Host Card Emulation (HCE) in transport ticketing systems. We must also congratulate Dr Mehari Gebrehaweriya Msgna, who successfully completed his PhD thesis on "Platform Verification and Secure Program Execution on Embedded Devices".

It is also good to see a continuation of collaboration and publication efforts with past visiting researchers to the SCC, including Damien Sauveron from University of Limoges, and with the University of Bordeaux on RFID protocols and security issues in Unmanned Aerial Vehicle (UAV) platforms. We have already a published a paper in TrustCom 2015 on RFID protocols and a journal version of this paper is ready for submission in April 2016. We also have a paper on security issues and how embedded devices can protect UAV communication/operations is under review in 35th DASC 2016 conference.

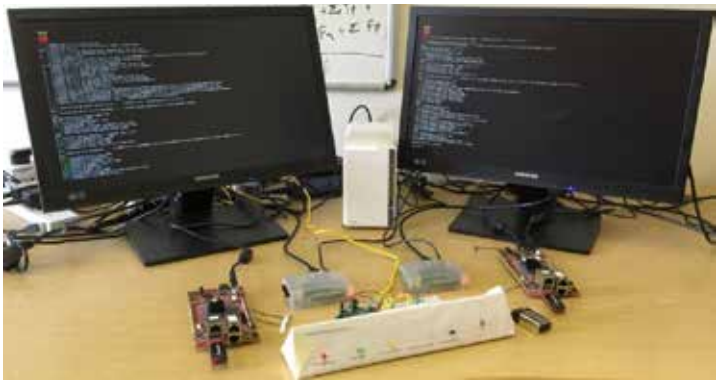
The SCC staff/PhD research activity has so far generated more than 140 published papers in international conferences and journals with 12 papers in 2015 (www.scc.rhul.ac.uk/publications.php). Notable publications can be found in ESORICS, ACM CCS, ACSAC, ACM TISSEC, TRUSTCOM, CARDIS, IFIP SEC and Elsevier's Information Sciences Journal. In 2008 Prof Keith Mayes and I edited, what has proven to be one of the most widely utilised smart card text books, "Smart Cards, Tokens, Security and Applications", published by Springer. The second edition is due to be published in autumn 2016.

The general philosophy of the SCC is inherited from ISG's motto "Academia and Industry in Harmony". SCC 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 has committed to another three years support for the SCC. Furthermore, the UK Cards Association has also extended its support. Of course in these belt-tightening times we are keen to hear from other organisations that can help us to continue research work that we expect to have real world impact. An example of such work is the SCC led sequence of expert studies on payment authentication for the UK Cards Association. The studies have addressed attacks and countermeasures for current chip & PIN cards and the evolution of security protocols and technologies that will impact how we will all pay for things in future. The work has been led by Dr Konstantinos Markantonakis and the ISG expert team included Professor Keith Mayes, Professor Fred Piper, Professor Keith Martin, and Dr Geraint Price.

The SCC celebrated its 13th anniversary on the 2nd September 2015. Exhibiting at the Open-Day were 14 industry exhibitors and 20 SCC students, and they were joined by record numbers of visitors. The Crisp event prizes went to PhD student Iakovos Gurulian for his poster Consumer-Centric Android Application Repackaging Detection and to MULTOS for its personalisation and control demos for apps, smart meters and cars. A special prize in memory of Stuart Atwood was awarded by MULTOS to MSc student Shreya Singh for her work on Secure Authentication in Vehicular Ad Hoc Networks (VANET). There were a number of short industry presentations showing the real world relevance of the SCC research area and training activities, rounded off by a guest lecture from Professor Sujeet Shenoi of the University of Tulsa, USA. The event was supported by the current SCC sponsors; Transport for London, the UK Cards Association and ITSO as well as event sponsors; Comprion, MULTOS, OpenSky, PA Consulting Group, Safran (Morpho) and Underwriters Laboratory.

The SCC is currently leading the organisation of our 5th Information Security Group (ISG) Alumni Conference and, on 22nd June, our 1st ISG Open Day. These events aim to showcase the breadth and depth of ISG research and teaching activities, and to strengthen and expand the wider ISG community. As a result there will not be an SCC Open Day in September 2016, but it will make a return in September 2017.

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.



SCC Open Day 2015

LEGO modelling of services and security: an example of a creative security technique

CREATIVE SECURITIES: THE CITIZEN, GOVERNMENT AND ACADEMIA

Prof. Lizzie Coles-Kemp

> Professor of Information Security

The ISG is best known for its work in computer and network security and cryptography. The ISG trailblazed cryptographic innovation and its leadership had the vision to create a world-leading masters programme.

However, another ISG story of innovation is emerging. Increasingly it is understood that information security sits within a wider security context. This context can be described as the safety-security nexus where safety is necessary for security and security is necessary for safety. Put simply, if people feel safe, then they are more likely to engage with digital services – whether as citizens accessing public services or as employees providing those services. In the case of digital public services, a sense of safety enables citizens to engage with online services free from fear of attack and this sense of safety is in part engendered through the protection mechanisms in the service but also through a person's relationship with the institution. A sense of safety is also engendered through the sharing of information about the security of the service within a person's kin and friendship networks.

Over the last few years, I have led a number of projects that have looked at the safety-security nexus and we have written about these projects in previous ISG reviews. The work from these projects has shown that where information security mechanisms are perceived as contributing to a person's safety and security, then the service security mechanisms are more likely to be complied with; where the services are perceived as threatening a person's safety and security, then the security mechanisms are more likely to be circumnavigated.

There are several securities at work when thinking about service design in this way. Information security from the safety-security nexus perspective is not only about protection from threat but also freedom to engage with on-line services. People need both forms of security to go about their everyday lives. Scientists, designers and security practitioners are seeking this bigger picture of security as a matter of some urgency in order to address some of the more challenging issues related to digital service management and design.

Since 2008, the ISG has been home to a creative security practice set-up to uncover hidden patterns of information sharing and protection that sit at the heart of the safety-security nexus. A creative security practice takes an anthropological approach to design and has story-telling techniques at its core. It uses a range of art practices to engage with communities to uncover their information sharing and protection stories. Such an approach helps us to more accurately characterise the real-world problem space, understand why those problems come into being and design new technologies, methods and services to respond to those problems.

In our research, a creative security approach has been most effectively used to uncover shadow practices of information sharing and protection. These are the unofficial practices that come into being to overcome shortcomings in the technology, difficulties with policies or respond to the complexities of everyday service delivery. The aim is not to stamp out such practices as they are often the life-blood of an organisation (the glue between systems supporting everyday practices) but to work with such practices to more widely support the safety-security nexus in the workplace. By bringing such practices into the light we are able to theorise about the roles different types of shadow practices play in the security of an organisation and learn lessons for future development of governance frameworks. The creative security approach is helping to transform attitudes by mapping different pathways to policy compliance and designing governance practices more compatible with the culture of different organisations.

The future for such work looks bright. Since 2008, the ISG has led four projects working in this area (both national and international) and has been part of a further two projects looking at information security from this perspective. One of these projects, CySeCa, was part of the UK's national Research Institute for the Science of Cyber Security (RISCS) and I am delighted that the ISG will continue to be an active member of this research institute in its next phase. To date, the techniques and tools that we have designed in these projects have been taken up across industry and government both in the UK and in Australia. This work is set to continue; I have recently been awarded an EPSRC fellowship to develop these ideas further over the next five years and embed the ideas into public service design philosophy. This is a huge privilege and a significant challenge – but a challenge that I am looking forward to!

SECURITY BREACHES ARE HIGH – IS IT TIME TO RE-THINK RISK ASSESSMENT?

John Austen

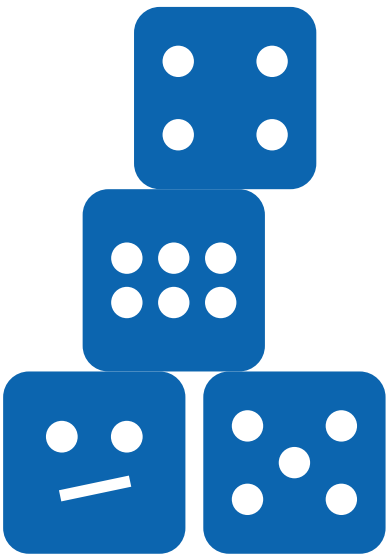
> Consultant Lecturer, ISG

By the time that you are reading this the latest Information Security Breaches Survey of 2016 will have arrived. If we were looking for good news it would probably be a search in vain as, historically, these reports make distressing reading, particularly regarding cyber crime. But, in terms of our strategies & security policies, what do they tell us? And probably more to the point, how will they affect the way we can look forward? One chilling statement from the 2015 review was that for large businesses "it is a near certainty that they will suffer a security breach" (90% was the figure given.). Perhaps it is time to re-assess the balances that constitute Risk Assessment. Whichever format is followed, (invariably from one of the standards) Risk to an Information Asset is described and analysed as a factor of a 'Threat' to 'Vulnerability'.

