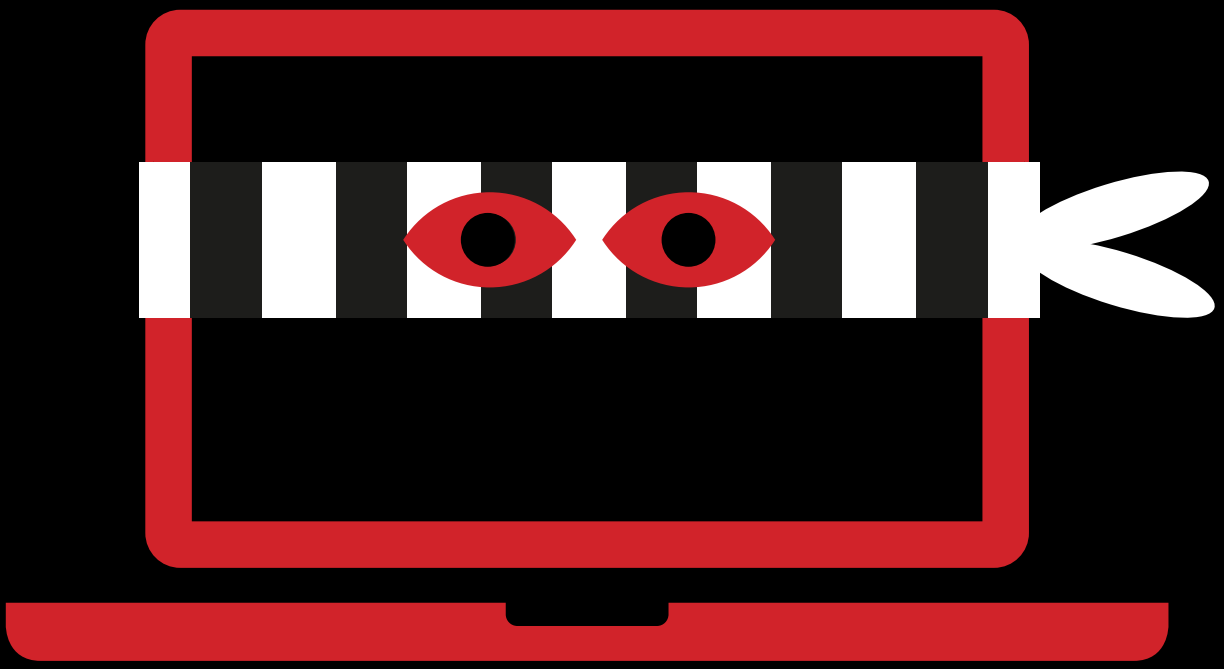
Information Security Group

Review 17/18



ROYAL HOLLOWAY UNIVERSITY OF LONDON

WELCOME
Prof. Keith Mayes

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

I wonder if there will ever be an ISG newsletter introduction describing how information/cyber security is under control, that there are enough experts, and that the world is now a safe and secure place. Well, it will certainly not be this year!

We have seen widespread outbreaks of ransomware, attacks on supply chains and software updates, with distributed Denial of Service attacks via IoT devices; and even hospitals and health systems are victims. Phishing and human engineering are rife, and perpetrators have no scruples when it comes to targeting the elderly and vulnerable. Criminal organisations and nation states are among the culprits.

Against this backdrop, the demand for our expert ISG graduates is insatiable, with 96% employability and student registrations growing rapidly each year. Between the campus and Distance Learning versions of our NCSC approved masters in information security, we will have between 400-500 registered students this year; working alongside our 90+ PhD students. We are also teaching security to an increasing number of Computer Science undergraduates; indeed there is now an NCSC approved BSC in Computer Science with Information Security. We are also providing security management teaching for our colleagues in the School of Management.

There is a lot of government activity to drive even more students towards information/cyber security, ranging from programmes aimed at secondary (and even primary) school pupils to degree apprenticeships. Our goal is to support all such activities and play our part in helping to plug the skills gap, both in the UK and internationally, and we were extremely pleased when our efforts were recognised at InfoSec 2017, winning the SC Award for best cyber security education programme.

Our research profile continues to expand on all fronts, winning research funding from national and international sources; and resulting in quality and quantity of academic publication. Recent international endeavours include our becoming an International Cyber Security Centre of Excellence (INCS-CoE); joining other elite institutions within the initiative founded by Keio University in Japan.

Our research activities have attracted new staff to the ISG and over the past two-three years we have welcomed seven extremely talented and enthusiastic new staff members, to our growing multi-disciplinary team and scope of endeavour.

I hesitate to predict the main challenges of the coming year, but I cannot foresee anything other than a significant expansion in our activities and impact.

Please do not hesitate to contact us if you require further information.

Prof. Keith Mayes

INDEX

MSC UPDATE
Dr. Jorge Blasco

> Lecturer, ISG

This academic year comes with a significant change within our MSc. After more than a decade, Dr Chez Ciechanowicz is stepping down as Programme Director. The transition to a new Programme Director started at the beginning of the academic year, and it is now almost complete.

I would like to use my first lines in this update to thank Chez for all his hard work and achievements. During these years he has secured the GCHQ certification, increased our student numbers and guided them with professionalism and empathy to ensure they got the best from their time at Royal Holloway. As a grand finale, our MSc in Information Security was awarded as the 'Best Cyber Security Education Programme' during the 2017 SC Awards Europe.

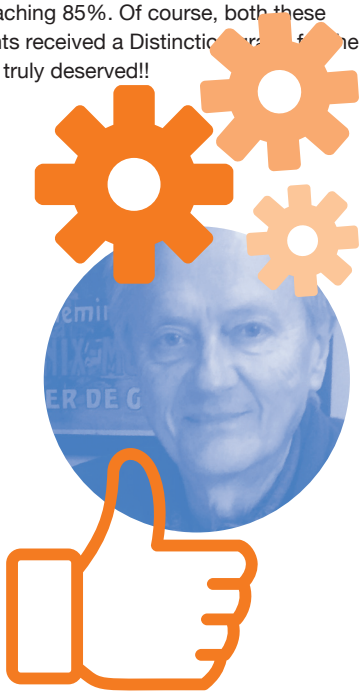
At the start of term in September 2016, we had a 15% increase in new student intake as compared with September 2015. This year, our student numbers have increased a significant 18% compared to 2016. Taking into account our Distance Learning MSc intake for this year, we have reached more than 600 registered MSc students. This must surely make our MSc, one of the most successful programmes in the UK, with a network of more than 4000 alumni.

However, there is more to be done. Up to date, women represent only a 7% of the cybersecurity workforce in Europe and 11% worldwide. This bias has a considerable effect on the ways we approach our day to day work and it also serves as another barrier that keeps women away from cybersecurity. Our female student population has consistently been in the range 19%-22% for the past five years. These numbers are a good start, but we must keep working to attract more women into our field. The Women In the Security Domain and/ Or Mathematics (WISDOM) group has been working towards this end very successfully during the last year. Of course, the WISDOM group is open to our MSc students so that they can benefit from a range of events and activities during their time at Royal Holloway.

Last year, we announced the introduction of a new module on “Human Aspects of Security and Privacy”. The module aims to fill a gap on current information security programs, which do not provide specific training to address the relations between individuals and the technical and managerial aspects of security.

After the first year running it, we can now say that the module has been a complete success. More than 50 students have picked the module as one of their options this year, making it one of the most popular ones among our students.

Each year there are two £500 prizes that are awarded during our December graduation ceremony. The first of these is awarded to the most outstanding MSc student of the year. This year the prize was awarded to Ijeoma Atuchukwu who achieved an overall average 91% – an outstanding performance. The second prize is awarded to the student that achieved the highest mark for the MSc dissertation. The prize was awarded to Jack Davidson who obtained a mark approaching 85%. Of course, both these students received a Distinctio[illegible] f[illegible]e MSc – truly deserved!!



CENTRE FOR DOCTORAL TRAINING UPDATE:
Prof. Keith Martin

> Prof. Keith Martin is acting Director of the EPSRC Centre for Doctoral Training in Cyber Security at RHU London

First CDT Students Graduate

The EPSRC Centre for Doctoral Training in Cyber Security at Royal Holloway reached a significant milestone on Friday 10th November 2017 when Conrad Williams of the 2013 cohort became the first student to complete his PhD viva. Well done to Conrad, whose thesis on Completeness in Languages for Attribute-based Access Control was successfully defended. Conrad is now working as a Cyber Security Specialist at reinsurance broker Capsicum Re. In December, Sam Scott successfully defended his thesis on The Design and Analysis of Real-World Cryptographic Protocols. Sam has joined a start-up programme at Cornell to prepare the way for commercializing research he has been involved in concerning password hashing. Sam was closely followed by Thalia Laing, Enhanced Threshold Schemes and their Applications, who is now a Research Engineer in the Cloud and Security Lab of HP Inc. In April ,Thyla van der Merwe also completed her thesis, which included important modelling and analysis work on the new TLS 1.3 standard. Thyla has been working at London-based Crypto Quantique and will shortly join Mozilla.

