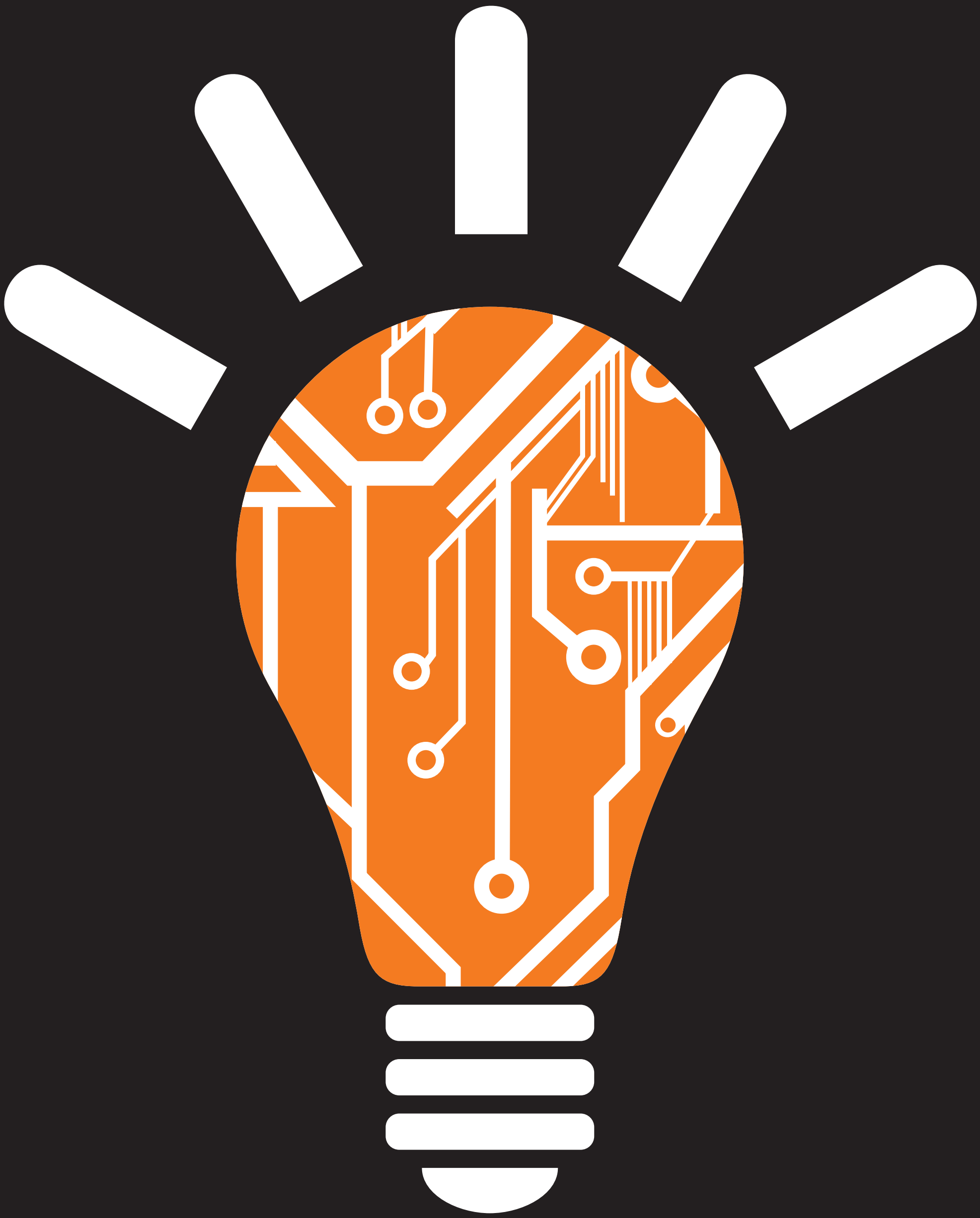
Information Security Group

Review 13/14



ROYAL HOLLOWAY UNIVERSITY OF LONDON

LETTER FROM THE ISG DIRECTOR

I am delighted to introduce the annual review newsletter of the Information Security Group at Royal Holloway, University of London.

The ISG is now over twenty years old and has been in constant evolution since its pioneering formation in the early 1990s. Back then there were very few academic groups focussing on cyber security anywhere in the world. In recent years, with the rise in importance and interest in this area, many universities have developed information security teaching and research programmes. However, Royal Holloway continues to pioneer new academic initiatives in cyber security.

In 2012 the Information Security Group became a university department in its own right, located within the Faculty of Science next to more conventional academic units such as Computer Science, Mathematics and Physics. Recognising Information Security as a distinct academic activity, albeit one with many closely forged links with other disciplines, makes Royal Holloway unique in the UK, and recognises the strength that we offer in this area.

This year Royal Holloway has launched a new Institute for Cyber Security Innovation. The Institute will complement the academic work of the ISG by offering a more industry-facing focus. For example, the Institute will foster incubation activities, conduct industrial research projects, and support continuous professional development training. This new initiative will greatly expand Royal Holloway's already impressive capabilities to engage meaningfully with the wider cyber security industry. You can read more about the Institute elsewhere in this review.

We were also delighted to launch our new Centre for Doctoral Training in Cyber Security in 2013. This extremely exciting project is funding ten PhD studentships per year, for three years in the first instance, and has already attracted some brilliant new research talent into the university. You can meet the team, and learn more about the CDT, in this review.

This is the eighth year that we have produced our annual review newsletter. Flicking through back issues (which are all available on our website) I continue to be proud of the depth and diversity of our activities. I am sure that you, too, will find something of interest.

We'd be delighted to explore how you could work with the ISG, or with the new Institute for Cyber Security Innovation. Please do get in touch if you want any more information on any of our activities.