Survey reports have been with us for quite a few years. I remember the Audit Commission Reports from 1982 – a similar style of survey but named Computer Fraud & Abuse, and these continued bi-annually for many years until replaced by the DTI & PWC reports. The difficulty with ALL surveys is that they end up with producing statistics & figures, some of which we remember, but most are instantly forgotten. However the trick (a very unscientific word) in utilising these numbers involves comparisons with previous surveys and identifying trends. So here is my take on the trends. If one looks back through fairly recent times, then the primary efforts have concentrated on boosting up the vulnerabilities of assets, and we can see that by a comparison to the Survey of 2004 to that published last year (2015). In 2004, 25% of businesses had a significant incident involving accidental systems failure or data corruption. In 2015 there was hardly any and it did not even get a mention. In 2004 only 33% of all organisations had an up and running security policy (although the larger businesses were better). Today a policy is more or less a de facto standard. In regard to viruses, they were still a significant issue in that a number were bypassing anti-virus (AV) software and targeting vulnerabilities in operating systems. Large businesses had one a week and each company in the UK had suffered a virus attack at least twice in a month, and 7% of businesses had no AV controls at all. Also, spam (although not an incident) was very disruptive. Today, malware is still an issue and a significant one at that. In 2015, malicious software was a cause of breaches to the extent of impacting 75% of large organisations and 60% of small ones – an identical figure to that of 2004, despite the fact that almost everybody is using AV controls and software. In looking at the Human Factor, twelve years ago only 10% of the security staff had any formal qualifications and although in-house security awareness training existed it tended to be a 'one-off'. Today the figures for ongoing training are at 72% and with the proliferation of University & commercial courses available, a formal qualification is usually a requirement to be hired and this is borne out by the 2015 statistics that 60% of businesses were confident that they had sufficient skills to manage their risks. This sounds fine and is a vast improvement shown on skills and skill sets. But hold on a minute; in the 2015 report 75% of large and 31% of small organisations suffered staff security breaches which was up from 58% and 22% respectively a year ago and to add to the woe, 50% of the worst breaches were caused by human error up from 31% in 2014. So an evaluation of all these reports through the years showed (with a few exceptions) improvement and effort had been made in addressing vulnerabilities – but the breaches are still at record levels. So this looks like a dilemma until one drills down into the facts a little. If these surveys were on one organisation, or even one type of organisation then none of the above issues would make any sense. But of course our commerce and industry is made up of different sectors and luckily the last survey mentioned that the one sector (and the only sector) that increased its spend on security was the telecoms sector and that sector increased its spend by double. And is it a coincidence (although not specifically highlighted in the reports) that the telecoms sector and those with a high web presence, like the on-line gambling sector were becoming the main targets for cyber crime activity? In other words we can re-address the question to a relationship between targeted victims of crime and the efforts to combat it.

Which brings us back to point on the analysis of risk. If we ask ourselves the question "Has the information security industry improved over the years?" – then of course the answer is yes, and it is yes because nearly all known vulnerabilities have been addressed. We have improved training & awareness schemes and encouraged qualifications, devised better procedural controls, enhanced education in encryption and encryption techniques, developed smart card activity as a safe access procedure, coped with Bring Your Own Device (BYOD) and remote access, and patched up the operating systems.

So all the efforts have gone into addressing vulnerabilities – but in risk assessment this is only half of the equation. The other half relates to threats and despite all of the advances on the plus side we still end up with security breaches getting higher and higher and reaching a near certainty. The evidence indisputably shows that threats, particularly in cyber crime activity are a constant and it is unproductive to just describe threats as a may or maybe not. They need to be unpicked. At random, one week in February I counted eight new and different Trojans and two new and different exploit kits. To re-balance out equations in risk assessment requires an examination of intelligence gathering into threats by addressing real threats rather than perceived threats - and only then can we attempt to stop, or at least reduce this acceleration towards a 100% security breach level.



SECURING THE INTERNET OF (MEDICAL) THINGS

Dr Stephen Wolthusen

> Reader in Mathematics in the ISG

We have recently been awarded a grant to study problems of security, privacy, and information governance in the medical Internet of Things (IoT), which will provide support for two post-doctoral research assistants for the duration of the project. This grant is part of the Technology Integrated Health Management (TIHM) test bed funded jointly by NHS England and Innovate UK between 2016 and 2018 supporting a consortium including the University of Surrey, Royal Holloway, Surrey and Borders Partnership NHS Foundation Trust, the Kent Surrey Sussex Academic Health Science Network, Arquiva Ltd., and a further nine IoT technology providers.

The application domain problem we will address in the project is that of monitoring the health and need for intervention in patients' homes, particularly for those affected by early stages of dementia that may no longer be in a position to reliably assess their health care needs, and hence may result in delayed diagnoses and treatment including hospitalisation. Similar issues arise with elderly patients that may suffer from chronic conditions requiring consistent monitoring, or suffer acute traumata whilst unobserved such as falls resulting e.g. in hip fractures whose complications can frequently be life-threatening.

The overall project will seek to embed homes with a variety of diagnostic and monitoring equipment together with personal sensors. This will allow monitoring of both the quotidian state of health as well as the longer-term trajectory of patients in a more effective and reliable manner. Such sensor data can be collected, aggregated, and processed in part automatically so as to be able to alert carers and medical staff not only of isolated events, but also of more complex combinations of symptoms that might otherwise be missed. Importantly, the variety of different sensor data can also be aggregated and analysed automatically by fusing the results from these sensors and any ancillary information.

Whilst we anticipate that this effort will yield substantial benefits for patients in the form of more reliable, rapid, and targeted intervention and regular care, such monitoring and surveillance does of course bring with it a number of serious security and privacy concerns; the ISG is ensuring that this balance can be maintained. The deployment of sensors and surveillance IoT devices in patients' homes, particularly near-invisible IoT devices, gives rise to concerns about misuse, not only invading the privacy of patients, but also that of any carers, family members, or visitors who may not be in a position to give consent or even be aware of such monitoring. Such consent should, however, always be sought, particularly since it is possible that highly sensitive medical information is captured by such third parties or that sensitive private information is disclosed including over longer periods.

Beyond the problem of alerting to such instrumentation that is likely to arise in other domains such as Smart Homes or indeed Smart Cities, a number of security problems also must be addressed. These problems include, but are not limited to, the aggregation of data and controlling access depending on the role and circumstances (e.g. overriding controls for emergency access), which is made more challenging not only by the need to collect information from a distributed system via cloud-based services, but also because of consumers including hospitals, general practitioners, and caregivers where each may require access to different views and levels of detail.

A more specific problem in the IoT space arises from the environment in which such sensors must operate. Some, but not all may be regulated as medical devices - a category which also includes software with medical purposes - under the newly-revised European Medical Device Directive, international standards such as IEC 60601, 62304, and ISO 14971 and requirements for computerised system and corresponding UK legislation; these, however, are largely focused on product and patient safety and do not speak to security concerns. The project must therefore investigate not only how a suitable security architecture can be constructed that allows the secure deployment of IoT components including in patients' homes, but also ensures that interoperability issues among multiple vendors do not lead to problems such as downgrading of security mechanisms.

It is also likely that such components will need to be deployed in heterogeneous environments shared with untrusted devices and may be subjected to attacks that can call into question the reliability, potentially resulting in omitting the sending of measurements or alerts, or even maliciously misreporting readings. One aspect of the project is therefore aiming to identify mechanisms for ensuring and validating the integrity of IoT devices and networks of such components, which may also aid in identifying non-malicious faulty behaviour at the same time.

The project is to combine theoretical research with laboratory-based studies based in part at an IoT laboratory at the University of Surrey's 5G Innovation Centre as well as field tests, and will allow the collaboration of researchers, technology companies, and clinicians. At the same time this will strengthen the research capabilities in the Internet of Things we have in the ISG, together with links to closely-related research groups.

Managing Medical Device Information Security Risk

Nigel Stanley

> Practice Director – Cyber Security, TÜV Rheinland OpenSky

Medical devices, be they for glucose monitoring, heart defibrillation, blood pressure management or many other clinical purposes, have seen huge leaps in their capability. This has been fuelled by advances in materials technology, health analytic models, local processing power and the ubiquitous Internet to facilitate device communications. As medical device technology continues to evolve it is inevitable that more use will be made of commoditised hardware and software. Quite rightly, smartphones are increasingly used as the patient-to-device interface as they provide local processing power alongside an ability to connect to the Internet and transfer data back to hospitals, family doctors and researchers.

This boon to device usability and the patient experience comes with a downside – the ever increasing threat of device compromise, hacking and disruption. Although information security or cyber risk is a consideration in all industries, few could claim their risks have the direct and possibly fatal consequences of a compromised medical device.

Medical device risk

Medical devices contain complex electronics (often electromechanical) with supporting software or firmware. The latter is often used to control specific features of a device and will often be loaded directly onto a chipset. Historically firmware was rarely updatable, but manufacturers are now aware that updateable firmware makes a device easier to support and update against cyber related threats.

There are a large number of potential risks to medical devices, but more common examples include;

- Flawed or defective software and firmware. Writing software code that is free of security issues is very difficult. In many instances software developers have not been trained to write secure software and are unaware of the risks. In many cases the software has not undergone a test to check for security issues.
- Incorrectly configured network services. This could include the use of unencrypted connections to the Internet resulting in patient data being transmitted in plain/clear text. Attackers could take advantage of open network services and use them as an entry point on a device.
- Security and privacy issues such as the use of poor passwords or excessive permissions where a basic user can access administration features. It is not uncommon to see passwords written down and taped or stuck to the device. Passwords may also be “hard coded” in a device, making their retrieval by hackers simple.
- Poor data protection. This may occur due to the absence or poor use of data encryption. If used properly encryption is a powerful mechanism to protect data at rest and in transit (i.e. as it is being sent across a network). Many failures in data protection stem from incorrect use of encryption keys and poor technical implementations.
- Improper disposal or loss of the device with on-board memory still containing patient data. The secure destruction of the device needs to be factored into the cost of ownership and the disposal process documented and audited. People lose smartphones every day, but if such a device has patient sensitive data on it the medical device manufacturer could be subject to a regulatory investigation.
- Malware and spyware targeting medical devices. Hackers and cyber criminals look for the easiest return on their investment of time and money for each attack. Medical devices may not yet be subject to more general cyber-attacks, but targeted attacks for specific nefarious purposes must never be discounted.