Several more PhD vivas are scheduled over the coming months as the remainder of the 2013 cohort conclude their studies. Pending their vivas, Steve Hersee has taken up a role in The Cabinet Office and Naomi Farley is working for Thales.

It is thrilling to see CDT theses being completed and, more importantly, to see the extremely rounded and skilled graduates progress in their careers. The primary objective of the CDT is to develop a cohort of highly-trained researchers with a broad understanding of cyber security, and an appreciation of the increasingly important interplay between theoretical, technical and human factors in this field. We are thus delighted to see this reaching fruition.
We look forward to reporting on the career destinations of the other students of the 2013 cohort as they follow suit over the coming months.

A New Cohort Start

October 2017 saw the arrival of our fifth CDT cohort of eleven students. They have an impressively wide range of academic backgrounds, including econometrics, geopolitics, psychology, computer science and political philosophy. Several have held previous employment in careers as diverse as security consultancy, finance and mathematics teaching. Our recent experience suggests this blend of life history will deliver a superb cohort, and early evidence was provided by their thoughtful and inspiring group project on the national cyber security strategy, which they analysed and critiqued. In March they had the opportunity to report back their findings during a visit to the National Cyber Security Centre.

End Of Current Funding

Such are the swings and roundabouts of funding that, just as we celebrate our very first PhD graduate, so we place the recruitment adverts for our final student cohort on the current funds. The CDT in Cyber Security at Royal Holloway has been, we hope you agree, a runaway success story. The outstanding students have brought an electrifying energy to our research environment. The innovative training environment has broadened their skill base, and we are now seeing the products of this through quality research that is hitting high standards and winning awards. The CDT has acted as the perfect vehicle to facilitate research beyond traditional disciplinary boundaries, with projects involving computer science, economics, geopolitics, geography, mathematics, psychology, and sociology.

The CDT has also helped to bridge conversations between academia, industry and government, some of which you can read about elsewhere in this newsletter. The ultimate fruits of these relationships are the graduate destinations of our first completers. The CDT has been a joy to facilitate and we hope that it can continue in some form. In March we submitted an outline bid for funds for a new CDT, competing against all disciplines and universities conducting engineering and science research work. Please get in touch if you are willing to help us tell the success story of the current CDT and support this new funding bid. As we have discovered, hosting a CDT is too rich an experience (and far too much fun) to not host one in the future!

THE ALL PARTY PARLIAMENTARY GROUP IN CYBER SECURITY

Dear Readers,

Cyber security, and protecting the safety and privacy of UK citizens, is of paramount importance to government. As the Member of Parliament for Chelmsford, I see it as my duty to help with this critical challenge, and so I became the chair of the APPG in Cyber Security, when Flick Drummond stood down.

My fellow officers of the APPG include, Richard Benyon MP, Nigel Huddleston MP, Admiral the Rt Hon Lord West of Spithead GCB DSC PC ADC DUniv, the Rt Hon Lord Arbuthnot of Edrom, the Rt Hon George Howarth and Baroness Neville-Jones; with Professor Keith Mayes and Andrew Henderson representing the ISG as secretariat.

Recent APPG meeting topics have included a discussion around ransomware and how it hit our NHS services; and a report from the Rt Hon. Ben Wallace, Minister of State for Security at the Home Office, on the Take 5 cyber awareness programme delivered via banks. At the time of writing, I am looking forward to the visit of Max Everett, the U.S. Department of Energy Chief Information Officer, to talk on cybersecurity, energy, and critical national infrastructure, and the challenges facing the West.

The APPG provides an opportunity for frank exchanges of views on critical security matters and contributes to the government's activities in this area. It is of course clear that as a nation, we need to train an ever increasing number of skilled men and women to keep us safe in the digital world, and we appreciate the long-standing efforts of the ISG in this respect, and for its on-going support for the APPG secretariat.

Yours Sincerely

Vicky Ford MP
APPG chair and Member of Parliament for Chelmsford

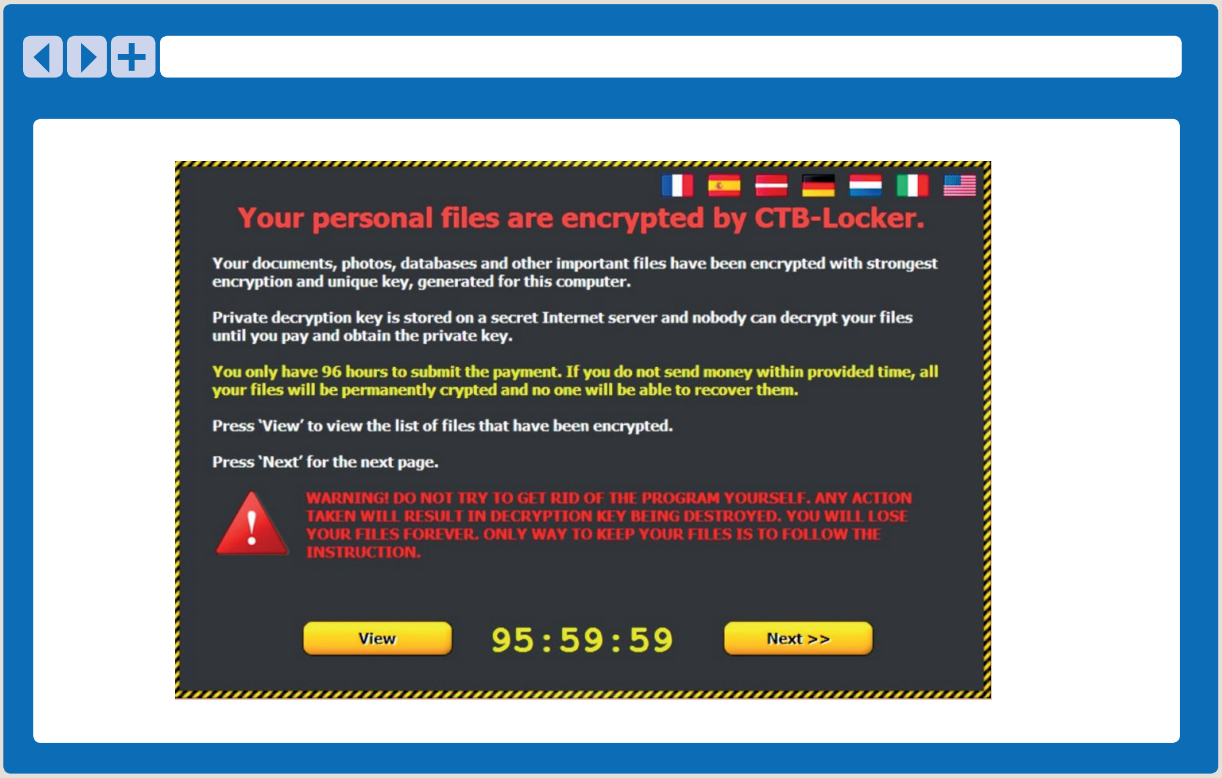


Fig 01: Ransom Demand

RANSOM... WHERE?

Dr. Daniele Sgandurra

> Lecturer, ISG

RANSOMWARE

In the last years, numerous Internet users and companies have been victims of world-wide cyber-attack campaigns based on extortion mechanisms. In particular, cyber-criminals have targeted Internet users with "crypto-ransomware", which is the malicious software that encrypts personal files to make them inaccessible to its victims and force them to pay a ransom to get their data back. (Fig 01)

Ransomware has featured prominently in the media, in particular when in 2014 a Police Department's computer system, in Durham, was infected by Cryptowall ransomware[1], and when in October 2016 a ransomware infected hundreds of computers at San Francisco's public transit agency and demanded 100 bitcoins to unlock data[2].

More recently, on 12th May 2017, a world-wide infection of the WannaCry ransomware was able to infect more than 200,000 machines, also thanks to its capability of autonomously infecting other systems[3]. Similarly, at the end of June 2017, a huge ransomware outbreak (NotPetya) has hit major banks, utilities and Telcos. This ransomware's main goal was to destroy data, and so companies could not get their data back even after paying the ransom[4].

Other destructive families of ransomware include Cryptowall, CrypotLocker, Cerber, and Locky. Petya, in particular, differs from other ransomware variants by overwriting the Master Boot Record: this effectively locks the victims out of their computer entirely. (Fig 02)

RANSOM DEMAND.

The average ransom demand is now around £500. The general consensus is that the total cost of ransomware in 2016 might have reached over £1 Billion[5]. For anonymity, the ransom payment is usually demanded in cryptocurrency, with Bitcoin being the most popular.

HOW RANSOMWARE IS INSTALLED?

Ransomware is installed through various means including the exploitation of a computer vulnerability by a remote threat, or by visiting a website that includes a malicious advertisements. However, most ransomware samples are deployed through spam email campaigns with emails containing a malicious link or attachment that installs the ransomware when the user clicks on it. Note that some ransomware variants do not require user intervention to infect machines, and can propagate across several computers and networks autonomously. Even if most of the infected machines run Windows operating systems, an increasingly higher number of attacks are targeted against databases, Web servers, and Android or iPhone smartphones[7].