Professor Keith Martin

INDEX

NEW COMPUTER SCIENCE UNDERGRADUATE DEGREE PROGRAMMES WITH INFORMATION SECURITY

In September 2014 a new set of Computer Science undergraduate degree programmes with an information security focus will start at Royal Holloway.

The launch of the new programmes is in response to the growing need for graduates who can shore up defences against the cyber threat that businesses, governments and individuals are facing. According to a National Audit Office report published in 2013, the number of professionals with information security skills in not increasing in line with the growth of the Internet: "it could take 20 years to close this skills gap".

In these new degrees, information security will be taught in an integrated fashion, with all students learning basic computer science principles as well as specialist courses introducing them to critical and highly relevant aspects of cybersecurity, including computer and network security, malicious software, and cryptography.

This is important because students need a solid understanding of how computer systems operate and communicate in order to fully master the techniques through which security attacks can be prevented or acted upon.

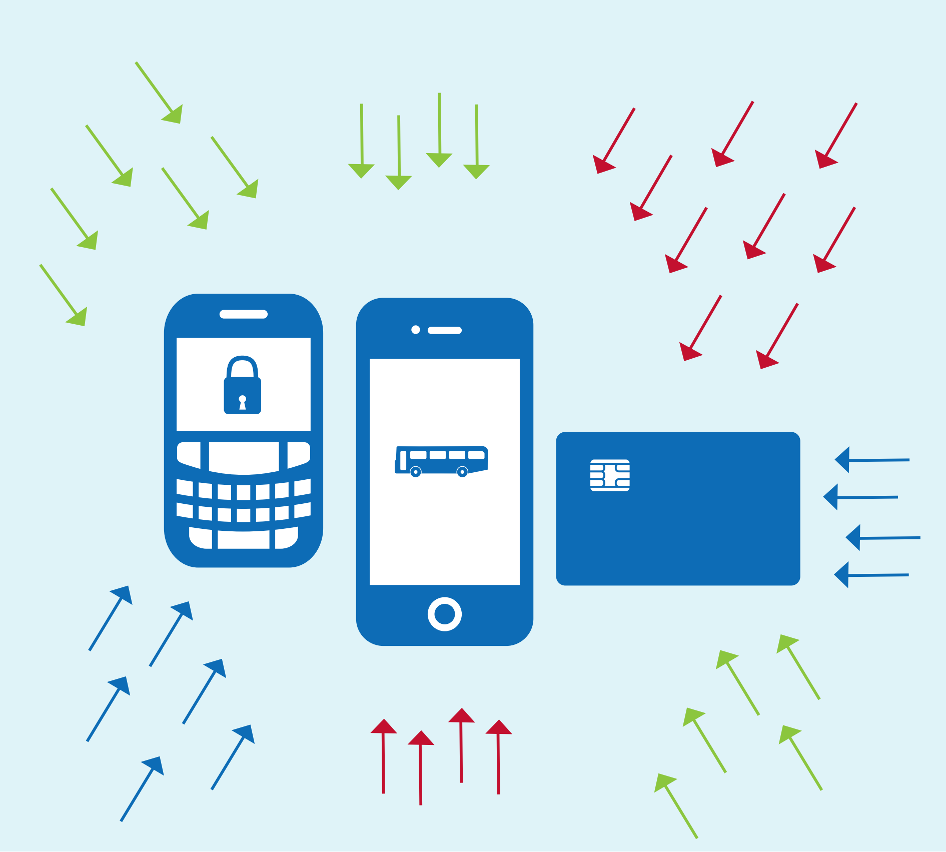
There will be four new programmes in total: a BSc Computer Science (Information Security), which is a three-year bachelors-level degree; an MSci Computer Science (Information Security), which is a four-year integrated-masters in which students will be able to choose courses from Royal Holloway's MSc Information Security in their final year; and a Year-in-Industry variant of each of those degrees, where students can take a year out on a placement.

The first year of all of these programmes is the same as the standard Computer Science degree at Royal Holloway, which is focussed on giving students a grounding in writing software and understanding the relevant mathematics for Computer Science. In the second year, one quarter of the courses the students take are in information security, including a hands-on hacking-oriented computer and network security class. Students also learn about software engineering, algorithms, databases, operating systems, and system-level programming. In the third year, students take more courses in malware and cryptography. The second half of that year will give the students the opportunity to learn about other advanced Computer Science topics such as bioinformatics, machine learning, or software verification. Students will also find out how such advanced topics play a fundamental role in information security, and their contribution to the development of a successful professional career.

All these degrees have a very strong project component. A team project in software engineering runs in the second year of their studies where they learn about Scrum-based Agile Development. Students conduct an individual project in an information-security related topic of their choice that counts for 25% of their third year. In the MSci, an individual project represents 50% of the fourth year, where students submit a masters-level dissertation backed up either by a research project or a more substantial development project.

The Information Security Group (ISG) will be responsible for the teaching of all information security courses and the supervision of individual projects. "We're very excited by the prospect of these degrees," said Dr Lorenzo Cavallaro of the ISG, who has been helping to develop the new programmes. "In order to develop a deep understanding of Information Security it is vital that one first has a grounding in the principles of Computer Science. We are sure that this excellent set of programmes will be popular with students."

Prof. Keith Martin, Director of the ISG, thinks that the balance between computer science and information security on these new programmes is right: "We have often been asked about the possibility of offering a BSc in Cyber Security, but we feel that Information Security as a discipline is best built onto a core skill area such as Computer Science. We're really looking forward to working more closely with our colleagues in Royal Holloway's Computer Science Department to make a success of this new venture."