Medical device hacking in practice

At the time of writing (February 2016), there have been very few medical device cyber-related hacks made public. Possibly the most significant hack was that involving the Hospira Symbiq Infusion System that culminated in a United States Food and Drug Administration (FDA) Safety Communication Alert in July 2015. Hospira and an independent cyber security researcher identified that the infusion system could be accessed through a hospital’s network that could, in turn, allow an unauthorised user to take control of the device and change the dosage delivered by the pump. Neither the FDA or Hospira were aware of such an incident occurring in a healthcare setting but the Symbiq Infusion System was withdrawn from sale, apparently due to unrelated issues. Concerns were raised that although the product had been removed from sale it could still be obtained from third parties. The Department of Homeland Security released a similar advisory. The flaws in the product were reported as including wireless, public and private keys being stored in plain text on the device, a lack of authorisation checking on the devices, and their vulnerability to either a denial of service attack or remote code execution.

Defending medical devices - system testing.

The technical testing of medical devices is a vital part of the device manufacturing process and helps manufacturers achieve a reasonable level of patient safety. During this process attack vectors, security-critical vulnerabilities and related architectural flaws will normally be discovered and then presented alongside remediation options and a clear understanding of any residual risk.

Typical system testing would include one or more of the following;

- Threat modelling to assess attack vectors unique to a product. This will help determine the best applicable security controls.
- Source code review - this will include a review of software code seeking defects. A penetration (pen) test can be undertaken to simulate an external hacking attack that assumes the hacker has no inside knowledge of the device beyond that which they can find out by probing the hardware or using information in the public domain. More usually the pen test will utilise information provided by the manufacturer including full source code and access to supporting documentation.
- Controls assessment – review of device security controls against appropriate standards including HIMSS/NEMA Standard HN 1-2013, Manufacturer Disclosure Statement for Medical Device Security (the MDS2 form)

Defending medical devices - corporate and end user cyber security

Once deployed into the clinical environment, device data will often traverse networks out of the device manufacturer’s control in places such as hospitals and clinics. Whilst subject to their own challenges and compliance requirements the clinical environment may have limited security resources and certainly their key concern will not be to focus on a specific manufacturer’s data security requirements. In practice it is probably better for a device manufacturer to consider the clinical IT environment as being the “Wild West” and apply their own technical controls rather than relying on those that may be in a hospital or clinic. For devices that are supplied to patients for use outside of the clinical environment, even more consideration needs to be applied to the cyber security challenges a medical device may face. This problem becomes more acute when considering a user may need to connect devices via their smartphones to medical device data services or similar. What measures have been put in place to educate and inform users how to protect their data? What controls have been implemented to manage a lost smartphone that may contain sensitive medical data? And finally, what measures have been put in place to adhere to legal and regulatory requirements for protecting patient data on its journey from the medical device, through the medical device data service and back to a manufacturer – in many cases in another legal jurisdiction?

CRYPTANALYSIS OF THE ALGEBRAIC ERASER

Prof. Simon Blackburn

> Professor of Pure Mathematics in the ISG

The Internet of Things (IoT) is a difficult place to implement security: computationally weak devices and strict constraints on cost and battery life mean that standard public key solutions such as elliptic curve Diffie—Hellman key exchange and RSA are often not suitable for IoT applications. So there is a pressure to adopt novel solutions that operate under these tight conditions. SecureRF, a U.S.-based company that has been around for about 10 years, markets (and owns the trademark to) one high-profile system for these constrained environments: the Algebraic Eraser.

Over the past few months I have been studying the security of the Algebraic Eraser. Working with Adi Ben Zvi and Boaz Tsaban from Bar Ilan University (Israel), the result is a cryptanalysis of the Algebraic Eraser key agreement primitive that recovers the shared key in under 8 hours of computation for parameters that are intended to provide 128-bit security. This is a very significant break: at 128-bit security levels it should be completely infeasible to recover this key. I have more recent results too, this time with Matt Robshaw (who many of you will know from his time as a lecturer in the ISG; in the past he has worked for RSA and France Telecom's Orange Labs, and is currently a Technical Fellow at Impinj). We concentrated on a protocol for RFID tag authentication that SecureRF have proposed for ISO standardisation. Exploiting an unfortunate interaction between the structure of the Algebraic Eraser and the structure of the protocol in which it was embedded, we managed to come up with real-time attacks that allow tag spoofing when this proposed standard is used.

All this work was a blend of academic cryptography with interaction with industry (the kind of thing the ISG provides such a good environment for), and with some beautiful pure mathematics. Let me provide some more detail and background to these results.

Most well-known public key cryptosystems (and certainly the schemes that are most widely used) are inspired by hard problems in number theory. However, cryptosystems inspired by problems in non-abelian group theory (an area of pure mathematics that comes from the algebraic study of symmetry) have been around for some time. The earliest group-theoretic cryptosystem I am aware of is due to Wagner and Magyarik in 1985, but the area became much more active after two beautiful proposals (by Ko, Lee, Cheon, Han, Kang and Park, and by Anshel, Anshel and Goldfeld) were published around 2000. The Algebraic Eraser is a group-theoretic cryptosystem, proposed in 2002 by Anshel, Anshel, Goldfeld and Lemieux.

I am currently a sceptic regarding group-theoretic cryptography: I think of new proposals as opportunities for cryptanalysis, rather than as new useful primitives to build on. Many proposals have been broken (and all the older proposals have all been affected by significant attacks). And many of the remaining systems have "security by underspecification": crucial details (such as parameter choices, and key generation methods) are missing, which makes a convincing security review difficult. Despite this, the field has had some lovely ideas which might just be a tweak away from practicality and security. So it is an interesting area to be involved with.

SecureRF have chosen to keep some crucial parts of parameter generation secret, but otherwise the Algebraic Eraser is a well-specified and concrete scheme. There are two classic ways of attacking a group theoretic cryptosystem: "length-based attacks", and "linearization". Both have been applied to the Algebraic Eraser. In 2009, Myasnikov and Ushakov mounted a length-based attack which meant that the suggested parameter sizes for the Algebraic Eraser had to be increased from their original values. At essentially the same time, Kalka, Teicher and Tsaban (KTT) independently mounted a clever attack combining linearization with an interesting use of a heuristic algorithm from the theory of permutation groups. Their attack works efficiently if parameters are chosen in a naïve way. But Goldfeld and Gunnells (from SecureRF) showed how parameters could be chosen in such a way that the KTT attack does not apply. So the early security reviews of the Algebraic Eraser were less positive than SecureRF would have liked, but the end result was a scheme that resisted known attacks.

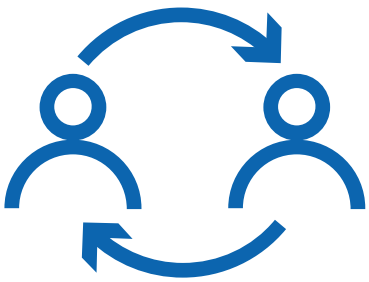
I first became interested in taking another look at the Algebraic Eraser when I heard that SecureRF had given a presentation to the Internet Research Task Force on their scheme, and that they had submitted an RFID authentication scheme for "ISO standardization".
I strongly believe that academic cryptographers should work to ensure that cryptosystems in their area that are close to deployment are subject to a robust security review! This is particularly important for IoT applications such as RFID tags, since it will be very hard to patch systems after deployment in many situations.

SecureRF kindly provided me with sample parameters of a type that would be used in practice. I asked two researchers from Bar Ilan University (Boaz Tsaban, who co-authored one of the previous attacks on the scheme, and his student Adi Ben Zvi) to join me; Adi visited Royal Holloway for some of last summer for discussions. By the early autumn we had a (non-optimised) implementation of an attack that recovered the shared key generated by the key agreement scheme (with purported 128-bit security) in under 8 hours. (Half of this time is a precomputation that only needs to be done once for each set of global parameters.) The attack uses the heuristic permutation group algorithms that form part of the KTT attack, but in a rather different way. The method also uses linearization in a novel way at two points. We informed SecureRF in case this caused problems with any deployed systems, and then published the work a few weeks later.

More recently, I collaborated with Matt Robshaw to study the proposed ISO RFID authentication proposal. We exploited some linearity in the protocol which meant that part of the tag's private key could be recovered after just 33 interactions with the tag. Techniques from the KTT attack and some novel uses of (rigorous, non-heuristic) permutation group algorithms were then enough to spoof the tag in real time.

I would not recommend using the Algebraic Eraser at present. Is there a future for the scheme? SecureRF have suggested a possible way forward: to massively increase certain parameter sizes, and then redesign the core primitive (introducing matrices that are not invertible at some point) to reduce the resulting cost penalties. There are no details as yet (not even parameter sizes) so it is far too early to say what the end result of this design process will be. I hope, both for the sake of the company and for the sake of the integrity of any resulting applications, that they are successful in their redesign.

If you are interested in reading technical details of the attacks (and know some group theory!) there are preprints linked from my home page. There is a good technical cryptographic discussion of the Algebraic Eraser on Cryptography Stack Exchange.
A recent article in Ars Technica by Dan Goodin ("Why Algebraic Eraser may be the riskiest cryptosystem you've never heard of") provides a very fair non-technical discussion, including some interesting comments from SecureRF.



ISG AND HUMAN GEOGRAPHY: AN INTER-DISCIPLINARY PARTNERSHIP

Klaus Dodds

> Professor of Geopolitics, Department of Geography, Politics, Development and Sustainability Group

One of the benefits of the EPSRC Centre for Doctoral Training in Cyber Security (CDT), hosted by the ISG, is the opportunity to work with colleagues across departments and faculties within the college. As a human geographer, working in geopolitics and security, I have the pleasure of supervising two PhD students (Andreas Haggman and Nick Robinson – more below) attached to the CDT and work closely with ISG colleague, Professor Keith Martin.