VICTIMS

Individuals are still the largest percentage of victims. However, there is a rapid growth in attacks on organisations. In particular,

hospitals are increasingly becoming targets of ransomware, as patient data are vital and attract cyber-criminals. The Financial Times reported in December 2016 that 34% of NHS trusts in Great Britain had been infected by ransomware over the previous 18 months with several being attacked multiple times[6]. Other possible future UK targets of ransomware are the Internet of Things and critical infrastructures: a proof-of-concept ransomware attack for both these scenarios has already been successfully demonstrated[8] [9].

RANSOMWARE PROTECTION

Prevention is the ideal solution for ransomware protection. In particular, by following this advice, users and companies may reduce their chances of being infected:

- User education. Users should be educated to never open an email attachment that looks suspicious. In doubt, they should ask system administrators. Furthermore, only low-privileged accounts should be used to log in.

- Patching. Operating system and applications, as well as browser plugins, should be updated as soon as patches are available.

- Backup. Users and companies should backup all important data regularly. There are several tools available that are easy to use and enable users to restore all their data in the event of a ransomware. It is important, however, to keep the backup storage areas separated from the computers, or ransomware might impact also backup copies.

At the Information Security Group of Royal Holloway we are exploiting the use of machine learning techniques to detect old and new families of ransomware by spotting anomalous behavior early[10].

References

[1] Karen Dandurant, “Cryptowall attacks Durham police files”. 7 June 2014. Available at: http://www.seacoastonline.com/article/20140607/NEWS/406070322

[2] Samuel Gibb, "Ransomware attack on San Francisco public transit gives everyone a free ride". 28 November 2016. Available at: https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

[3] S. Osborne. “NHS cyber attack: Ransomware hits 200,000 victims in at least 150 countries, says Europol director”. 14 May 2017. Available at: http://www.independent.co.uk/news/uk/crime/nhs-cyber-attack-wannacry-ransomwarevictims-countries-europol-rob-wainwright-a7735001.html

[4] Iain Thomson, "Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide". 28 June 2017. Available at: https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/

[5] Danny Palmer, "The cost of ransomware attacks: $1 billion this year". 8 September, 2016. Available at: http://www.zdnet.com/article/the-cost-of-ransomware-attacks-1-billion-this-year/

[6] Financial Times, "NHS cyber attack far more extensive than thought, says report". 26 October 2017. Available at: https://www.ft.com/content/4110069a-ba3d-11e7-8c12-5661783e5589

[7] Chen, Jing, et al. "Uncovering the Face of Android Ransomware: Characterization and Real-Time Detection." IEEE Transactions on Information Forensics and Security 13.5 (2018): 1286-1300.

[8] David Formby, Srikar Durbha, Raheem Beyah, "Out of control: Ransomware for industrial control systems". February 2017. Available at: http://www.cap.gatech.edu/plcransomware.pdf

[9] Ken Munro. "Thermostat ransomware. Or how i learned to hack like it was 1994". September 2016. Available at: https://www.owasp.org/images/2/2f/OWASP20160929_Thermostat_PTP.pdf

[10] Sgandurra, Daniele, et al. "Automated dynamic analysis of ransomware: Benefits, limitations and use for detection." arXiv preprint arXiv:1609.03020 (2016).

Fig 02: Not Petya

ENHANCING WEB USER SECURITY AND PRIVACY

Prof. Chris Mitchell

> Prof. ISG

Introduction

We all know about the dangers of the web – it's a dangerous world out there on the Internet. There are many threats to our security and privacy as we use our web browsers, from drive-by downloads to phishing and all its variants. Most of us are also aware, perhaps only from the evidence that is hard to escape, that we are being tracked as we browse across multiple sites. However, often we feel powerless to do anything about these threats to our security and privacy.

Of course, we know (I hope) not to click on links in emails unless we are absolutely sure they are genuine; indeed, perhaps we are careful and only view emails in text form and not in HTML. Most of us are also aware that if anything on the web is too good to be true then, as with everything else in life, it almost certainly isn't true. However, apart from routine caution and a good helping of suspicion as we go about our business, what else can we do to help make ourselves safe from fraud and minimise our loss of privacy?

Well, there are a growing number of tools we can use to help make ourselves a little safer as we use the web. The purpose of this article is to describe recent research involving current and past ISG PhD students which has developed two such tools that give you the chance to take greater control over your own security and privacy.

Tracking

It is hard to avoid the fact that our activity is being tracked as we browse the web. Perhaps the most obvious evidence of this is the ubiquitous advertisements for products that we may have looked at once on a retail site – adverts for these products then appear on a multiplicity of sites we subsequently visit. Many of us are aware that web cookies are widely used to help enable this tracking. Whenever we visit a site, which involves the browser sending an http request to this site, an http response (typically containing a web page) is sent back, and this response will often contain a piece of data known as a cookie. The browser automatically stores this cookie and sends it back to the site with the next http request. The storage and transmission of cookies can be disabled, but if we do this then many useful functions, e.g. shopping baskets for retail sites, stop working (since the contents of our shopping basket will typically be stored in a cookie).

However, there appears to be much less awareness of another widely used technique for tracking, namely browser fingerprinting. Browser fingerprinting takes advantage of the fact that modern browsers have rich APIs, designed to enable a range of useful functions. These APIs can be accessed by JavaScript programs, downloaded to a browser by a website as part of a web page. The use of JavaScript enables many features we take for granted in modern web pages, including dynamic behaviour. Disabling JavaScript is possible, but it has the effect of preventing most modern websites operating properly.

The information that can be accessed by JavaScript includes a wide range of information about your device's hardware and software configuration, e.g. screen resolution, the set of installed fonts, or the particular version of browser in use. This information can, invisibly to the user, be automatically sent back to the website that issued the JavaScript or, indeed, to any other site. The combination of the information obtained in this way has been shown to uniquely characterise the vast majority of devices on the web, i.e. it enables your device to be tracked – this is browser fingerprinting.

Experiments performed by a current ISG PhD student, Nasser Al Fannah, have shown that browser fingerprinting is very widespread, and that the most common form is so-called third-party fingerprinting, where the information gathered by JavaScript is sent back to a specialist data analysis third-party site. Third-party fingerprinting is particularly privacy-threatening, as it enables a single entity to track individual devices as they visit many different sites. In collaboration with a former ISG student, Wanpeng Li, now a post-doc at City, University of London, Nasser has also developed a website providing a host of information about web fingerprinting: https://fingerprintable.org/

Wanpeng and Nasser have also developed a tool, which they call FingerprintAlert, which monitors the data being sent by your browser to visited websites for possible fingerprinting activity. Not only does this tool enable you to see who is tracking your web browsing, but it also allows third party fingerprinting to be automatically blocked. That is, it offers the ability for you to reduce the degree to which you are tracked. Fingerprint Alert takes the form of a browser add-on, which is available for both Chrome and Firefox. To use this add-on, simply visit the Chrome or Firefox store and search for FingerprintAlert; alternatively, follow the links on the Resources section of the https://fingerprintable.org website.

Single sign on

Many websites require users to register and then login to gain access to services. Almost always, the method of user authentication involves use of a password, which means that we all have many passwords which we are somehow expected to remember. One way of reducing this burden is to use a single sign-on (SSO) service, as provided by sites such as Facebook or Google; that is, when logging in to a site, we are often given the option to 'log in with Facebook'. If we click on this option then, if necessary after a Facebook authentication, we are automatically logged in to the target site.

These SSO services, for which there a number of providers, are commonly based on either OAuth 2.0 or OpenID Connect, two closely related protocols (in fact, OpenID Connect is essentially a layer of functionality on top of OAuth 2.0). The SSO service provider will typically provide a set of instructions enabling a site to take advantage of its service.

Unfortunately, many websites using these SSO services fail to implement them properly. That is, when building their websites, they don't properly implement the necessary interactions with the SSO service provider. Practical experiments, including those performed by the former ISG PhD student Wanpeng Li, have revealed a large number of serious security flaws in implementations of OAuth 2.0 and OpenID Connect – in the worst case these could lead to a complete compromise of your account.