AN UPDATE FROM THE SMART CARD CENTRE
By Keith Mayes

> Prof. Keith Mayes is Director of the ISG Smart Card Centre

In 2013 the ISG Smart Card Centre (SCC) celebrated its eleventh anniversary, but without the usual fanfare of the open-day exhibition due to the commitment of SCC staff and students to supporting ESORICS 2013 and its seven co-located workshops. We are pleased to announce that the SCC open-day exhibition makes its comeback this year, so reserve a place in your diary for Tuesday 2nd September 2014.

We are delighted that several MSc students working with the SCC last year enjoyed considerable success with their projects. Thyla van der Merwe was awarded the ISG best project award for her work considering elliptic curve technology for transport ticketing systems, and Pallavi Sivakumaran won the BCS David Lindsay prize for her analysis of Android memory security. From the 25 SCC project students, four were selected for Search Security Awards and will be presenting their work in articles for Computer Weekly.

Last year saw the end of Orange Labs' three-year sponsorship of the SCC and we thank them for their valued support and expertise. A pleasing outcome is that they have now employed an SCC PhD student who was working on the mobile-research thread. This year the SCC is delighted to acknowledge some new sponsorship from Visa, which will allow recruitment of a Research Assistant in order to boost the payment and transaction research currently supported by the UK Cards Association. We are currently funding a PhD student to work in this area, as well as one for our transport-related research. Although our work is split between these different research threads, there is considerable overlap, especially where mobile devices are concerned, since they seem to be part of many industries' future strategies. The work on enabling smart technologies such as RFID/NFC, secure platforms, attacks and biometrics is also on-going and evolving, with some innovative applications to gesture authentication, virtual worlds and securing difficult environments.

Last year we reported on some game-changing developments in transport (the use of EMV cards as tickets). This year there are some changes that could affect many industries and services that use mobiles and tamper-resistant security modules. For example, the NFC phone standards define the Security Element (SE) as the safe place to put your smart card/RFID emulation. There are several options in the standards, but the general view (from a security viewpoint) was that the SE should use specialist attack-resistant hardware, e.g. a chip embedded within the phone hardware, on a secure memory card, or hosted within the network operator's UICC (supplied for the SIM/USIM functionality). Which SE to use, who is in control of it and who they will allow to use it, are thorny issues and the uncertainty has done nothing to encourage developers to create new services.

So what has changed? Well, Google has announced a new version of the Android OS called "Kit Kat" and, with over 70% of the world's phone market, its capabilities cannot be ignored. If the NFC interface of such a phone comes within range of a smart card reader the communication no longer goes directly to a pre-determined SE, but instead to the phone OS to find the appropriate handler. Potential SEs/equivalents need to be registered with the OS and Google is encouraging the use of Host Card Emulation (HCE), which is basically emulating your smart card/RFID within a phone app. Blackberry were the first to offer HCE, but as a niche supplier this did not create the same impact as the Google announcement.

In case you have missed the significance of this development, it is equivalent to a software-only security module, which normally has no physical, side-channel or fault-attack protection. Being in a phone, this may be vulnerable to a whole host of other threats such as malware, viruses, remote access, etc. If we consider this from an information security purist's viewpoint (or that of a traditional card service provider) then we might be appalled at the removal of security protection and thus fear future attacks on services.

However, the picture is a little different if we consider service creation. The SE is designed to have good security properties but the multiple options, and the fight around who owns and controls the SE, mean that most developers have almost no opportunity to create consistent services that make use of it. History shows us that if hardware security is not easily available then services will appear anyway, and phone apps already abound that risk our sensitive and private data. The security situation is not completely bleak since future phone processors may have a little more extra protection than today, with the idea of the Trusted Execution Environment (TEE) that has some hardware support to segregate secure and non-secure functionality. This may help against viruses, malware and general remote mischief, but it seems not to address physical, side-channel and fault attacks.

The SCC continues to attract students and companies to carry out innovative research projects. This research arena is kept fresh by a range of significant industry and technological developments, and the SCC evolves its activities in order to keep pace. The Host Card Emulation capability will no doubt send shockwaves around the service provision industry, especially if accepting the principle of a software SE means eventual acceptance of the software SIM. Fellow veterans of the mobile telecoms industry will remember the cloning issues from the last time that we relied on phone software based authentication, so let us hope that history does not repeat itself with shiny new technology. In any case the future will not be dull!

THAT LITTLE THING KNOWN AS THE MSC PROJECT
By Pallavi Sivakumaran

> **Pallavi Sivakumaran is a former MSc student in the ISG, now working as a Systems Engineer at Hughes Network Systems**

"Project": a word that strikes fear into every MSc student's heart and holds within it the promise of three months of sleepless nights, anxiety and tears! The first time it was mentioned, I felt a chill down my spine. (Although, that could just have been because it was winter in the UK…)

In all seriousness, the project was a far more daunting prospect - to me, at least - than even the MSc examinations (and the exams are pretty challenging, as anyone who has taken them will tell you). The reason for this might be partly to do with the uncertainty that is associated with the project. With exams, you know to a large degree what will be covered, the materials to refer to, and the preparatory work you should undertake. The main things you don't know beforehand are the exam questions! With the project, especially during the initial stages, there are a lot of unknowns, the primary one being the project topic. In my case, I had an idea that my project was going to be in the area of mobile security, but the exact details were very vague. Fortunately my project supervisor, Prof. Keith Mayes, was able to help me by explaining which of my ideas were feasible and how I could fine-tune them to decide on a project that was both fairly substantial, but also possible to be completed in the given time.

Analyzing Application Data Security on Android Devices was the topic I finally decided on. With more and more businesses publishing mobile applications, and with those applications increasingly handling sensitive personal and corporate information (banking and financial information, user login credentials, and potentially even corporate IP are some examples), the subject of application data security seemed very relevant. Android was selected as the target test platform because of its widespread usage and accessibility, and the project analysed the security that is inherently afforded by the Android operating system to data belonging to a third-party application.