Inter-disciplinary supervision and collaboration more generally is not straightforward but it is rarely unrewarding in the sense that you have an opportunity to learn new conceptual approaches, scholarly languages and empirical areas that you may not have known even existed. Over our regular meetings, now stretching into their second year of occurrence, we have many engaging conversations about cyber-security, and how social science approaches can interweave with technical, computational and infrastructural expertise.

I asked Andreas recently how he thought his doctoral project on war-gaming and cyber-security was progressing and one of the things I was struck by was how working with an industry partner (a consultancy firm) and one of their clients (a petro-chemical company) had been incredibly instructive.

As Andreas reflected:

"In addition to theoretical elements bringing together geopolitics, cyber security, and ludology, the research also had a large practical part consisting of me making a prototype board game that modeled a cyber attack by a nation state on a private corporation. This work generated a lot of excitement in a number of different communities (war gaming, industry, government and military), which led me to decide to continue with this topic for my PhD thesis.

I now have buy-in from one IT industry partner who is interested in the research. Conversations are also ongoing with two defence contractors, one northern European defence establishment, and one East Asian industry corporation. My most significant coup, however, has been commitment from the UK defence establishment to partner with me and help bring my games to an appropriate audience".

As supervisors, we were very impressed how this summer-based project in year 1 has proven so productive for Andreas and been a springboard onto networking with a variety of stakeholders and a professional 'buy-in' for his project. For Andreas, his interest in war-gaming is not only theoretical (Why use war-gaming? How might we conceptualise war-gaming as discourse and practice?) but also practical and applied (How might companies learn from war-gaming? Can war-gaming encourage and inculcate cyber-security within organizations?).

What was also comforting to us as supervisors is that Andreas really appreciates our different disciplinary perspectives on war-gaming and cyber-security. As he noted, "By having input and guidance from both hard and social sciences, I feel extremely well-placed to bridge the divide between these two audiences. Tomorrow[1]s cyber security experts will need to not only have knowledge of the standards in cryptographic algorithms and networking protocols, but also an appreciation of the political, cultural and social environment into which these are implemented. The inter-disciplinarity offered by working in two departments puts me in a great position to fulfill this role".

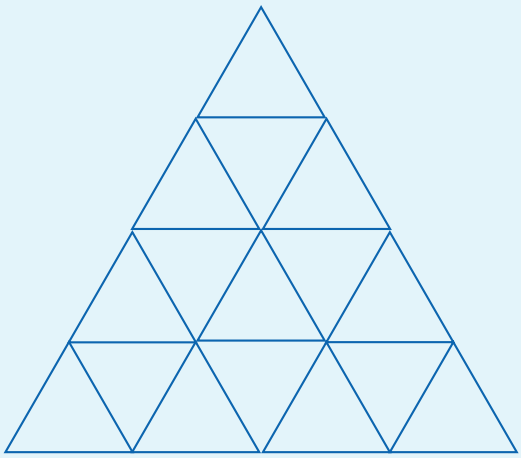
This confidence in the inter-disciplinary played a part in Andreas being invited to the Doctoral Symposium held at the UK Defence Academy last November. He participated in their 3 Minute Thesis competition a format that challenges students to summarise their research into a three-minute presentation aided by a solitary slide. Andreas won and we were very proud of his achievement.

Our other PhD student, Nick Robinson has just started his research. Nick graduated from Royal Holloway's masters course in Geopolitics and Security. It is worth noting that the CDT cohort participates in some of the teaching of this Masters program and in particular Principles of Geopolitics and Security. Through this exposure, Nick was introduced to the CDT cohort and this unquestionably inspired him to apply to the PhD program. Nick has an interest in Estonia and in particular their often-cited experience and expertise in cyber-security and cyber-defence and whether there are lessons to be learnt for the UK. As a first year student in the CDT, with a social science rather than a computer science background, Nick would be the first to admit it has at times been challenging. As he noted, "Given my background in Geopolitics and Security at Royal Holloway, my pathway into the ISG has perhaps differed slightly to years gone by - but starting the program with a focus on cryptography, network and computer security, and security management has been both refreshing and challenging. What's more, I've been presented with an opportunity to broaden my interests, of which I'm sure my future research will benefit from".

As part of the training year within the CDT, Nick participated in an array of cyber-related seminars, workshops, and conferences. He has continued to participate and assist in the teaching of the Geopolitics and Security MSc (co-editing the group blog and assisting in student activities) but also participate in other events such as the Royal Geographical Society's Postgraduate Forum in March 2016. Now attention is increasingly turning to the summer project, and we hope it will be as inspirational and formative an experience as it was for Andreas.

Given his interests, Nick is going to spend time with the Estonian company, Guardtime, where he will be examining the potential for implementing block-chain technology in the cloud. He will be engaging with the Estonian Virtual Data Embassy as well and in the process will be asking intriguing questions about identity politics, geopolitics, security and borders in and beyond the Estonian nation-state.

As one half of the supervisory team, it has been immensely enjoyable supervising Andreas and Nick and I am very grateful for the opportunity to work with colleagues like Keith Martin at the ISG. Our conversations are never dull!



THE TEACHING EXCELLENCE FRAMEWORK AND THE ISG

Prof. Peter Komisarczuk

> Programme Director of Distance Learning

Introduction

The Teaching Excellence Framework (TEF) is the continuation of the Government's reform of the Higher Education market that started in 2011. This article outlines what it is, what it means to the HE sector and how it applies to the ISG and our courses.

In 2011 the Government changed the way in which the HE sector was funded by charging the student with the whole cost of the undergraduate tuition fees (apart from some funding to help certain HE sectors such as STEM which continued to receive a small top up from the Government). The money to fund universities was capped by setting a maximum tuition fee and using the student quota system (called the student number control) to allocate a limit to home student recruitment and the burden of debt effectively transferred to the student. The sector sets tuition fees through the Office for Fair Access (OFFA) and until recently bid for a quota of home students that could be recruited and identified how the tuition fees would be used e.g. for maintenance grants for students from low income households, enablement of widening participation in HE and other student welfare as well as to cover the costs of running a university.

The maximum full time undergraduate tuition fee has been set at £9,000 for a number of years with many universities and courses having set their tuition fees at or close to the maximum with the average full time undergraduate fee for 2015-16 being £8,703. The tuition fee management has effectively forced universities and HE colleges that have degree awarding powers to become more efficient (including the extended use of zero hour/fixed term contracts, reducing cost base through redundancies and consolidation of infrastructure, closure of poorly recruiting courses etc.) and to seek funding from other sources, such as further increasing the number of overseas students, and investment in masters programmes that are not capped. One of the new changes proposed through the TEF will be the ability to charge more than the current maximum full time undergraduate tuition fee of £9,000.

The home student undergraduate quota system allowed the government to set the number of places being offered within the HE sector for undergraduate home students. The quota system used a set of fines to limit over recruitment of home students and if a university failed to meet their quota the quota could be reallocated to other more successful universities. These measures had the effect of reducing the number of home students at some universities and the closures of poorly performing degree programmes as universities sought to optimise their operations and meet their obligations. In addition the government pushed the development of higher apprenticeships leading to the development of vocational degrees, typically Foundation degrees, which have included a number in cyber security through the Tech Partnership. In 2014 the government removed the quota system allowing the student more choice in selecting the university they want to attend and the universities the ability to expand on their successes. The TEF will further enable this transformation and also allow new entrants to enter the market.

The Teaching Excellence Framework

On 6th November 2015 the government published its Higher Education Green Paper, Fulfilling our potential: Teaching Excellence, Social Mobility and Student Choice. This called for public feedback and ran until 15th January 2016 and in addition an inquiry by the Business, Innovation and Skills Committee, reported on 23rd February 2016 and published The Teaching Excellence Framework: Assessing quality in Higher Education. The overall purpose of the reforms is to:

- Introduce the TEF to measure quality, deliver effective university league tables, and ensure value for money,
- Increase access and success in HE from disadvantaged and under-represented groups,
- Effectively create a single system for all HE providers and enable a streamlined mechanism for the entry of new providers, exit of failing providers, with a new Office for Students to reduce regulatory burdens.

Specifically the TEF aims to help the HE sector and change HE provider behaviour through the following:

- Encourage excellent in teaching (lecturers, facilities, experience, "learning gain"), and promote improvements by highlighting exemplary practice,
- Promote cultural change by reducing the importance of the Research Excellence Framework (REF) so as to balance the contribution of teaching and research
- Provide clear information on teaching quality to assist student choice,
- Provide clear information to help employers recruit students with better and known skills, and
- Recognise and respect the diversity of provision, support for students and different types of teaching excellence.

What does this mean? Firstly the use and creation of appropriate metrics to measure teaching excellence, secondly a system to evaluate metrics and assess quality, thirdly a streamlined regulator and the opening up of the HE sector to alternative providers, with the potential to increase fees and change the market dynamics.

In terms of the proposed TEF rollout, we have the following guidance:

- TEF 1, for 2017-18 introduction. Institutions that pass the Quality Assessment review will be allowed to raise undergraduate fees in line with inflation.
- TEF 2, for 2018-19, will have multiple levels of quality; with institutions graded at different levels and potentially being able to charge tuition fees at different levels.
- TEF 2+, 2019 onwards, introduction of more and new teaching quality metrics, with the potential for assessment at the subject/discipline level. Thus we see an introduction over several years ending up potentially with subject specific assessments and several tiers of universities

The current draft proposal is to use the following already available metrics, even though there have been a variety of flaws identified within each of them:

- Employment/graduate destinations – a survey called DLHE carried out 6 months after a student has left the institution.
- Student retention, which measures the number of students that leave a course before completion
- Student satisfaction, which is measured through the National Student Survey (NSS).

The Quality Assessment will apply for the whole institution rather than be subject/discipline specific until 2019 or later, so individual areas of excellence will be rewarded only in the medium term. In terms of future metrics a number are being considered for suitability such as "Learning Gain" and "value add" which look at the relationship between the qualification and the knowledge/skills gained.