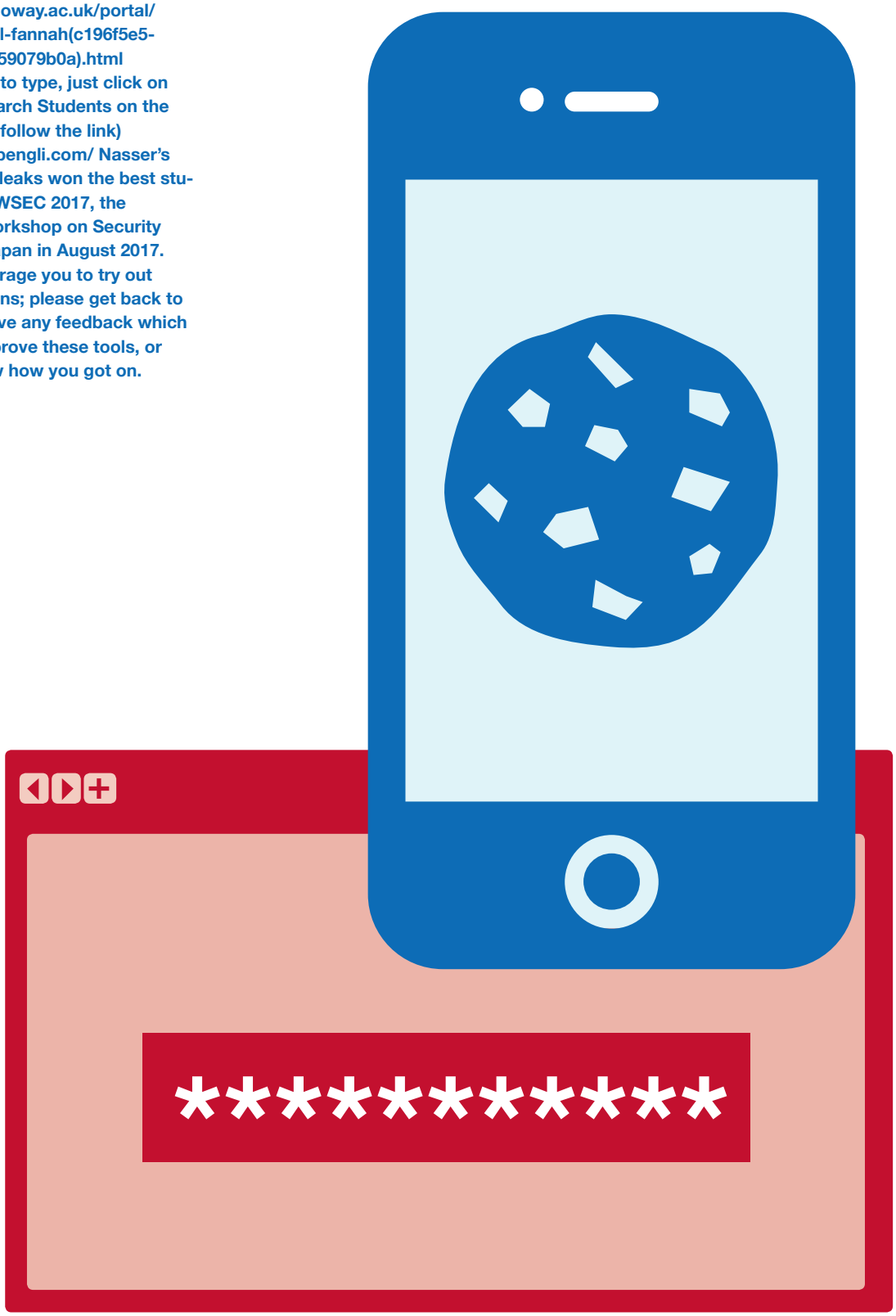
The problems in implementation appear to arise from the work of developers with little background in security; sometimes this is made worse by unclear or incomplete explanations from the SSO service providers. Of course, Wanpeng has warned all the websites affected, and some of them have rectified the problems identified. However, there are very large numbers of websites out there using SSO services, and he cannot possibly check them all.

This puts the user in a very difficult situation – how can they know whether or not an SSO service is safe? To help address this dilemma, Wanpeng has developed a browser add-on called OAuthGuard, which monitors

how websites perform SSO. If it detects poor practice it either corrects the problem, reducing the threat or, if it cannot rectify the issue, at least warns the user not to use the service. OAuthGuard is available as a Chrome add-on from the Chrome store – simply search for OAuthGuard at the store.

More information

Both Nasser and Wanpeng have published a number of papers on the topics covered in this article. To access these articles, go to their respective web pages, i.e. https://pure.royalholloway.ac.uk/portal/en/persons/nasser-al-fannah(c196f5e5-e3e0-413f-ac62-9fa259079b0a).html (or, if this is too long to type, just click on Staff Directory/Research Students on the ISG home page, and follow the link) and http://www.wanpengli.com/ Nasser's paper on IP address leaks won the best student paper prize at IWSEC 2017, the 12th International Workshop on Security held in Hiroshima, Japan in August 2017. I would like to encourage you to try out these browser add-ons; please get back to the authors if you have any feedback which could be used to improve these tools, or simply let them know how you got on.



THE ISG SMART CARD AND INTERNET OF THINGS SECURITY CENTRE (SCC)

Prof. Konstantinos Markantonakis

> Director of SCC

As they say in Japan, "time flies like an arrow", and this is precisely how it feels like since our last year's SCC update. The SCC's activities in 2017 demonstrate another very successful year!

Members of the SCC took part in the ISG delegation that visited the British Embassy in Tokyo for the UK-Japan-US Cyber Security Collaboration on the International Cyber Security Centre of Excellence (INCS-CoE). The ISG delegation also attended the 6th International Cybersecurity Symposium at Keio University, and visited Hitachi center to discuss a potential security research collaboration based on the use of common system simulation tools for modelling critical infrastructures.

In the last academic year, we have supervised more than 30 MSc projects in topics related to embedded systems, Internet-of-Things (IoTs) and payment systems. In fact, the MSc project "An evaluation of the security of the Bitcoin Peer-to-Peer Network", by Jack Davidson, supervised by Prof Konstantinos Markantonakis, won the David Lindsay Prize, awarded every year by the British Computer Society's Information Security Specialist Group to the project that best addresses innovative applications of Information Security. Findings from the project are also submitted in a major BlockChain conference. Furthermore, another project "Security Analysis of Smart Home Security Devices", by Yee Ching Tok, supervised by Dr Daniele Sgandurra, investigated the firmware of a popular smart home security device. Two vulnerabilities (CVE-2017-13663 and CVE-2017-13664) were found and disclosed responsibly to the vendor. A detailed explanation of the vulnerabilities and of the disclosure timeline is available here: https://poppopretn.com/2017/11/30/public-disclosure-firmware-vulnerabilities-in-ismartalarm-cubeone/. Additionally, during his final MSc project testing/analysing Internet of Things devices, Andrew Watson, supervised by Prof Konstantinos Markantonakis, found various security vulnerabilities across multiple IoT CCTV/DVR products. These included the discovery of two previously unknown vulnerabilities - which are currently being progressed for resolution with respective vendors following responsible disclosure.
These projects extend the long list of MSc projects supervised by the SCC resulting in conference papers, which demonstrates the excellent work of our MSc students.

We also celebrated the successful completion of four PhD students supervised by the SCC. They are: Dr Danushka Jayasinghe, "Enhancing the Security of Centralised and Distributed Payments", supervised by Prof Konstantinos Markantonakis. Additionally, Dr Sheila Cobourne, "Challenging Environments: Using Mobile Devices for Security in Real and Virtual Worlds", Dr Assad Umar, "On the Security and Performance of Mobile Devices in Transport Ticketing" and Dr Lazaros Kyrillidis, "Using the Smart Card Web Server to enhance the security of Web applications and the Web of Things" all three supervised Prof Keith Mayes. Well done to them! On that front, we have to congratulate Dr Daniele Sgandurra who received a grant of £100,000 from HM Government for a PhD Studentship on threat modelling of IoT devices to start in October 2018. We also have to welcome our new PhD student, Mr Benjamin Semal, who joined the SCC in January 2018, and will be supervised by Prof Konstantinos Markantonakis. On that note, we have to reiterate the message that Prof Markantonakis and Dr Sgandurra are actively looking for strong PhD candidates to join our research teams. If you are interested, please do get in touch (https://scc.rhul.ac.uk/open-positions/).

In September 2016, we started (along with the Universities of Surrey, Southampton, and Loughborough) a three-year EPSRC project DICE (Data to Improve the Customer Experience) aiming to develop the technology foundation for providing personalised customer experience while preserving their privacy requirements. The project is led by Prof Konstantinos Markantonakis and Dr Raja Naem Akram. As part of this project, the ISG-SCC is actively developing a set of technologies that enable transparent data management practices for an organisation. Transparent data management allows the consumers of an organisation to view the data the organisation has collected about them and what operations are being performed on them. Furthermore, individual users can perform real-time data privacy assessment and verify whether the organisation is using their data according to the relevant regulations (e.g., GDPR) and terms & conditions. The technology can potentially pave the privacy landscape, especially after the Facebook and Cambridge Analytica revelations, giving users more control over their data and also, as an organisation, becoming more transparent to the consumers in a win-win proposition. Dr Raja Naeem Akram, played an instrumental role in defining the overall framework. As a result of this effort, in 2017, the ISG-SCC offered a summer internships to an undergraduate (UG) Computer Science student (James Tapsell). At the end of this internship, a patent application was filed by the College in which Dr Raja Akram, Prof Konstantinos Markantonakis and James Tapsell appear as co-inventors. Besides this, the intern has also contributed to a research paper for a conference (under review) and to another ongoing paper: this is a great achievement! Finally, the Royal Holloway Research and Enterprise (R&E) department is looking into potential possibilities of commercialising the project's developed idea.