To do this, I developed a mobile application which wrote data to known locations on an Android phone and then made use of physical and logical data acquisition methods to try to retrieve the data from the device. This experiment showed that application data stored on external memory could be recovered, not only while the application was still installed on the device, but also after the application was removed from the device and different applications installed. The experiment was then re-run after rooting the phone (which is essentially the process of obtaining root or superuser privileges for the device), to test for the effect of this procedure on data security. This second test showed that data on the device's internal memory (which had previously not been recoverable) was now vulnerable to retrieval. I also conducted additional tests to determine data longevity after erasure and the effectiveness of root hiding mechanisms, and proposed steps that could be taken during application development to safeguard sensitive data.

Looking back, I would say that working on the project was a very rewarding process. I gained a lot of knowledge regarding my chosen subject, as well as about various related technologies. But even more, given that it was the first time that I undertook an individual project of this scale, I also learned about time and project management. And once the project was underway, I found myself actually enjoying working on it. That isn't to say that there weren't setbacks - it seems to be the nature of projects that at least one thing will go wrong about halfway through. It's also not to say that I didn't heave a great sigh of relief once I'd completed the project and handed it in. But, overall, it was a great learning experience.

The icing on the cake was when, about three months after submitting the project, I received an email from Programme Director Dr Chez Ciechanowicz informing me that I had been awarded the BCS David Lindsay prize for my project. That was honestly one of the biggest surprises since, although I had heard of the prize before, I never thought I had any chance of actually winning it.

I feel very honoured that my project was even considered, and would like to thank the British Computer Society who awarded me the prize. None of this would have been possible if not for the involvement of so many others: namely my supervisor, who guided me throughout; the entire ISG staff, who work so hard to make this MSc programme available; and, at the risk of sounding so very clichéd, my family and friends.

I'd like to end with some advice to all MSc students concerning projects: Put your best efforts into it and enjoy it (yes, seriously). All your hard work will surely pay off in the end.

RESEARCH ROUND UP

//
Multilinear Maps

Prof. Kenny Paterson has been awarded a new research grant by EPSRC, the UK's main science funding body. The grant provides funding for Kenny and two postdocs for a period of three years. The team will investigate a new and rapidly developing area of research: multilinear maps. These hold great promise for enabling new cryptographic functionalities, but new research is needed to properly understand the security they offer, to develop suitable cryptographic abstractions, and to develop new cryptographic schemes that make use of them. All of these aspects will be explored in the project.

The project builds on collaboration with Prof. Dennis Hofheinz of TU Karlsruhe. In addition, the grant reunites the ISG with Prof. Steven Galbraith from the University of Auckland, who will be a visiting researcher providing cryptanalytic expertise, and postdocs Dr Martin Albrecht, who will conduct cryptanalysis, and Dr Pooya Farshim, who will develop new cryptographic schemes making use of multilinear maps.

//
Cryptography for Secure Digital Interaction

A new network of European research centres focusing on cryptography will be launched this spring, with more than 20 partners from 15 countries. The COST Action "Cryptography for Secure Digital Interaction" will bring together European experts working in different sub-areas of cryptography (e.g. symmetric cryptography, public-key cryptography, protocol design and analysis), to stimulate cooperation between the different national efforts for developing and analysing cryptographic solutions for secure digital interaction between citizens. As with other recent European-wide research networks in cryptography (ECRYPT and ECRYPT II), Royal Holloway is one of the main partners in this new COST Action.

Dr Carlos Cid is one of the UK representatives in the COST Action Management Committee, and will work to stimulate participation of UK-based researchers in cryptography in the research network.

//
Internet of Energy

The project "Internet of Energy" funded by the EU ARTEMIS JU programme began in May 2011 and will extend until the end of October 2014. It brings together a large consortium consisting of 42 European partners from academia and industry, with the aim of developing a combination of hardware, software, and middleware for the seamless and secure connectivity and interoperability between the Internet and energy networks, with particular applications in the area of electric mobility.

This objective requires secure and reliable end-to-end communication among generators and loads, which in the case of electric mobility are varying not only over time but also in location. Unlike in conventional power networks, smart grids seek to enhance efficiency through avoiding massive over-provisioning and instead rely on real-time energy balancing and demand response. This requires that measurements and the communication of current and future demand, as well as demand control and response, are trustworthy, reliable, and secure. Moreover, communication and computation will often have to satisfy real-time requirements.

Recent work on this project by Alessio Baiocco, Chris Dowden, Yangyue Feng, and Stephen Wolthusen has concentrated on secure communication over restricted networks, and particularly on the notion of robust state estimation in dynamic smart grid environments. State estimation is performed both in micro-grid environments, and also at larger scales, to ensure that supply and demand for energy are always in balance and interacting with energy pricing systems. Such systems are inherently distributed and must give an accurate view of current network state based on partial information and measurements.

Whilst conventional state estimation can effectively deal with random faults and missing data, recent research has revealed that fault injection by attackers can lead to erroneous state estimation, even for relatively limited numbers of compromised measurements. By extending the concept of state estimation to a hierarchical state estimator, work within the project has enhanced the robustness of state estimators to a number of attacks. This has resulted in recent publications in the 2014 IEEE PES flagship Innovative Smart Grid Technologies (ISGT) conference, the 2013 ACM e-Energy conference, and the 2014 ISGT Asia conference.