The TEF and the ISG?

Predominantly the teaching within the ISG is around the MSc in Information Security in its various forms, although our joint undergraduate degree (BSc/MSci Computer Science with Information Security) with computer science is becoming a significant teaching component.

Masters degrees are currently not covered in TEF 1 as the focus is on undergraduate degrees and some of the metrics proposed, such as the NSS do not as yet apply specifically to masters' degrees that use the Postgraduate Taught Experience Survey (PTES - where some questions are based on the NSS). However the masters market cannot remain exempt from such measurement for long, as the government extended the postgraduate student loan scheme, which provides loans of up to £25,000pa to post graduate students, in the 2016 budget to cover masters and PhD programmes and the governments green paper (paragraph 17) identifies the TEF will be open to all HE qualifications in the future.

In terms of some metrics the MSc in Information Security will do really well, such as employability and median salaries as reported in last year's ISG review. One of the developments both in the undergraduate and postgraduate area has been the inclusion of internships and a year in industry option that can further improve employability and enhance skills. However, we cannot be complacent and must ensure that we score well in all areas.

Throughout its 25+ year's history, the ISG has been fully committed to excellent teaching quality and maximising the employability of its students. Moving forward we will continue to encourage staff to engage with developments in teaching and the TEF, which will become as important to us as the Research Excellence Framework (REF) is today.

For 2015-16 the College is undertaking an overall review of learning and teaching, and the ISG is represented by Dr Geraint Price. We look forward to engaging with their findings over the next year.

THE DISTANCE LEARNING MSC

Prof. Peter Komisarczuk

> Programme Director of Distance Learning, ISG

Introduction

Distance learning (DL) is becoming increasingly popular, especially through the development of the Massive Open Online Course (MOOC) phenomenon which launched in 2008. Many millions of students have registered for MOOCs and as a result, distance learning has gained in popularity. The ISG have a successful variant of our campus MSc Information Security delivered through DL in collaboration with the University of London Academic Programme (UoLIA). This launched in 2003, gained GCHQ certification in May 2015 and has currently around 250 registered students (2014-15).

Distance learning has helped the ISG to deliver the MSc into over 100 countries and provides a flexible way to study the MSc. Students usually take between two and five years to complete the degree, fitting study around their personal and work circumstances. Students come from a wide variety of backgrounds with many already working in some aspect of the security industry. We encourage DL students to attend campus where possible; they can attend the block mode delivery of modules and there is a weekend conference each year in early-mid September. The conferences are recorded and available on our website, isg.rhul.ac.uk/dl/weekendconference2015/, and they combine presentations from industry, ISG staff, PhD students and the best DL project students who present their work to inspire their colleagues.

Characterising the DL Degree

Undergoing the certification by GCHQ allowed us to analyse our degree against the GCHQ selected evaluation framework. This is based in part on the Institute of Information Security Professionals (IISP) Skills Framework which segments the security discipline into groups, to which were added indicative topic coverage resulting in an evaluation framework with 13 areas of coverage. The DL degree is based on the campus Core A technical pathway with seven options (two of which are unique to the distance learning degree – Application Security and Advanced Cryptography).

The analysis showed an impressive breadth and depth of coverage in Information/Cyber Security; and gave indication of where we could potentially add more DL coverage. In addition, DL students can take a campus block mode module if they wish, as that can be credited to the DL degree. This allows extended framework coverage, for example including aspects of industrial control systems and critical infrastructure, which are covered as part of the IY5612 Cyber Security module.

Distance Learning Developments

In common with the campus programme the DL degree received feedback from the industry led External Syllabus Review. The review is undertaken by a panel from industry and government and feeds into our revision of the syllabus. For 2015-16 we are offering the campus module in Security Testing: Theory and Practice, this includes student access to the Royal Holloway virtualised laboratory where the students will be able to scan and hack a number of virtual machines. Major new content for the modules in Digital Forensics and Smart Cards is being developed for 2015–16 along with the usual updates to other modules.

In addition we have enabled the integration of campus and distance learning through the ability to share campus recordings of lectures through the virtual learning environment and the cloud. The campus systems, provided by Panopto, allow the capture of audio plus the computer desktop (slides and demonstrations), and through this we hope to provide distance-learning students with a glimpse of campus lectures and content where feasible.

STANDARDS FOR SECURITY

Prof. Chris Mitchell

> Professor of Computer Science

Introduction

Security standards have undoubtedly grown to become of huge importance to information security practitioners worldwide. In line with its long-term commitment to supporting information security in industry and commerce, members of the ISG have been involved in security standards development work for the best part of 30 years. In the ISG we believe it is important to contribute to standards development where we have the expertise, not least as a way of transferring the fruits of our research into practice.

It is interesting to recall that an option on security standardisation was one of the courses provided in the founding year of the Information Security MSc, back in 1992/93. Of course, since then security standards have become a part of just about every course in the master's degree, and so eventually the stand-alone course became rather redundant and was replaced.

I personally have been involved in security standards for almost 30 years, and one lesson I have learnt in that time is that if you are prepared to put in the effort to provide constructive inputs to standards being developed, and to spend time learning how things are done, it is possible to have a major impact. In turn, a great deal of satisfaction can be gained from seeing standards published which incorporate one's own ideas and input. Participating in standards has also greatly influenced my own research, and has given me many interesting research questions to think about. I would therefore like to encourage all of you to consider getting involved! I am sure your help and participation will be welcomed, wherever you choose to participate.

ISO/IEC JTC 1/SC 27

My personal involvement in security standards development has mainly been in ISO/IEC Joint Technical Committee 1 (JTC 1)/Sub-Committee 27 (SC 27), entitled simply Security techniques. I have regularly attended international meetings of SC 27 for nearly 25 years. These meetings occur twice a year wherever a national standards body is prepared to act as host. Most recently we met in Kuching (May 2015) and Jaipur (October 2015), and in 2016 we will meet in Tampa (April) and the UAE (October).

SC 27 has a very broad scope, and its activities are divided into five different working groups (WGs). Further details of the work of SC 27 can be found at its home page: din.de/en/meta/jtc1sc27?level=tpl-home&contextid=jtc1sc27&languageid=en

WG 1, which focuses on security management, is the custodian of the hugely influential ISO/IEC 27000 series of standards which, particularly interesting for those of us from the UK, has its origins in a British Standard, BS 7799, of which ISO/IEC 27002 is the direct descendant. WG 2 focuses on cryptography, and has produced standards covering almost every aspect of the subject. Interestingly, cryptography was the sole focus of the ancestor committee of SC 27, namely ISO TC97/SC20, which gave way to SC 27 in the late 1980s. That is, cryptography standardisation is the longest established work area within SC 27. An interesting connection to the ISG is that the late Donald Davies CBE, who was for a number of years a visiting professor at Royal Holloway, was one of the founding fathers of SC 20. Another ISG visiting professor, Michael Walker OBE, was a regular attendee at SC 27 meetings some 25 years ago, and for a period a few years ago, while he was an ISG academic, Alex Dent also regularly attended WG 2 meetings.

WG 3 is concerned with security evaluation, and is the home of the standards underlying the formal security evaluation process, namely the multipart standard ISO/IEC 15408. The last two WG s, WG 4 and WG 5, are of more recent origin, and were created in 2006 to address the growing scope of SC 27 work. WG 4 inherited work previously dealt with by WG 1, whose work programme had grown unmanageable, and covers a range of security management-related work outside of the ISO/IEC 27000 series. WG 5 covers the closely related topics of identity management and privacy.

I personally have attended WG 2 meetings since 1993, and before that I was involved with preparing UK contributions to this WG from the late 1980s onwards. More recently I have also attended WG 5 meetings (something of a problem, given they are held in parallel, albeit typically at the same venue).

The British Standards Institution (BSI) runs a security-focussed committee known as IST/33, whose role includes 'shadowing' the work of SC 27. Its home page is here: http://standardsdevelopment.bsigroup.com/Home/Committee/50001780

IST/33 is responsible for formulating responses to all the ballots on, and requests for expert input to, ongoing SC 27 work, as well as voting on proposed new items of work. It delegates the task of preparing detailed input to SC 27 to five sub-committees mirroring the five WGs of SC 27. These sub-committees (and the parent committee IST/33) are always happy to welcome new members as long as they are prepared to contribute towards the work in some way. For details on how to become involved, follow the links on the IST/33 home page or contact me directly at me@chrismitchell.net.

I have chaired sub-committee 2 (mirroring WG 2) since 1991, and I am particularly happy to welcome new members. IST/33/2, as we are officially known, meets four times a year to discuss UK contributions to ongoing SC 27/WG 2 work. We always meet in the very pleasant environment of HP Labs in Bristol, courtesy of Liqun Chen who has been an active member of IST/33/2, and a regular attender at WG 2 meetings, for something like 20 years; Liqun worked at the ISG for five years in the 1990s. Over the years, UK contributors have been very influential in WG2, especially considering the relatively small number of experts involved.

I should additionally mention that the chair of IST/33/4 is former ISG academic Andreas Fuchsberger, who is also convenor of SC 27's Special Working Group on Transversal Items (SWG-T), charged with looking after matters which cross boundaries between the five WGs, or are outside their existing scopes.

As a brief example of work within SC 27, in recent years I have acted, and am acting, as editor of two privacy-related standards in WG 5. The first is ISO/IEC 27018:2014, the Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, which establishes control objectives, controls and guidelines for the protection of Personally Identifiable Information (PII) stored and/or processed in the cloud. This timely addition to the ISO/IEC 27000 series has become something of a 'best seller' amongst ISO/IEC documents.