Capitalising further on last year's success in working with UG students, this year (2018) ISG-SCC has offered 8 internships related to the DICE project to undergraduate students. These students will jointly contribute to the development of the overall architecture of the transparent data management system, and so they will benefit from the research and development experience. Furthermore, each of these internships has a specific research challenge for the respective intern. The overall objective of these internships is to foster understanding of information security challenges and train them to be part of a research team.

The SCC is part of an international consortium focusing on developing the next generation TPM (Trusted Platform Module), which is embedded into computing systems to make its host computer platform trustworthy and secure. TPMs are currently incorporated into over a billion computers worldwide. Our newly funded H2020 Project 'FutureTPM' (Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module) will be focusing on developing next-generation security solutions to mitigate against quantum computers. These computers

are anticipated to be able to break some of the cryptographic algorithms currently used in existing TPMs. The consortium consists of high calibre industrial and academic partners from across Europe. Royal Holloway's project activities will be led by Dr Daniele Sgandurra, who has received a grant of €375,065 from the European Commission to carry out the work alongside Professor Konstantinos Markantonakis, Professor Chris Mitchell, and Dr Elizabeth Quaglia.

Dr Raja Akram is leading our very active research thread on Unmanned Aerial Vehicles (UAVs) in collaboration with the University of Limoges and University of Bordeaux. This collaboration has produced a number of research papers (in key avionics conferences) on wide-ranging topics including secure communication, UAV platform reliability, artificial intelligence, swarm intelligence, flight formation optimisation and machine ethics. As a result of our in-house expertise, this research theme has produced an EPSRC grant application in collaboration with Cranfield University and Edinburgh Napier University. This grant application aims to create a fully autonomous, cyber-physical (predictive) resilience and adaptive cybersecurity platform for single and multi-UAVs with strong foundation in machine ethics and sustainable technologies. In addition, we have also submitted a H2020 RISE proposal related to the autonomous Air Traffic Management (ATM), UAV detection and compliance evaluation of UAVs operations with airspace regulations in real-time. The consortium for this research proposal includes four industrial companies and the Ecole des Ponts (France).

We have also established a strong relationship with the University of Surrey, as evident with the two existing research projects running at the SCC. Beside this, we are currently underway in the development of an EPSRC grant proposal with 5G Innovation Centre, University of Surrey. Also, Dr Raja Akram and Prof Markantonakis are leading the development of a further three EPSRC research proposals with colleagues from the University of Southampton, Imperial College, Edinburgh Napier University and University of Kent. We hope to foster a network of external collaborators to build a strong and diverse research portfolio.

In addition to above activities, we are also focused on building interdisciplinary collaborations, especially with applied ethics, human behavioural, neural behaviour, human perception, social aspects of openness and empowerment, governance models, artificial intelligence and data monetisation. These collaborations are expected to generate innovative ideas that transcend the traditional boundaries of Information Security research.

Furthermore, the SCC celebrated its 14th anniversary on the 30th of August 2017 with the SCC Open Day. The event was attended by more than 100 visitors, including 12 industry exhibitors and 15 SCC students. This year, three student prizes were awarded: the First Prize was awarded to Mr Jack Barker “Vulnerabilities in Geofencing Strategies Used to Prevent the Flight of Unauthorized Aerial Drones in Restricted Airspace”, the Second Prize to Mr Andrew Watson “Testing/Analysing IoT devices for vulnerabilities”, and the Third Prize to Mr James Tapsel for the “Scalable NoSQL Provenance Logging”. The first and third best project prizes were won by UG summer interns at the ISG-SCC. The event also hosted four interesting sound bite talks, which covered a range of Smart Card and IoT security issues: in particular, John Moor, IoTSF, presented “IoT security – so what’s new?”, Chris Loreskar, Trustonic, discussed "Securing IoT"; Nationwide presented "Squaring the circle; balancing compliance and innovation in security" and finally NCSC discussed “Physical threats to smart cards”. The day ended with a prestige lecture from Ken Munro, Pen Test Partners, entitled “The IoT does actually make me WannaCry. The truth behind ransomware, botnets and your household goodies”. The event was supported by the SCC sponsors: Transport for London, the UK Cards Association and ITSO as well as event sponsors; Infineon, MULTOS, Nationwide, PenTestPartners and Underwriters Laboratory.

It is well known that the ISG SCC’s activities would not have been possible without the endorsement and membership of our sponsors. We would like to thank our past valued members of Transport for London and ITSO and the UK Cards Association. At the same time, we would like to thank ITSO for renewing their SCC membership. We look forward to establishing further collaborations with additional partners to expand the real-world significance of the SCC's research. We welcome any such opportunities for collaboration and memberships so please feel free to us at https://scc.rhul.ac.uk/partners/.

SCC Open Day

Transport for London

ITSO™

THE UKCARDS ASSOCIATION

ISG in EQUALS
Dr. Elizabeth A. Quaglia

> Lecturer in ISG

EQUALS is a global initiative started by a network of partners including UN Women, ITU, UNU-CS, ITC and GSMA, aimed at reducing the digital gender divide.
Within this initiative, the EQUALS Research Group was set up in 2017 with the aim to conduct research on gender equality, facilitate knowledge-sharing, and track progress towards reducing the gender gap in technology from all of the following aspects: access, skills and leadership.

Royal Holloway, University of London (RHUL), is an active member of this group and has been involved since its inception. Indeed, RHUL's Emeritus Professor and UNESCO Chair Tim Unwin was present at the very first UN-wide discussions, and was responsible for RHUL's prominent role in the partnership. "The initiative has tremendous potential, but much depends on how the partnership evolves. EQUALS was created as a specific partnership initiative, in which organisations were willing to commit resources in return for certain expected benefits. For RHUL, one of the benefits is thus a clear link to influencing policy at a global level, and building relationships with many of the main UN organisations, as well as the companies and other organisations involved in EQUALS. This is highly relevant, for example, to our REF profile", and Tim continues "Already EQUALS is beginning to make an impact. […] The Research Group itself has huge potential to develop innovative, collaborative, multi-disciplinary research that will really provide the evidence around women and ICTs upon which future policy can be based."

Liz Quaglia, lecturer in the ISG, attended the first physical meeting of the Research Group in December 2017 in Macau with Tim, for two full days of conversations, research exchanges and decision making. As a result, it was decided to include the important issue of security in the group's first inaugural report on the state of digital gender equality.
Liz and her PhD student, Ashley Fraser, have since worked on such report, exploring the fundamental notions of digital security and privacy from a gender perspective.

As a first step, they researched how the lack of an adequate level of knowledge in online security and privacy can have a deeply negative effect on technology users, especially women. Unfortunately, studies show that as much as digital technologies represent an incredible opportunity for growth and change, they also offer a much larger platform from which abuse can occur. Recently, the Association for Progressive Communication has pointed out that cyberstalking, online harassment, image manipulation and privacy violations have compromised women and girls' safety online and off-line in many countries. This disturbing behaviour has branched out to geo-tracking and surveillance in certain extreme cases. These considerations lead to the realisation that new technologies may expose users to an unprecedented level of threats, such as control, abuse and theft of sensitive data, caused directly by the lack of certain security properties.

Equipping women with the adequate digital knowledge and skills to ensure a more secure and private online experience could prove to be an effective way to limit this kind of abuse. Furthermore, observing women have a greater agency in the area of Information Security would certainly represent a step forward. However, when looking closer at women's involvement, it appears women are severely underrepresented in the area of Information Security. A recent report on women in cybersecurity showed a large underrepresentation of women. Globally, women only account for 11% of the cyber security workforce, and they are also more likely to hold non-managerial and entry-level positions, revealing that decision making regarding Information Security is disproportionately carried out by men.

Such imbalance in skills has led to a lack of diversity in the design and development of security solutions, reaffirming the realisation that technology, and security as part of it, is indeed gendered. There is a growing awareness that security solutions cannot be based on a single viewpoint, and need to take in consideration much more diverse design principles. Given that women have specific security and privacy concerns, working towards such diversity is of the utmost importance.

As Tim highlights, "EQUALS is a great opportunity for colleagues at RHUL to engage actively in international policy making and practice designed to ensure that we move much more swiftly towards digital gender equality. Liz and I have been active in crafting the initiative, and are very eager to enable many others in College to participate and contribute to this critically important objective."

The ISG is fully committed to this goal, as the work with WISDOM testifies, and we hope that by next year's Newsletter we will already witness, in particular, a more balanced Information Security landscape.

CASE STUDY: FOSTERING INDUSTRY-ACADEMIC COLLABORATION

Robert Carolina

> Executive Director Institute for Cyber Security Innovation

THE SHORT STORY

Working through the Institute for Cyber Security for Innovation, members of the Information Security Group joined with technology leaders at Post-Quantum (PQ Solutions Ltd) to produce a submission to the NIST Post Quantum Cryptography standardisation competition. The submission paper, "NTS-KEM", highlights a successful close collaboration between academia and industry. The paper was co-authored by Dr Martin Albrecht (RHUL), Prof Carlos Cid (RHUL), Prof Kenny Paterson (RHUL), Dr CJ Tjai (Chief Architect, PQ), and Prof Martin Tomlinson (Chairman and CSO, PQ).