//
Mining the Network Behaviour of Bots

This is a £680K three-year project investigating novel (use of) machine learning techniques to infer the behavioural traits of bots (hosts infected with malicious software). The project is led by Dr Lorenzo Cavallaro from the ISG's new Systems Security and Malware Analysis (S2Mal) Lab. The project team also consists of Prof. Gammerman, Dr Luo, Dr Shanahan, and Prof. Vovk (all from Royal Holloway's Department of Computer Science) and two PostDocs (Dr Nouretdinov and Dr Wang). Between them, the project team has combined expertise in machine learning, network analysis, bioinformatics, network and systems security, and malware analysis detection. The project is also engaging with external organisations, including Nominet, McAfee Labs UK, and HP Labs Bristol, which will provide real-world data.

Our initial line of enquiry within the project is being conducted in collaboration with Politecnico of Milano, Italy. Modern botnets rely on domain-generation algorithms (DGAs) to build resilient command-and-control infrastructures. We are currently investigating DGA-based botnets. Recent works focusses on recognizing automatically generated domains (AGDs) from DNS traffic, which potentially allows identification of previously unknown AGDs to hinder or disrupt botnets' communication capabilities. State-of-the-art approaches require low-level DNS sensors to be deployed to access data. However the collection of this data raises practical and privacy issues, making adoption problematic. A mechanism is being proposed that overcomes these limitations by analyzing DNS traffic data through a combination of linguistic and IP-based features of suspicious domains. In this way we are able to identify AGD names, characterize their DGAs, and isolate logical groups of domains that represent the respective botnets. Moreover, this system enriches these groups with new, previously unknown AGD names, and produces information about the evolving behaviour of each tracked botnet.

This new system has been used in real-world settings to help researchers who requested intelligence on suspicious domains and was able to automatically label them as belonging to the correct botnet. Additionally, an evaluation was run on 1,153,516 domains, including AGDs from both modern (e.g. Bamital) and traditional (e.g. Conficker, Torpig) botnets. The approach correctly isolated families of AGDs that belonged to distinct DGAs, and distinguished between automatically-generated and non-automatically-generated domains in 94.8% of the cases.

//

Malware and Security in the Mobile Age

Lorenzo Cavallaro from the ISG's S2Mal Lab is leading an exciting new four-year project MobSec, funded to the tune of £750K by the EPSRC under the BACCHUS research funding call. The project will also benefit from co-investigation by Johannes Kinder from the Department of Computer Science at Royal Holloway, and is conducted in partnership with McAfee Labs UK.

With more than one billion activations reported on September 2013, Android mobile devices have become ubiquitous, with trends showing that the recent pace of adoption is unlikely to slow down. Android devices are extremely appealing: powerful, with a functional and easy-to-use user interface to access sensitive user and enterprise data, they can easily replace traditional computing devices, especially when information is consumed rather than produced. Application marketplaces such as Google Play drive the entire economy of mobile applications. For example, with more than one million installed apps and a market share of 35%, Google Play has generated revenues exceeding nine billion dollars.

Such a wealthy and quite unique ecosystem with high turnover and access to sensitive data has unfortunately also attracted the interests of cybercriminals, with malware now hitting Android devices at an alarming rate. Privacy breaches (e.g. access to address book and GPS coordinates), monetization through premium SMS and calls, and colluding malware to bypass two-factor authentication schemes, have become real threats. Recent studies report how mobile marketplaces have been abused to host malware, or seemingly legitimate applications embedding malicious components. This clearly reflects the shift from an environment in which malware was developed for fun, to the current situation where malware is spread for financial profit. According to the security roadmap provided by the European Network of Excellence SysSec, "more research focussed on the development of defensive tools and techniques that can be deployed to current smartphone systems to detect and prevent attacks against the device and its applications is needed". To this end, MobSec aims to explore mobile-related threats and develop comprehensive mitigation techniques. In particular, the MobSec research agenda will revolve around the following themes.

a) Mobile application analysis to build the necessary knowledge for understanding the new slew of cyber-criminal mobile-related threats we are facing.

b) Development of evasion-resistant information leakage solutions to replace (or complement) state-of-the-art approaches vulnerable to easy-to-deploy evasion attacks.

c) Detection of malicious mobile applications.

d) The exploration of hardware-supported virtualization to provide efficient in-device mitigations against mobile threats.

//

Cyber Security Cartographies

Now into its second year, the CySeCa (Cyber Security Cartographies) project has already made its mark when it comes to attracting the attention of those in industry. The project goal is to develop interventions and tools which can be used to support the decision-making process for those making security-relevant decisions.

Probably the main output to date has been the use of interviews, in combination with the application of suitably robust analysis techniques, to provide a `baseline' of the experiences of a range of security practitioners in industry. These interviews have provided some very insightful and surprising findings; for example, the sheer variety of answers which were received when the question "what is your definition of information security?" was posed. Some interviews crucially highlighted the fact that technology is only part of the puzzle, and that a lack of more general skills, such as critical thinking, interpersonal skills, etc., are seen as key inhibitors to the building and developing of suitably experienced personnel.

One of the outputs of these interviews was the innovative use of comic strips to demonstrate the experiences of those who are making decisions. This will be taken forward in the next phase of the project to collect and display the multiple perspectives which are important in the processes which are being analysed. This has been greeted very warmly by those in industry who have seen the work to date. Using novel techniques like this should allow the project to develop a richer narrative for security practitioners which helps them reflect on the problems faced in their day-to-day role, and ultimately seek out solutions to some of those problems.

As well as the sociological work, there has also been a parallel technical piece which is in the process of developing novel techniques to map and identify convergent behaviours through the use of machine learning techniques. One of the innovative ways in which this work differs from previous uses of these techniques is to take an agnostic view of the observed behaviours. In this, the ultimate goal is to improve the availability and presentation of the information to the decision makers, rather than have the tools themselves make the decisions on our behalf.