The second is a relatively newly commenced project on Privacy enhancing data de-identification techniques. This draft standard, intended to become ISO/IEC 20889, is currently at the 'first working draft' stage of development – that is a substantially complete draft exists, but it needs to pass several

more hurdles before publication, which is planned for 2018. This draft standard, which focuses on enhancing the privacy properties of stored data ('big data'), seeks to specify data de-identification terminology, provide a classification of de-identification techniques according to their characteristics, and describe their applicability for reducing the risk of re-identification. The idea is to provide an informed guide to these techniques, recognising that all such techniques have limitations which must be acknowledged when they are used.

I have attempted to mention some of the contributions of ISG staff, past and present, in the above summary. However, many apologies for any omissions, particularly of the many MSc alumni who have contributed, and continue to contribute, to the work of SC 27.

ETSI

Royal Holloway has been a full member of the European Telecommunications Standards Institute (ETSI) for several years. ETSI is particularly well known as the home of standards for mobile telecommunications, but has also provided a range of security-relevant standards with a broader focus. Current work includes a programme on cybersecurity. The ISG has made a range of contributions to ETSI's mobile security standards over the years, including providing reports on ETSI-adopted cryptographic algorithms. ISG visiting professor Michael Walker chaired the ETSI Security Algorithms Groups of Experts (SAGE) committee for many years; SAGE specifies cryptographic algorithms for use in standardised telecommunications systems. The ISG has also regularly provided attendees at the annual security event at ETSI headquarters in Sophia Antipolis.

The IETF

Kenny Paterson is involved in standardisation through his co-chairing of the Crypto Forum Research Group (CFRG), a research group of the Internet Research Task Force (IRTF). This group is tasked with proposing and evaluating cryptography that is being considered for deployment in IETF protocols. As one example, the group has recently reached consensus on new elliptic curves and associated cryptographic primitives to be deployed in TLS 1.3, the next version of the TLS protocol that is currently being worked on in the IETF. In future, the group will be studying how post-quantum cryptography can be smoothly integrated into IETF protocols.

The work of CFRG is carried out in a consensus-based manner through collaborative work on the CFRG mailing list (http://www.ietf.org/mail-archive/web/cfrg/current/maillist.html) and at thrice-yearly IETF/IRTF meetings. Its end products are recommendations on cryptographic algorithms and primitives taking the form of RFCs. Kenny's role in CFRG is to provide process management and leadership, and to help build bridges between the academic community of experts and the IRTF.

The future

The ISG will continue to contribute to security standards wherever and whenever opportunities arise; it remains a key part of our mission to ensure our research and knowledge have the maximum possible impact on real world practice. Indeed, this was one of the main reasons why we launched the MSc in Information Security back in 1992.

We also hope to use our extensive working experience and influence to build bridges between different security standards activities with overlapping focuses, and also between the standards community and real world standards users. One small step in this direction was the founding of the Security Standardisation Research (SSR) series of conferences, the first of which was held at Royal Holloway in December 2014.The third in the series will be held at NIST in Gaithersburg in December 2016.

We are always glad to welcome new contributors to the standards work in which we are involved, and I personally hope that this brief article will inspire some of you to join us in helping to make better and more effective standards.

STAFF PROFILE: DR MARTIN ALBRECHT

> Lecturer, ISG

How did you become interested in Computer Science?

I think this is mostly inspired by my mother, who has a degree in mathematics and worked as a computer scientist. I grew up in Eastern Germany. When I was about 7 years old, my godfather from Western Germany – on behest of my parents – smuggled an Atari ST over the border, so that I could learn about computers. I was probably one of, say, two kids in all of Eastern Germany with access to an Atari. Since then, my parents made sure I always had access to reasonably current hardware. For the first few years, though, I completely ignored any attempt of them to teach me programming. But after they signed me up for afternoon programming lessons, I picked up Turbo Pascal. I also recall trying some stack overflow tutorial as a teenager with some friends but giving up frustrated by this thing called vi. I only returned to smashing the stack for fun and profit at uni.

How did you become interested in Information Security?

As a teenager, I was quite active in social movements – anti-racism, ecological, anti-fascism – and we were convinced that we needed to secure our electronic communications and to encrypt our computers. I was the guy who liked computers, so I had to learn about PGP etc. and explain it to the others. I recall trying to understand the RSA problem, but giving up. When I went to uni to study computer science, all professors gave "hello" lectures about some stuff they were interested in. One professor explained RSA to us. At this point I decided that I'll do my Diplomarbeit (Masters thesis) with him on cryptography (I did). I mostly focused on other topics such as robotics during my studies, though. Information Security was more of a hobby that I pursued with some friends. We implemented Kenny's first IPSec attack for ourselves and played with stack overflows on PPC CPUs over drinks.

I took a few mathematics courses and enjoyed implementing mathematical algorithms. It was algebraic cryptanalysis, the topic of my Diplomarbeit and my PhD, which pulled me into cryptography properly. In fact, the first crypto paper I read was by Sean Murphy and Matt Robshaw. I thought I found a mistake, but Sean explained why I was wrong in a very kind e-mail. My focus on implementing mathematical algorithms also meant I became quite active as an open-source software developer for mathematics software such as Sage (general purpose), M4RI (linear algebra), Singular (commutative algebra) and fplll (lattice reduction) with an eye to applying those software packages to problems in cryptography. I still do that.

How has contributing to open-source projects has influenced you as a researcher?

I think contributing to projects like Sage has had a huge impact on me as a researcher. Firstly, working on large projects is really useful to learn about project management, coordinating, development and so on. I learned a lot in this regard from just watching William Stein manage the Sage project in the early years. Also, these projects tend to have really good people involved from whom you can learn a lot. This activity also put me in touch with leading researchers in a variety of fields who I could ask for advice in many situations. Also, quite a few research collaborations came out of this activity, say, in the form of us writing up the tricks we used to speed up computations. Also, the skills I picked up here were instrumental in a number of research projects later. But even if all of that wasn't there, I find working on code that is used by others immensely rewarding and fun.

What are your main research areas of interest?

I work on different aspects of cryptography. I have worked in theoretical cryptography arguing about the possibility of certain constructions under idealised assumptions, on the mathematics underpinning the security of cryptographic constructions by designing and improving algorithms for solving such problems, on efficient implementations of mathematical algorithms for cryptography, on the design and cryptanalysis of cryptographic primitives such as block ciphers and on practical cryptanalysis of real-world cryptographic protocols and their implementations such as TLS and SSH.

Lately, I have focused on post-quantum cryptography. In particular, I focus on lattice-based cryptography, algorithms for breaking, constructions and implementations. I have also worked on cryptographic multilinear maps, program obfuscation (encrypting programs) and homomorphic encryption (computing with encrypted data).
As mentioned before, I am also very interested in efficient implementations of mathematical algorithms relevant to cryptography.

I am currently teaching the MSc security testing module; maybe some interesting research question will emerge from this as well.

Modern cryptography may seem quite self-referential and removed from the real world by outsiders. What is your view on this?

It is true that it can be at times hard to explain to an outsider what problem we're trying to solve or why. Moreover, a lot of research in recent years has focused on Indistinguishability Obfuscation where it is not clear that it indeed can be done. Even if it is possible, our current constructions are well beyond the reach of what can be done in practice.

Still, in my view, it is part of science to pursue questions without an immediate application. As scientists we are not consultants but seek to understand our world. On the other hand, cryptography clearly has many applications in the "real world" and I care about some of those applications. I want Alice and Bob to be able to communicate, to work on documents together, to share data in a way which is protected against powerful adversaries such as nation-state sponsored attackers.
I would caution against using "the real world" or "society" as intended beneficiaries of our research, though. What "social benefit" means can vary a lot depending on who you ask. Take Digital Rights Management as an example or privacy enhancing technologies. At AsiaCrypt last year, Phil Rogaway gave the IACR Distinguished Lecture titled "The Moral Character of Cryptography Work". I highly recommend for anyone who works in our field to read the accompanying essay. I, for one, found it well worth paying attention to and it motivated me to think harder about what I am trying to achieve with my research beyond scoring the next publication and platitudes of "benefiting society".

INSTITUTE FOR CYBER SECURITY INNOVATION UPDATE

Robert Carolina

> Executive Director,
Institute for Cyber Security Innovation
> Senior Visiting Fellow, ISG

Defining cyber security needs. Solving cyber security problems. Bringing together experts from different domains to assist understanding and create solutions. Bettering cyber security here and now. This is why the Institute for Cyber Security Innovation exists. We are here to help.

Building on the pre-eminent foundation established by the Information Security Group, and with the support of University leadership, the Institute is already pursuing a number of exciting projects. These projects draw on the prodigious talents of the ISG as well as other academic colleagues throughout the University, plus our ever-expanding network of alumni and trusted advisors.

Projects currently under management include:

- A study on end user risk-taking behaviour conducted for a multinational pharmaceutical company. This project is staffed from the University's faculties of sociology and social psychology, using a combination of focus group and psychometric research methods. Having identified how study subjects conceptualise "risk" the team have already suggested different styles of interventions (e.g., messaging styles and delivery channels, plus technological interventions). The client will implement these selectively with their global staff. Our team will then follow up by measuring the impact of these various interventions on risk-taking behaviour. Practical consequences of the study include immediate recommendations about the most effective methods to modify risk-taking behaviour, as well as new methods that can be used to measure the effectiveness of various behaviour change interventions.
- A study reconceptualising end-to-end security methods used on the Internet. Conducted at the request of a global telecommunications equipment manufacturer, this study is lead by Professor Kenny Paterson of the ISG. He will spend two years working through this rigorous thought leadership exercise to identify various routes that will assist in remedying an emerging group of weaknesses in standard Internet security protocols. Practical consequences will include published articles to assist product designers and the standards community with design activity in the medium-term.
- A contact and outreach programme delivered to a critical national infrastructure operator. This on-going programme has been created in consultation with the client to assist with business transformation needs, helping a diverse team of system designers achieve a solid grounding in principles of information security risk management. Delivery is being achieved through a combination of ISG staff and trusted third party advisors.
- A study examining current market perceptions of the apparent skills gaps in the field of cyber security. Commissioned by a large security consultancy, the study is driven by Professor Fred Piper.
- An on-going industrial training programme for a major security product and services consultancy and channel partner, to acquaint new graduates working in customer relationship management with principles of cyber security to strengthen their ability to identify gaps in coverage and appropriate solutions. The programme is being delivered by a combination of ISG staff and trusted third party advisors.