THE QUANTUM THREAT

The impending arrival of quantum computing threatens the security of many existing cryptosystems. Systems are relatively secure only so long as brute force attacks remain "computationally infeasible". Quantum computing will rapidly move code breaking efforts that are currently computationally infeasible to computationally not-very-difficult. The shift, when it happens, is expected to be dramatic and would decrease or destroy the security value of widely adopted schemes like RSA and elliptic curve systems.

THE CLIENT

Post-Quantum is a London-based privately held company that develops and sells quantum resistant cryptography products and services. The company's initial product set is based on the venerable McEliece code-based cryptographic methodology with improvements that significantly increase the efficiency of the scheme. As part of their growth and development, PQ approached Royal Holloway hoping to form a relationship to enable external expert review of their cryptographic development work.

THE RELATIONSHIP

Our work moved forward in carefully scoped steps. Prof Paterson and Dr Albrecht from ISG began with an initial report that confirmed the potential viability of the PQ scheme, provided some notes to assist PQ in presenting the system to other external reviewers, and highlighted the possibility of constructing a formal security proof for the scheme. In a follow-up project, Paterson and Albrecht then constructed a formal IND-CCA security proof for the company's algorithm. This laid the foundation for everything that was to follow.

THE NIST PQC COMPETITION

In 2016, the US National Institute of Standards announced a Post Quantum Cryptography standardisation competition and invited researchers from around the world to propose new quantum resistant cryptographic algorithms. The submission deadline was November 30, 2017. PQ decided to submit their key exchange mechanism to the competition.

THE COMPETITION ROADMAP

PQ asked for assistance in preparing a submission to NIST. Although PQ's team had significant technical expertise, they wanted to describe their offering in a fashion that would facilitate analysis by the large world of cryptography experts who will be reviewing and critiquing the many competition submissions. Prof Carlos Cid of ISG stepped in to build an application framework for PQ, and he briefed the PQ team on the process of creating a competition submission.

THE INVITATION

On the strength of the relationship that had developed, PQ then invited the Royal Holloway academic team to participate formally as co-authors of the submission. What had started as discrete consultancy and coaching developed into collaboration. The Institute worked quickly with both the PQ leadership team and the ISG academic team to confirm appropriate division of responsibilities for a joint submission, and to clarify the terms of engagement to give everyone involved the confidence to move forward as a team. Arrangements were made in a matter of days.

THE SUBMISSION

After a brief period of intensive effort, the team submitted the NTS-KEM paper to NIST. The scheme is one of more than 60 to be accepted and published for evaluation and the global cryptographic research community is now studying these submissions. Some entries have already been withdrawn following the discovery of weaknesses, and we expect others will fall in due course. We will be watching the progress of NTS-KEM with interest, and we look forward to providing further support to Post-Quantum.

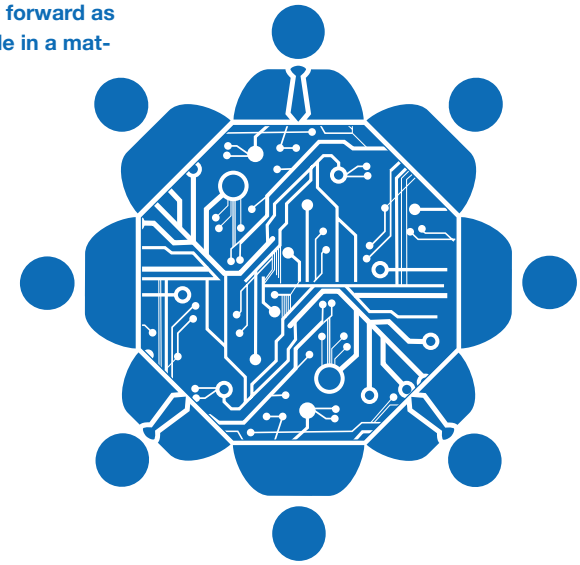
THE MORAL OF THE STORY

This project helps to showcase why Royal Holloway chose to create the Institute for Cyber Security Innovation. Fostering collaboration between academia and industry is a time consuming and challenging business. Brokering a project like this is a bit like being a movie producer. The job is part negotiator, part coach, part project manager, and not well understood by outsiders. I'm grateful for the patience and professionalism of everyone on the submission team, and for the support of Post-Quantum on this and other projects.

ARE YOU FACING A CHALLENGE?

We will continue foster collaboration with industry whenever we can. We bring academic rigour to a wide variety of cyber security domains including cryptography and network security, as well as psychology, sociology, law, and public policy. Write to me, and we can discuss your needs! Robert.Carolina@rhul.ac.uk

The NTS-KEM submission is available online at: https://nts-kem.io



RESEARCH ON THE EDGE

Prof. Lizzie Coles-Kemp & Dr. Rikke Jensen

> Prof. ISG
> Lecturer ISG

"…getting access was not a simple matter of being 'in' so to speak, but rather skating along an edge of inside and outside, an edge that tracked across multiple sites, people, encounters and indeed ways of being in."

Kenneth MacLeish, *Making War at Fort Hood* (2013)

Information security is a multi-perspectival topic where information security problems can be examined and understood from many points of view. This is because any type of security can be both a process, a felt experience and an artefact. This is clearly seen in information security where the process of making information secure is greatly influenced by feelings of insecurity and where the act of securing often involves an artefact such as a password, lock or firewall. Over the last ten years, a strand of information security teaching and research has evolved that focuses on the ways in which communities experience, make and maintain information security.

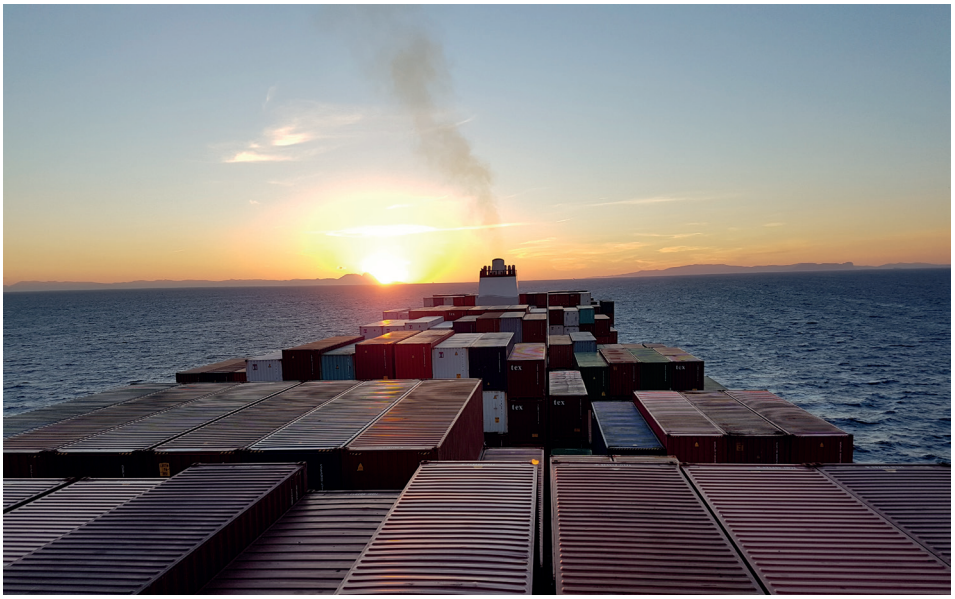
The Information Security Group has two social researchers, Rikke Bjerg Jensen and Lizzie Coles-Kemp, who, whilst often undertaking different security inquiries, both work with communities "on the edge" in terms of their geography, their position in society and their values. The edge, in these contexts, therefore constitutes a multidimensional space that is not tied to a specific location or subject matter. Researching with and within these often marginalised, underserved and unvoiced communities enables a broad understanding of how security concerns connect with everyday lived experiences. Working with such communities is valuable for enhancing both the understanding of research communities and informing policy makers on the everyday lives, concerns and experiences of such communities. However, working across, in and around such communities enables not only an understanding of the community practices themselves but also helps researchers to identify the underlying, fundamental social mechanisms that influence the creation, curation, sharing and protection of information that can be found across society.

Kenneth MacLeish's experience of working with and within one such community on the edge – the military in his case – illustrates how we as social researchers navigate multiple edges through our research practices and engagements. These edges take many forms and require flexible research approaches rooted in the everyday rhythms and routines of the individual research communities. They demand a certain sensitivity to the internal security processes and felt experiences engrained in such communities. Having worked on the edge of several communities, including refugees and migrants, families separated by prison, long-term unemployed, military families, and seafarers, the ISG's social research highlights these sensitivities whilst bridging multiple human and technological security dialogues.

Rikke's research with seafarers on how they negotiate everyday connectivities with friends and family during long periods at sea exemplifies this by revealing the extent to which the multiple, digitally facilitated connections, relations and networks, enabled through mobile devices, affect crew and individual feelings of security. Taking an ethnographic approach, living and working on board container ships, enables nuanced research insights that are sensitive to the everyday work patterns and rhythms of the ship. It highlights how the mobility of the ship, uneven and unreliable networks, limited data allowances and access restrictions raise new security questions as the ship moves in and out of digital connectivity and across multiple edges. Whilst seafarers negotiate connectivity and security through multiple channels and devices, fragmented connectivity creates a series of pressures and emotional stresses that need to be better understood by ship owners, shipping agents and charities working with seafaring communities.