Ultimately, there are two overarching goals to CySeCa: to integrate the research conducted at the technical level with the sociological and user experience level to enhance the quality of, and speed at which, the information is available; and to develop new and innovative techniques of presenting this information to decision makers. From the feedback received so far from the `target audience', it is clear that CySeCa is creating something of genuine interest to those in industry. The novel model of interaction used in the project will surely only become more relevant over time.

The CySeCa team is Lizzie Coles-Kemp, Makayla Lewis, Davide Papini, Lorenzo Cavallaro, Allan Tomlinson and Geraint Price.

//

International Technology Alliance

The ISG has been now involved in the International Technology Alliance (ITA) project for several years. Funded by UK MoD and the US DoD, this collaborative research project has the participation of over 20 universities and companies from both sides of the Atlantic, conducting cross-disciplinary research on the security of communication and information services for military coalition operations.

A specific current focus of the project is the development of new cryptographic techniques to support outsourced and delegated computations, to be deployed securely in hybrid coalition networks. Dr Carlos Cid worked in collaboration with researchers from University of Maryland in the proposal of a novel secure outsourcing computation scheme ("Multi-Client Non-Interactive Verifiable Computation"), which was presented at the TCC 2013 conference in Japan. Dr Cid and colleagues in the ISG also considered the problem from a totally different angle: one can incorporate incentives to the design of outsourcing computation schemes, and deal with the problem using game theoretic tools ("Optimal Contracts for Outsourced Computation").

The ISG has also been collaborating with IBM-UK in the design of a distributed authentication mechanism for decentralised networks (such as deployments of the Gaian database, a dynamic, distributed and federated database developed by IBM-UK). The work was presented at the ITA Autumn event in October 2013 in New York ("Decentralised Certificateless Public-Key Infrastructure"). The current phase of the ITA project continues until May 2015.

ISG RUNS ITS FIRST MOOC

In June 2013 the ISG embarked on a new adventure by running its first Massive Open Online Course (MOOC) on the Coursera online platform. MOOCs provide open access to short online courses. The ISG's first MOOC was prepared, delivered and supported by Lorenzo Cavallaro and entitled Malicious Software and its Underground Economy: Two Sides to Every Story. It was one of seven courses offered by the University of London International Programmes through Coursera.

Lorenzo's course mixed a practical, hands-on approach with the theory and techniques behind the scene, to discuss current academic and underground research in the field, trying to answer the foremost question about malware and underground economy: "Should we care?"

The format of Coursera MOOCs consists of short video/audio segments alongside formative assessments, with the addition of hands-on challenges to be completed by the students as self-assessed study. Lorenzo's course featured 27 such videos, totalling over seven hours in length. The course ran over six weeks and was fully supported online. This involved a great deal of preparatory filming, and a substantial amount of support work while the course was running.

The statistics for the course are fairly staggering. Over 40,000 students around the world registered to take the course. Of these, around 21,000 were active during the first week of study. Impressively, over 6000 of these students remained active by the final week. In the end, over 2,500 students were issued with Statements of Accomplishment.

Lorenzo was delighted with the results. "The course preparation required a lot of time, but active forum participation throughout the class contributed to an even higher workload. Feedback from students was very positive - some of them particularly thanked us for giving them a chance to get access to academic-quality research, influencing deeply their perspective (and knowledge) on this important security topic."

The question that is really engaging the higher education sector is whether MOOCs are the future, or just a passing trend. Our limited venture into the world of MOOCs suggests that they are amazing courses to engage with. The global reach of this MOOC can certainly have done no harm to Royal Holloway's international reputation. In terms of tangible results, apart from Lorenzo getting recognised in the street (!), we had at least half a dozen registrations for our distance learning MSc Information Security from students who mentioned having completed Lorenzo's course. So, if nothing else, MOOCs are good advertising mechanisms.

Malicious Software and its Underground Economy: Two Sides to Every Story, will be running again from April 28th, 2014. Come and join the party!

INSTITUTE FOR CYBER SECURITY INNOVATION

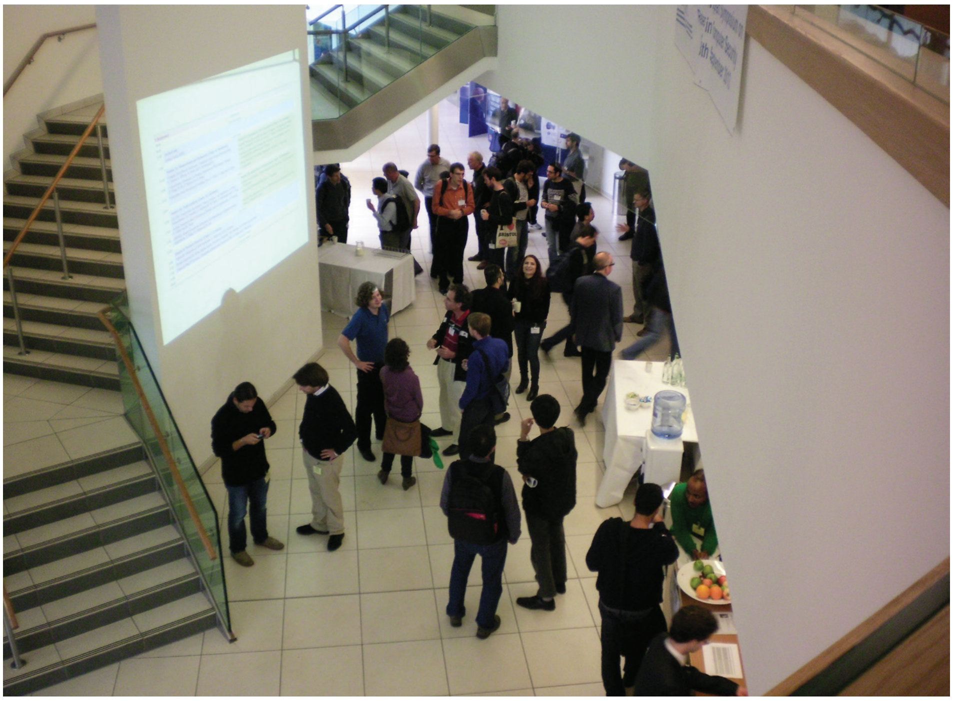
Royal Holloway recently announced its commitment to establishing an Institute for Cyber Security Innovation, to build on the ISG's world class presence in this area. The Institute's mission will be "to bring together Academia, Industry and Government to be a catalyst for innovation in Cyber Security policy, research and solutions on a scale that has real impact, generates significant economic growth and delivers a more secure cyber environment for us all".