The Institute is actively searching for more projects. Challenges we are prepared to address include:

- Directed research into any problem that currently weakens cyber security (whether from "technological" or "human" factors)
- Assessing the security design of new products, services, or methods, on behalf of innovators, investors, operators or other stakeholders
- Directed research in cyber security public policy and regulation
- Generalised industrial training in cyber security topics
- Specially designed industrial training created to meet the specific needs of a client

The Institute is a not-for-profit undertaking resident at the Royal Holloway University of London. We operate on commercial principles and are project-driven. We want to partner with those who wish to form project-specific consortia in examining solutions to the cyber security problems of today.

If you or your organisation want to engage with the Institute for Cyber Security Innovation, as a client or a member of our trusted delivery network, please contact me!

Robert Carolina, BA, JD, LL.M
Robert.Carolina@rhul.ac.uk

ROYAL HOLLOWAY UNIVERSITY OF LONDON
INSTITUTE FOR CYBER SECURITY INNOVATION

HUMAN FACTORS & RISKY CYBER BEHAVIOURS IN A GLOBAL COMMERCIAL ORGANISATION

Dr Rikke Bjerg Jensen
& Prof David Denney

> School of Law

Risky cyber behaviours by employees can potentially create huge costs whilst simultaneously causing reputational damage to institutions and businesses across the globe. Human factors within organisations can therefore not be ignored when trying to understand the underlying drivers for cyber-attacks. Indeed, cyber-attacks may be unwittingly facilitated by employees clicking on unsafe email attachments or suspicious links, or by an organisation's lack of clear online security policies, limited online security awareness amongst employees, and insufficient information protection training. Although some risky cyber behaviour might be modified through technological advances, technology-based solutions alone appear insufficient to overcome or modify behaviours that otherwise place an organisation at significant risk. A focus on human factors is becoming a crucial piece in the puzzle of understanding risk in an increasingly complex environment where users interact with technology to a much greater extent than has been the case previously.

Royal Holloway has been engaged with GlaxoSmithKline (GSK) over a two-year period in attempting to understand the meanings that employees ascribe to their own online behaviour. The research team comprises Professor David Denney (School of Law), Dr Rikke Bjerg Jensen (School of Law), and Dr Marco Cinnirella (Department of Psychology). The interdisciplinary research team joined forces with GSK in 2014, in order to examine and understand phishing attacks which pose a particular risk to GSK, a major pharmaceutical company operating globally. Real phishing emails are specifically intended to entrap people into giving sensitive information which could be of commercial advantage to foreign governments and other business interests, or to cause harm to organisational systems.

The starting point for the joint venture was a literature review produced by the Royal Holloway team, which examined phishing and unsafe behaviour within GSK, from sociological, organisational, and psychological perspectives.

The findings of this initial study were used to design a methodological strategy for a wider research project which encompassed a mixed-methods approach and was set within a cross-disciplinary framework. This larger piece of empirical research with GSK began in July 2015 with a phase of exploratory focus groups and a survey delivered globally to understand the meanings that employees ascribed to their cyber behaviour. This phase of the research also encompassed an investigation of the main risks to cyber security in the organisation as understood by employees. An intervention phase was then designed, incorporating the findings from the first research phase and a series of testable measures which can be taken forward by the company to address the initial findings. This will be followed by a second research phase later this year, which will examine whether the interventions implemented as part of the project have had any impact on employee behaviour and awareness of policy and training.

Emergent research findings

The research combines focus groups, interviews and a psychological attitude survey. By combining qualitative and quantitative methods, the study investigates risky cyber behaviours from a number of different perspectives and within over-lapping disciplines. This approach has resulted in a broad range of significant findings that will inform and shape intervention planning, future research and final recommendations to GSK. Although the research is incomplete at this stage (due to finish in early 2017), some tentative observations can be made from what has emerged thus far.

Research participants expressed high levels of trust in the security of information and communication systems in place within GSK. Employees also noted that they feel more secure on the GSK network than on their home network, which meant that the majority of participants preferred carrying out personal tasks that required them to submit sensitive information, such as online banking, whilst at work. This kind of trust in the GSK system may also result in increasing levels of unrealistic optimism, which was prevalent across the survey sample in particular.

Participants also expressed a number of different views and perceptions in relation to the level of responsibility and accountability in the context of cyber security more generally. In particular, most participants acknowledged some level of shared responsibility in terms of phishing, whilst a minority of participants understood phishing to be the sole responsibility of GSK. The majority of respondents therefore seemed to accept some degree of personal responsibility for keeping GSK data and IT equipment safe.

In terms of risk-taking in the context of cyber behaviour and the responsibility that this entails, participants did not believe that they typically acted in a risky manner at work, at the office or whilst in the field (sales staff). There was, however, a general lack of awareness amongst GSK employees of any efforts by the organisation to educate with respect to phishing although a number of phishing simulation exercises have already been carried out.

The significance of this project for Royal Holloway and GSK

The project demonstrates how a global business and Royal Holloway can work together to attempt to understand the human factors behind risky cyber behaviour. From the company's perspective the project is enhanced by the application of theoretical and methodological knowledge and by employing a team of experienced researchers to a particular cyber risk problem. The project is based upon the idea that new knowledge is essential in this area, if progress is to be made in combating this particular form of cybercrime. The researchers have considerable experience of delivering research on cyber related problems in large organisations. This effectively means that the company is receiving a level of service and knowledge that could not be achieved through business consultancy.

From Royal Holloway's perspective, the University is receiving research income, the possibility of high ranking academic publications which will flow from the research, and an example of study which has demonstrable impact. Additionally, the researchers are making further links with businesses which are facing similar problems and who require research to be carried out within their own organisation. In many ways, this is a win-win situation for all involved and characterises the way in which funded research may increasingly be moving in the future.

COMPUTER WEEKLY/ SEARCHSECURITY ROYAL HOLLOWAY INFORMATION SECURITY MSC THESIS SERIES

Dr Siaw-Lynn Ng

> Senior Lecturer, ISG

Founded in 1992, the ISG's flagship MSc Information Security Masters degree programme has now produced over 3000 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 how to manage the risk of hosting line-of-business applications in the cloud, to detailed technical studies of antivirus behaviour.

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 fifteen articles covering topics from digital cash to rogue USB attacks.

Critical infrastructures such as electricity grids and water distribution systems provide services that are vital for the functioning of modern societies. In "A Case Study in Critical Infrastructure Interdependency", Bernhard Schneidhofer (supervised by Stephen Wolthusen) examined the protection of a regional critical infrastructure against cyberattacks and showed how this required extensive efforts from all sectors. This dissertation was also awarded the David Lindsay prize from the British Computing Society for innovative applications of Information Security.

The blurring of the line between the virtual world and the physical world is also examined in the article "Policing Cybercrime" by Esther Snell (supervised by John Austen), where the role of the UK police in cyberspace is examined. Another interesting example is the advent of autonomous vehicles.Michael Haddrell (supervised by Keith Martin) argued in "Towards an Autonomous Vehicle Enabled Society - Cyber Attacks and Countermeasures" that the successful embracing of autonomous vehicles in future transport systems will be best achieved by taking a sensible risk-management approach to tackling the potential cyber security threat.

To better understand the underlying causes of risks and to allow more effective risk management solutions, Timothy D. Williams (supervised by Lorenzo Cavallaro) gave an overview of the value of threat modelling and described some common modelling techniques in "The Value of Threat Modelling". In "Enterprise Cloud Applications - Can We Trust Them?", Rob Sperrey (supervised by Geraint Price) examined a number of the more significant risks involved when an enterprise utilises line of business applications hosted in the cloud and discussed which of those risks are straightforward to address and which demand special attention and understanding from management.

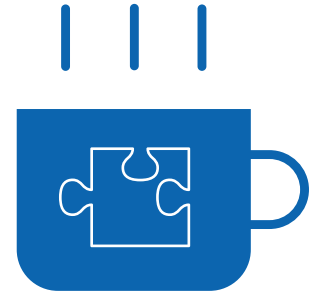
Another technology that adds to the complex problem of enterprise data management while enabling flexible working and new business opportunities is mobile devices. In "Managing Android Devices in the Enterprise - Understanding EMM, MDM and MAM", Jill Dove (supervised by Geraint Price) summarised the complexities of contemporary mobile device management and described two approaches to the device management problem in the context of Android devices. In the event of lost or stolen smartphones, Oliver Kunz (supervised by Keith Martin) examined the effectiveness of full-disk encryption as a method of protecting data in "A Security Assessment of Android Full-disk Encryption".

In addition to lost and stolen devices, computer systems and mobile devices are also vulnerable to attacks from malicious software. Much effort has gone into the detection and prevention of these attacks. In "Sandnet++ - A Framework for Analysing and Visualising Network Traffic from Malware", Anthony Nelson (supervised by Lorenzo Cavallaro) studied how malware communicates over a computer network in order to identify and block them, and in "Understanding Behavioural Detection of Antivirus", Soon Chai Liang (supervised by Lorenzo Cavallaro, with Andrea Lanzi of the University of Milan) aimed to improve virus detection by studying what the antivirus software are monitoring and what activities trigger a reaction. In "The Devil's Right Hand: An Investigation on Malware-oriented Obfuscation Techniques", Reza Hedayat (supervised by Lorenzo Cavallaro) looked at the origins of obfuscation and its significance in malware design, drawing parallels with the natural world and highlighting the importance of a means to measure their effectiveness in evading detection mechanisms. Another attack comes from rogue USB hardware implants, and in "BadUSB 2.0: Exploring USB Man-In-The-Middle Attacks", David Kierznowski (supervised by Keith Mayes) proposed using BadUSB 2.0 which could emulate USB attacks to provide an insight into how these attacks may be prevented.