Lizzie started her work on the edge in communities in the North East. The communities she worked with were coping with long-term unemployment and the challenges of social and economic deprivation. She undertook several case studies, exploring how the introduction of digital by default for essential everyday services affected the security and safety of these communities. Lizzie used creative techniques such as wall collage, storytelling and physical modelling with LEGO together with more traditional ethnographic techniques to better understand the day to day rhythms that shape the flow of information. From these studies, Lizzie has developed both theoretical and practical understandings of the impacts that digital communications have on everyday stresses and precarities and the implications these have for both the security of the individual and of the digital service.

These narratives from the edge, we suggest, need nuancing through the people, however far removed, who live closeness and distance in differentiated ways, particularly through their mobile phones, tablets and computers. The notion of "the edge" therefore holds multiple meanings for us as social researchers working with often marginalised and unvoiced communities in wider security contexts. First, the edge represents a research approach where we involve ourselves in the everyday lived experiences of our research communities and which, in MacLeish's words, requires us to "skat[e] along an edge of inside and outside" across multiple research settings. Second, the edge refers to the communities themselves and their position on the edge of society. Through these edges we learn how approaches to, and experiences of information security can be both stretched and distorted, and we identify the basic social principles that impact upon how information is understood and protected across distinct communities and societies.



WRITING FOR PUBLICATION: AN OPPORTUNITY FOR GRADUATE STUDENTS

Dr. Siaw-Lynn Ng

> Senior Lecturer, ISG

The ISG has a proud tradition of information security education. Founded in 1992, the ISG's flagship MSc Information Security masters degree programme has now produced over 3000 graduates from more than 100 countries in the world. The ISG also has a long tradition in cyber security research, and is one of the largest academic cyber security research groups in the world. In addition to academics and research assistants, there is a large group of postgraduate research student, working on topics ranging from cryptography to cyber economics.

New ideas and insights abound in such a rich environment, and besides publications in journals and conferences, we provide an opportunity to communicate these ideas more informally to other security professionals. This also allows postgraduate students to hone their technical and communication skills, to establish them as an expert in their fields of study, and to influence the development of those fields. These articles are written mainly for security professionals, and give general introductions to topics of interest, or provide analysis of current issues in cyber security, without assuming that readers have an extensive mathematical or computer science background.

One of the publication venues of these articles is the Computer Weekly ISG MSc Information Security thesis series. This is a series of informative leading-edge articles distilled from outstanding MSc projects which best present research in an area of information security of interest to information security managers and professionals. These MSc projects are re-written in collaboration with the individual ISG project supervisors as accessible short articles for a general professional readership and published online at www.computerweekly.com. As they are published by Computer Weekly we announce them on our website (https://www.royalholloway.ac.uk/isg/informationfornewreturningstudents/mscproject/thesisprizes.aspx).

Articles from past years are also listed on the website. Note that these articles are distilled from the full project reports and necessarily omit many details. Readers interested in particular articles can obtain the full reports from the ISG website (https://www.royalholloway.ac.uk/isg/research/technicalreports/technicalreports.aspx).

This year there are seven articles on topics ranging from information security culture and the protection of personal data, to the security of wireless protocols we rely on in the Internet of Things.

We depend on the internet heavily in our daily lives, and many organisations attempt to track our activities for various reasons. In "The difficulties of defending against web tracking", Darrell Newman (supervised by Geraint Price) introduces web tracking, provides an overview of how organisations track users and discusses a few of the difficulties one may face when trying to defend against it. The profusion of personal information online also leads to the question of who is responsible to keep it safe. In "GDPR: Risk, Opportunity and What It Means for Security Professionals", Neil Fraser (supervised by Geraint Price) discusses why the EU General Data Protection Regulation (GDPR) is necessary, what it means for security professionals and how it can be approached from a positive perspective. As cloud computing becomes even more pervasive as a way to store and process all this information, Christopher Hodson (supervised by Geraint Price) looks into the constituent components of public cloud ecosystems and assesses the service models, deployment options, threats and good practice considerations in "Demystifying the myths of public cloudcomputing".

Information security breaches appears to become more commonplace. In "Information security culture: A former helicopter pilot's perspective" Ashley Bye (supervised by Siaw-Lynn Ng) provides an overview of how a framework, adapted from the UK Military Aviation Authority's model for an engaged air safety culture, could be employed to reduce the prevalence and severity of cyber security incidents.

As smartphones, with NFC capabilities, are gradually becoming one of the preferred method over credit cards in contactless payments, Shana Micallef (supervised by Konstantinos Markantonakis) presents a set of risks associated with using smartphones for contactless payment transactions in "A study on the security aspects and limitations of mobile payments using Host Card Emulation (HCE) with Near Field Communication (NFC)". In "Digital Secure Remote Payment: How Apple Pay can change the future of remote payments", Marcel Fehr (supervised by Konstantinos Markantonakis) considers the role of Apple Pay's digital secure remote payment in the future of digital payments that bridge device boundary, supporting not only mobile in-app purchases also connected devices.

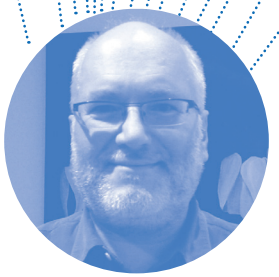
Bluetooth Low Energy (BLE) is a wireless protocol designed to consume very little power, and is increasingly implemented in more sensitive devices like baby monitors, smart-locks, biometric authentication systems and health management devices. In "The IoT BattLE", Jennifer Janesko (supervised Jorge Blasco Alis) provides a set of security guidelines, tools and considerations for anyone within an organization who is considering to acquire, implement or use BLE-enabled devices.

Another recent venue of online publication is the Infosecurity magazine (https://www.infosecurity-magazine.com/) Next-Gen Infosec series. These are very short blog-style articles from postgraduates for a readership of IT security practitioners. PhD graduate Liuxuan Pan (in collaboration with Allan Tomlinson) discusses the possible use of portforlio theory in risk assessment in her article "Risk Assessment in Information Security - An Alternative Approach". And in her article "The Cybersecurity Skills Shortage: What can Organizations Do to Tackle it?", MSc in Information Security graduate Erin L. Jones discusses what constitutes the cybersecurity skills shortage and what short-term and long-term steps can be taken to deal with it. These articles are written in a style making them accessible to everyone, and I would recommend them to anyone interested in various aspects of information security.

NEWS ON DISTANCE LEARNING

Dr. Peter Komisarczuk

> Programme Director of Distance Learning



The academic year 2017-18 has been another outstanding year for our distance learning MSc programme. The MSc Information Security distance learning programme achieved a fourth year of rising applicant and student numbers with the University of London showing 427 active students on our degree. With our increased numbers we have also increased our tutoring teams again, as several of the core modules have around 100 registered students. Likewise the pipeline of students completing the degree is increasing with over 40 students who registered for their dissertation project this academic year.

The best student prize and best project prize for graduates in 2017 went to Jennifer Janesko who undertook a very extensive project on security in Bluetooth Low Energy, she and Christopher Hodson, Marcel Fehr, Nikolas Karlsen and Heinrich Klopping presented their dissertation projects at our annual distance learning weekend conference . The conference has run for 7 years and provides a great chance for students to hear from researchers and industry speakers, meet their tutors and colleagues on the degree as well as to celebrate the achievements of the graduating students. We are looking forward to the eight conference which runs from 7th to 9th September.

As our field develops and grows we look forward to extending our master's degree. This year we will have a new module available on distance learning, which is the campus module on Human Aspects of Security and Privacy. This will be led by Dr Konstantinos Mersinas who also will become Programme Director for distance learning from 1st August. This module helps us to expand coverage and meet more of the knowledge areas (KAs) that are being documented in the CyBOK (Cyber Security Body of Knowledge) initiative funded by National Cyber Security Programme and created by a consortium of UK universities in consultation with industry and academia. The first year of consultation has developed an excellent resource that identifies 19 KAs and a top level structure that shows the breadth of our discipline and profession.

TLS 1.3 & THE ISG

Prof. Kenny Paterson

> Prof. of Information Security, ISG

TLS 1.3, the new version of the TLS protocol, has now completed development in the IETF after several years of effort, and ISG research has heavily influenced its design.

TLS is one of the most important secure communications protocols in use on the Internet today. It started life as SSL in the mid 1990s, when it was developed by Netscape for protecting credit card data and passwords in web browser sessions. It was adopted by the IETF and rebranded as TLS, with the TLS 1.0 specification being released as RFC 2246 in 1999. With the growth of the web and the Internet more generally, TLS has become increasingly important. Today, TLS is used to build billions of secure connections per day, protecting all kinds of data. There are more than a dozen independent implementations, and a thriving eco-system of software developers, hardware vendors, certification authorities and researchers all working with the protocol.