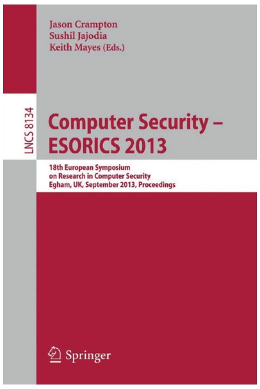
The strategic plan for the Institute is ambitious and the College has mapped out a 10-year programme culminating in the establishment of substantial purpose-built premises, some occupied by major cyber security companies, and at least 20 incubation start-up companies. There will be a dedicated venture fund for these start-ups.

In addition to incubating start-ups, the Institute will concentrate on commissioned applied research (Technology, Policy and Human factors) and CPD training.

Although it is still in its infancy, the idea of an Institute at Royal Holloway has been welcomed enthusiastically by a number of large organisations, many of whom already have close links and working relationships with the ISG. Indeed it is the proven track record of the ISG and their long standing tradition of industrial collaboration that instigated the formation of the Institute. There is clearly, and understandably, significant activity in cyberspace and the profile of cyber security is increasing. Thanks to the activities of the ISG and their ever increasing network of over 3,000 alumni, Royal Holloway is uniquely placed to act as a catalyst for uniting the cyber security community.

ESORICS 2013





Jason Crampton
Sushil Jajodia
Keith Mayes (Eds.)

LNCS 8134

Computer Security – ESORICS 2013

18th European Symposium
on Research in Computer Security
Egham, UK, September 2013, Proceedings

Springer

In September 2013, Royal Holloway hosted the 18th European Symposium on Research in Computer Security (ESORICS 2013). Prof. Jason Crampton from the ISG was the co-chair of the Programme Committee alongside Professor Sushil Jajodia of George Mason University (USA). Prof. Keith Mayes (Director of the Smart Card Centre) was the General Chair.

ESORICS is the premier venue in Europe for the dissemination of research in all aspects of computer security. The aim of ESORICS is to further the progress of research in computer security by establishing a European forum for bringing together leading researchers in this area, in order to promote the exchange of ideas with system developers and by encouraging links with researchers in related areas. ESORICS started in 1990 and has been held in several European countries, attracting an international audience from both the academic and industrial communities. ESORICS was last hosted in the UK in 1994, so it was a great honour for Royal Holloway to be chosen as the venue for ESORICS 2013.

A further seven workshops (Cryptoforma, Data Privacy Management, EuroPKI, Quantitative Aspects in Security Assurance, Autonomous and Spontaneous Security, Security and Trust Management, Trustworthy Clouds) - a record number - were co-located with ESORICS 2013.

Over 320 delegates attended the conference and affiliated workshops. ESORICS 2013 itself attracted over 240 submissions from 38 countries, of which 43 were accepted. The conference programme included two papers co-authored by members of the ISG. The best paper prize was awarded to researchers from Bristol University for work on improving the performance of secure multi-party computation.

The conference presentations took place in the main auditorium in the Windsor Building. The conference was a great success, with the delegates being impressed both by the state-of-the-art facilities in the Windsor Building and the grandeur of Founder’s Building and the Picture Gallery, where the conference dinner was held.

The success of the conference depended, in large part, on the efforts of an army of local volunteers, drawn from the administrative staff, as well as PhD students in the ISG and the Department of Mathematics. Special thanks go to Sheila Cobourne and Emma Mosley for all their efforts.

ALUMNUS INTERVIEW: NICK PESTELL

//

Tell us a little about yourself.

My name is Nick Pestell and I was born in Johannesburg, South Africa. I developed varied IT skills at a very young age: mostly as a programmer for my father's business, but later as a systems administrator when my interest in hacking and security evolved.

Towards the end of my first year of university as a computer science major, I found myself staring down the wrong end of a gun and promptly immigrated to the UK, my parents' homeland. After acquiring some popular certifications, I found my skills in high demand and worked around Europe wherever the money trail took me. Whilst working on a large PKI implementation in Luxembourg I met my current business partner and Royal Holloway alumnus Richard Mulholland who introduced me to Royal Holloway's Information Security MSc programme. Post Royal Holloway, I lived and worked in London for a few years before moving to Malta where I have been living for the last five years, together with a large Maine Coon and my partner, overlooking the sea at Sliema.

//

Tell us about your company IVPN .

IVPN provides a security and privacy service for consumers and small businesses. The words 'privacy' and 'security' are an important distinction since VPN technology can be used for many other purposes such as bypassing geographic content restrictions, bypassing government censorship, and downloading copyrighted content without fear of reprisal. The purpose of our service is to defeat passive surveillance of our customers' Internet activity by their ISPs, and at the same time provide additional security when connecting to the Internet from an untrusted network, e.g. public Wi-Fi. When a customer subscribes to our service they receive VPN client software and credentials to access our network. The idea is to remain connected to our network 24/7, ensuring that no unencrypted traffic passes through the ISP.