If a system is infected with malware, there will in general be some forensic artefacts left behind. In "Extracting Actionable Data from Banking Malware", James Wyke (supervised by Frederik Mennes) discussed actionable data extracted from banking malware, and described how this data can be used to help defend against highly damaging cyberattacks. This may be a non-trivial exercise, as explained in "Analysis of the Linux Audit System" by Bruno Morisson (supervised by Stephen Wolthusen), where serious flaws due to architectural limitations of the Linux kernel cast doubts on its ability to provide forensically sound audit records.

Being able to buy and sell merchandise online is convenient and very much taken for granted now. In "Digital Cash and Anonymous Fair-Exchange Payment Protocols", Danushka Jayasinghe (supervised by Konstantinos Markantonakis) examined how fairness may be achieved in these transactions when virtual currencies are used, while Kevin Law (supervised by John Austen) explained how we may prevent criminal use of virtual currencies in "Virtual Currencies and Their Potential Role in Cybercrime".

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 (follow the links for "Information for Current Students" - "MSc Project" - "Thesis prizes"). Articles from past years are also listed on the website.



JOURNEY TO THE CENTRE FOR DOCTORAL TRAINING

Thyla van der Merwe

> CDT PhD Student

Coffee, both stale and fresh, that's what the office smells like on any given day. And I would know, I have spent, and will spend, many days in this office. That's what a PhD is, it's thinking about the same problem day in and day out, often without much success, it's babysitting experiments in the cloud only to discover later that one of your instances crashed and that you need to start all over again, it's the emotional roller coaster that is the peer-review process, it's commitment, it's sacrifice. 'Why do it at all then?' I hear you ask. This is an opportunity to become a producer of knowledge, knowledge that may be of some lasting benefit, and to no longer merely be a consumer of knowledge, that's why. It's the simplest and potentially the most naive of reasons but it's why I'm here; it's why I'm now a member of the Centre for Doctoral Training (CDT) in Cyber Security at Royal Holloway.

My journey to the CDT has been an interesting one. It all started with an undergraduate project supervised by an ISG alumnus, Dr. Christine Swart. Dr. Swart joined the Mathematics department at the University of Cape Town just as I was completing a degree in Mathematics, Statistics and Economics at this institution. An undergraduate project lead to a research-based masters dissertation on hash functions and before I knew it, I had a job offer from an engineering firm in South Africa, namely Tellumat (PTY) Ltd. I spent four happy years at Tellumat as a security engineer, learning about real-world systems that employed cryptography, and navigating some of the more hairy aspects of software development. During my time at Tellumat I represented South Africa on the International Organization for Standardization (ISO) committee responsible for standardizing cryptographic mechanisms and protocols. I had the pleasure of attending various standards meetings all over the world, and my role as a delegate was to defend the South African position and to contribute to the international standards where possible.

Although I was learning a great deal about how cryptography was being used in the wild, up until this point, I had never attended a formal university course on cryptography or anything security related. It was for this reason that I embarked on the M.Sc. in Information Security at Royal Holloway – I wanted to bridge the gaps in my knowledge with regards to topics in the broader field of information security. The M.Sc. degree did this, and more. It exposed me to a wide range of security related areas and imbued me with a greater appreciation for the many sub-fields that come together like a colourful jig-saw puzzle to make up what we think of as Information Security. It was a rewarding year, culminating in the Most Outstanding Student prize and a Computer Weekly-Search Security dissertation award.

Even though I had the option of returning to industry, I found myself being drawn to the research aspects of information security, specifically cryptography, as the M.Sc. year progressed. I realised that I wanted to move beyond a somewhat superficial understanding of cryptography and challenge myself to think more deeply about the structure, purpose and application of cryptographic mechanisms. This curiosity prompted me to apply for a place on the CDT.

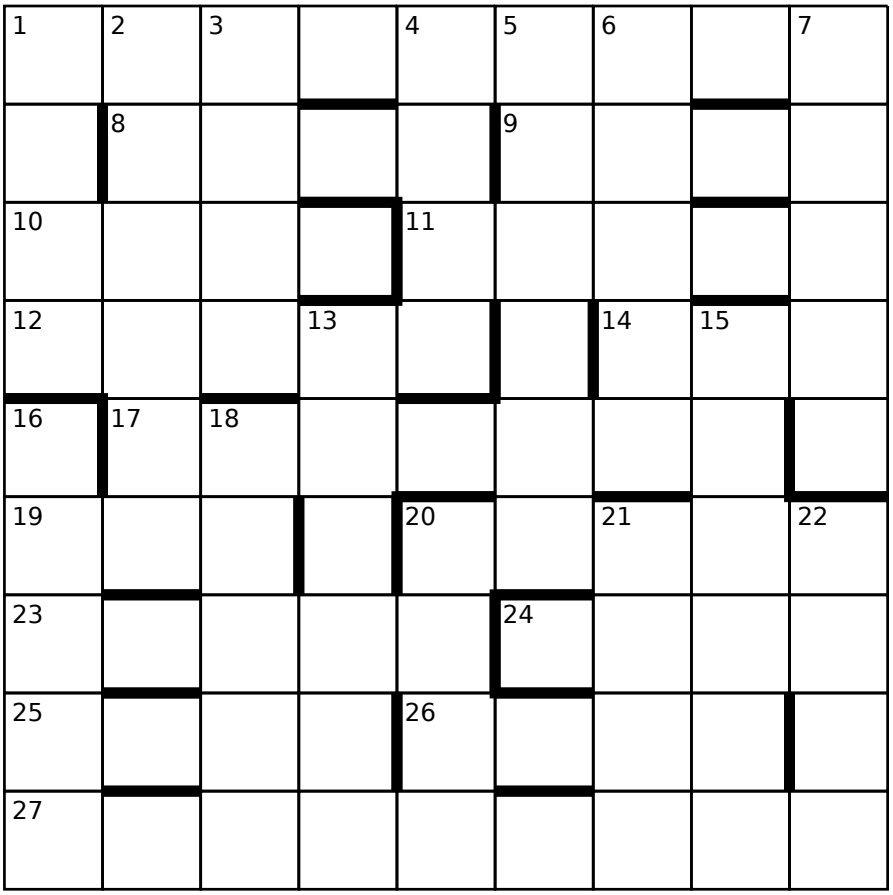
The CDT course structure is somewhat different to that of a traditional UK-based PhD in that the first year is spent completing coursework and a three-month project over the course of the summer. The summer project definitely kick-started my research and under the excellent supervision of Prof. Kenny Paterson, I have collaborated on two research papers focusing on the use of RC4 in TLS, and in August of last year I delivered the conference presentation at the USENIX Security Symposium in Washington D.C.

A requirement for all CDT students is the completion of an industry placement. I was fortunate enough to complete an internship at the Mozilla Corporation in Mountain View, California, where I was mentored by Eric Rescorla. Eric is the editor of the TLS 1.3 specification, the next version of the TLS protocol. TLS 1.3 is The Internet Engineering Task Force (IETF)'s answer to the weaknesses in TLS 1.2 and the TLS Working Group is in the process of finalizing its design. Under Eric's guidance and together with Sam Scott, a fellow CDT cohort member and Mozilla intern, I worked on the symbolic verification of TLS 1.3.

We conducted our analysis in collaboration with Prof. Cas Cremers and Marko Horvat of the University of Oxford and have recently received news of acceptance at the IEEE Symposium on Security and Privacy 2016. The work was presented at the Real World Cryptography conference in January and I recently spoke on the subject at the TLS Ready or Not (TRON) workshop in San Diego. The team has been in constant contact with the TLS Working Group regarding the state of our analysis and we are in the process of updating our formal model to incorporate the latest changes to the TLS 1.3 specification.

'So, what are you going to do when you're done?' is a question that I face with increasing regularity. The jury is still out on this one but my time at Royal Holloway will undoubtedly set me up to pursue either an academic or a industry-based career. With just under two years left on the clock there's still time to decide, but for now, it's back to the aroma of coffee.

CROSSWORD
Double Puzzle by Serpent



Answers to the clues produce clashes in 26 cells. These clashes, interpreted numerically, provide the starting point for a second puzzle (in which the bars should be ignored), whose solution involves replacing all the original entries. Use of a pencil is recommended!

Across

1 Process used to prevent putrefaction (9)
8 Circle of light (4)
9 Heroic tale (4)
10 1979 film starring Ray Winstone (4)
11 Harmonious condition of society (5)
12 Collaborative athletics event (5)
14 Place providing food and accommodation (3)
17 Informal term for the entertainment industry (7)
19 Be indebted to (3)
20 Lice and mice perhaps (5)
23 Bowl used by Jesus at the Last Supper (5)
24 Talkative bird (4)
25 Unit of area (4)
26 Strong impulse (4)
27 Obstacle to driver? (9)

Down

1 Not requiring much effort (4)
2 What Rossini's magpie did (6)
3 Shout loudly (4)
4 Reluctant (4)
5 Procession of troops (6)
6 Bones in the forearm (5)
7 Bony and emaciated (5)
13 Like an anchor unconnected to the seabed (6)
15 Oceanic bird with a hooked bill (6)
16 Novel by Ian McEwan first published in 2010 (5)
18 Listened to the sound of cattle! (5)
20 Strike one's toe against (4)
21 Starchy cereal used in puddings (4)
22 Slang term for an American (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 443101
E: isg@royalholloway.ac.uk
W: royalholloway.ac.uk/isg