Work on TLS 1.3 began in the IETF in early 2014. There were two main motivations for designing a new version: to improve security and to improve performance. For the former, ISG-led research played a key role. For example, earlier versions of SSL and TLS allowed CBC-mode and the RC4 stream cipher for confidentiality; both of these were shown to have security vulnerabilities in two research papers published by the ISG in 2013. These attacks led directly to the decision by the TLS Working Group (WG) of the IETF to abandon these encryption algorithms and adopt only more modern Authenticated Encryption modes in TLS 1.3. For improving performance, the key focus was on reducing the number of ``round trips'' or communication flows needed during the protocol's key exchange phase, so that the overall latency before data could be securely delivered was reduced. This requirement necessitated a major redesign of the protocol, with TLS 1.3 eventually looking quite different from its predecessor. This in turn brought about the need for a new analysis effort, to ensure that the major changes did not lead to a degradation of security.

Fortunately, the TLS WG was much more open to academic input than for previous iterations of the design process. Indeed, one of the main architects of TLS 1.3, Eric Rescorla, actively sought out interns from RHUL's Centre for Doctoral Training (CDT) to join him at Mozilla to work on analysing the protocol. Thyla van der Merwe and Sam Scott answered the call, and joined Eric in Mountain View, California, for three months in the Summer of 2015. During this time, they built a symbolic model of the TLS 1.3 protocol (as it then stood) and used the Tamarin prover to study its security. This work led to a publication at the IEEE Symposium on Security & Privacy in 2016, a joint work with Cas Cremers and Marko Horvat from the University of Oxford. As part of this work, the team discovered a security vulnerability in a part of the protocol that was under design, the post-handshake client authentication mechanism. The team were able to prevent the TLS WG from taking a serious mis-step in their design. In a follow-up work published at ACM CCS 2017, this team of four was joined by Jonathan Hoyland, also from the CDT. In this second paper, the authors updated their analysis to the latest version of TLS 1.3, extended it to include more features of the protocol, and gave a finer-grained analysis of the protocol's security properties.

This pair of papers provided important assurance to the TLS WG that the protocol design was sound; they stand today as the most comprehensive analysis of the TLS 1.3 design to date. In recognition of their contributions to the development of TLS 1.3, Jonathan, Sam and Thyla are all named as technical contributors in the specification.

At the time of writing, in April 2018, the TLS 1.3 specification is reaching the final stages of development in the IETF. TLS 1.3 is already being experimentally deployed by Google, CloudFlare, Facebook, Mozilla, and others. Because of its enhanced performance - and security - it will be rolled out on billions of desktops and mobile devices in the next couple of years. The ISG can be justifiably proud of its contributions to influencing, designing and analysing this hugely important new protocol.

To read more on TLS 1.3 and the ISG's work:

TLS 1.3 specification: https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/

Webpage describing the Tamarin model of TLS 1.3: https://tls13tamarin.github.io/TLS13Tamarin/

A paper reflecting on the TLS 1.3 design process: Kenneth G. Paterson, Thyla van der Merwe: Reactive and Proactive Standardisation of TLS. SSR 2016: 160-186. (https://link.springer.com/chapter/10.1007%2F978-3-319-49100-4_7)

Research publications analysing TLS 1.3 using the Tamarin prover:

Cas Cremers, Marko Horvat, Sam Scott, Thyla van der Merwe: Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication. IEEE Symposium on Security and Privacy 2016: 470-485. (https://ieeexplore.ieee.org/document/7546518/)

Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott, Thyla van der Merwe: A Comprehensive Symbolic Analysis of TLS 1.3. CCS 2017: 1773-1788. (https://dl.acm.org/citation.cfm?doid=3133956.3134063)

CYBERFIRST

August 2017 saw 98 young people on campus for the delivery of two weeks of the CyberFirst training for 14 to 16 year olds. Students came from as far as Gibraltar to attend and were accommodated in the Founders Building and given a wide range of practical and classroom instruction on computer, mobile and network oriented cyber security topics. The CyberFirst programme is offered by NCSC and facilitated by QA Ltd, the Smallpiece Trust and local universities and provides a great way of engaging younger students in cyber security.

The CyberFirst programme is run by NCSC and offers a range of free courses, competitions, a bursary scheme and also a degree apprenticeship with NCSC aimed at engaging students in cyber security at school. The courses come in four flavours:

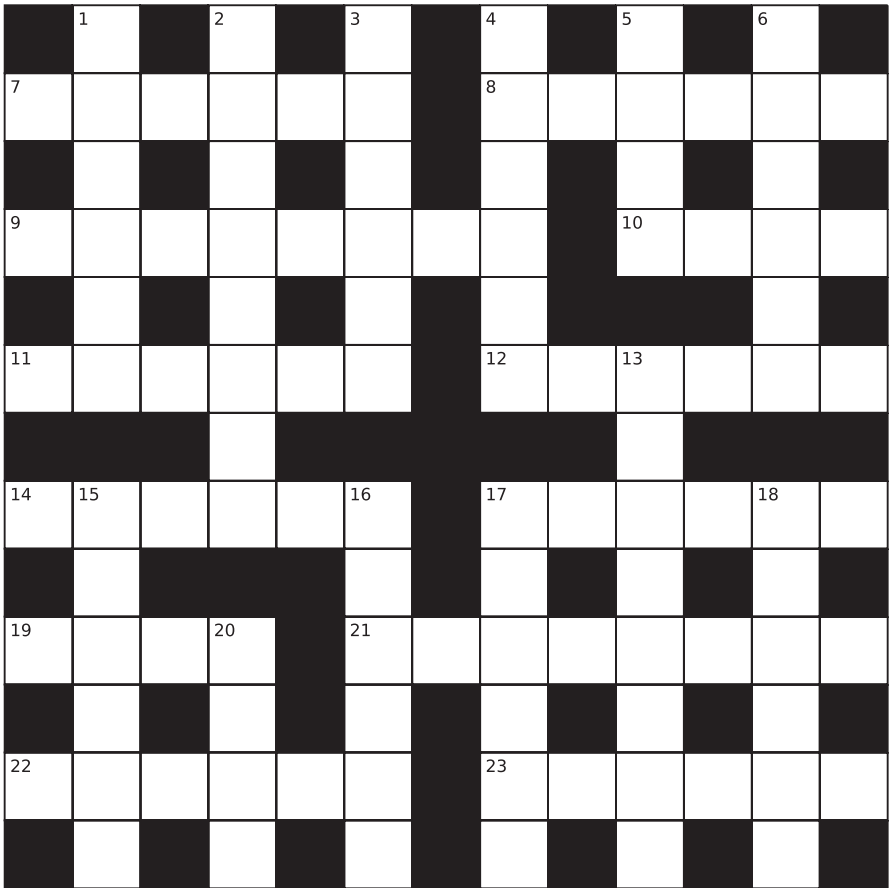
- Adventurers, which is a one day course aimed at students between 11 and 14, that have not made up their GCSE choices.
- Defenders, which is a five day residential, or non-residential course for students around 14-15 years of age that provides a practical hands on opportunity to learn to build and protect small networks and personal devices.
- Futures, which is a five day course for students aged 15 to 16. The course covers some more advanced content that explores security threats to devices, applications and software and provides a practical opportunity to investigate the ways in which we can protect them.
- Advanced, which is a five day course for 16 to 17 year olds, that is designed to complement the curriculum of A/AS levels in Computer Science or equivalent qualifications. Again the course provides classroom and laboratory based training in cyber security.

We saw 50 students attend the Futures training and 48 attend the Defenders, with presentations from Keith Martin, Rikke Jensen and Peter Komisarczuk as well as other invited speakers from NCSC, industry and the Cyber Security Challenge.

In addition to this training, CyberFirst also offers bursaries to students studying for undergraduate degrees in Computer Science and other STEM subjects, and in September a number of the Royal Holloway first year students applied for bursaries. Along with £4000 a year the students also get cyber skills training through industry placements.

This year we are looking forward to see the new and returning students for the CyberFirst Futures training course from 6th to 10th August.

CROSSWORD
by Serpent



Across answers must be encoded before entry.
The top and bottom rows identify the encoding method.

Across

7 Tremble with cold (6)
8 City of dreaming spires (6)
9 Discoverer of X-rays (8)
10 Design used as an organisational symbol (4)
11 Substance coating the surface of the teeth (6)
12 Ability to dance? (6)
14 North American edible clam (6)
17 Inert gas (6)
19 Chant (4)
21 Venture capitalist, perhaps (8)
22 Shopkeeper (6)
23 Express sorrow (6)

Down

1 Place of refuge (6)
2 Place to stop (8)
3 Place to eat (6)
4 Former pupils (6)
5 Form of wrestling (4)
6 Break in continuity (6)
13 Publicity booklet (8)
15 Related to element with atomic number 26 (6)
16 Root vegetable (6)
17 Private detective (6)
18 Remove impurities from liquid (6)
20 Vehicle for hire (4)

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

Twitter:
twitter.com/isgnews
@ISGnews

LinkedIn:
linkedin.com/groups?gid=3859497

You Tube
youtube.com/isgofficial

CONTACT INFORMATION:

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

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

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