We have used all of our industry experience to build a highly secure network, following strict Center for Internet Security (CIS) benchmarks for server builds and designing an exclusive multi-hop network where traffic is routed through two or more separate jurisdictions. Adversaries typically use traffic analysis and various 'timing' attacks to locate the source/identity of a traffic stream. Thus by having a connection to our network in one location and the traffic exiting in another jurisdiction, it is significantly more difficult to be in a position to perform those attacks. However, it's important to note that although our service provides a degree of anonymity if you are an active target, we don't pretend that using our network will be much of a deterrent. Our technology in no way replaces the use of high anonymity tools such as TOR. Look at our guides on combining TOR with a VPN - https://www.ivpn.net/privacy- guides to see how they can complement each other in order to achieve very high levels of anonymity. On its own our network is designed to subvert passive/ dragnet surveillance with the ISP as the threat/adversary, not the NSA.

//

Tell us about the formation of IVPN.

After graduating from Royal Holloway my business partner Richard Mulholland and myself started contracting as risk analysts for various banks in London. My responsibility was to assess the security risks that new technologies were introducing to the organization and communicate that risk to the business. I found myself working on several projects where vast amounts of data were being collected about the banks' customers. When data about an individual is aggregated from dozens of databases, either collected in-house or bought from a data brokerage, the result is an identity captured so fully that even the individual who owns the data would learn something about themselves.

As a result I quickly become concerned about how my own personal data was being bought and aggregated. I researched every privacy enhancing technology I could get my hands on and found that generally they were surprisingly complex to implement and, if misconfigured, could potentially engender a false sense of security; a situation often much worse than no security at all.

Clearly there was a large gap in the market for user-friendly privacy enhancing technologies and we were looking for an exit from the corporate world we'd become so mired in. I've always considered the ISP to be in the best position for data collection since all of a customer's Internet traffic passes through them. Today we see that legislation such as the EU data retention directive has been introduced to force ISP's to retain records on every one of their customers as well as enforce various censorship laws. For this reason, setting up a service which encrypted all data passing through an ISP would be commercially feasible, and VPN technology was mature and cheap to implement for both consumer and business solutions. With our backgrounds in security and passion for privacy we incorporated IVPN in Malta.

//

How useful was Royal Holloway's MSc programme to your future work?

For me, the MSc was a framework for developing IT security knowledge and practical skills. It's a doorway with many paths leading into different specialisms. Being able to synergize all these areas reveals the bigger picture of the role security plays. It has given me the ability to more confidently roadmap how the market is likely to develop and how products will meet perceived customer requirements down the road.

//

There seems to be a lot of interest in cyber security in Malta - why is that?

I believe the demand for cyber security in Malta is driven primarily by the multibillion euro online gambling industry. Malta has created an incredibly attractive environment for these companies for several reasons:

- Malta is in the EU
- Malta is on the UK's 'white-list' held by the UK Gambling Commission. Maltese gaming operators can thus advertise in the EU.
- The Lotteries and Other Games Act (2001), the Remote Gaming Regulations (2004), and The Lotteries and Gaming Authority (2005) provide the most sophisticated and well-regulated location for offshore gaming activities. Malta now has the largest worldwide gaming jurisdiction.
- Online gaming and financial services account for some 5% of Maltese GDP.

//

How concerned do you think members of the "public" should be about the Snowden revelations?

Edward Snowden has revealed to the world what our governments and their agencies get up to when inadequately supervised. We've learnt that the surveillance state is not only real but robust. We know respected agencies such as the NSA continue to conceal the truth from the public, testifying that a particular surveillance activity is not implemented in one particular program, conveniently omitting that it is done under another. There is little evidence to show that this intense surveillance makes the public safer. This become even clearer with NSA Director General Keith Alexander claiming in June that the NSA disrupted 54 terrorist plots, then in October revising that number to 13, and finally to one or two. I believe that the loss of privacy and our freedom is more damaging to society than the occasional terrorist act. Privacy is fundamental to democracy and individual human development but it feels like we are sleepwalking into a new age of totalitarianism. Ultimately the public needs to be educated on exactly how their freedoms are being limited, how this specifically affects the individual, and the long-term consequences of not acting soon.

Has IVPN seen an uptake in business since the Snowden revelations?

What's bad for privacy is good for IVPN. Every Guardian article, every Snowden leak, every NSA own-goal; they all raise the public's awareness of privacy. We did a survey in August last year to better understand which privacy threatening programs had influenced signups. It emerged that 28% said that PRISM was the biggest factor. This appears to be supported by our own increase in subscriptions. We saw a 56% increase in sign-ups to IVPN during June and July, compared to the previous two months (the PRISM revelations broke on June 6th). After PRISM, the next single biggest influence on VPN sign-ups was the US Patriot Act (11.2% of the vote), which some say allowed PRISM to operate without seemingly breaking any US laws. Closely following the Patriot Act was the European Data Retention Directive with 9.5% of the vote. The EU Data Retention Directive, which was enacted in 2006, mandates that all European ISPs store user data, including web logs, billing info and more, during a user's subscription period, and up to two years after they leave the service.

Do you think we can ever have secure systems given the Snowden revelations and information that has arisen since then?

No, it will never be possible to have perfectly secure systems: systems need to be fit for purpose.

IVPN

HP DAY

The ISG was delighted to host the 24th HP Colloquium on Information Security on 18th December 2013. About 120 attendees from industry, government and academia enjoyed three excellent invited talks, around 25 research posters, and the opportunity to network with friends old and new.

The day was kicked off in dynamic style by Stephen Bonner from KPMG. His talk was (loosely) based on Dickens' classic "A Christmas Carol" and featured cybersecurity highlights from past, present and future. Remarkably, Stephen had the whole audience on their feet singing a cyber-version of "Hark the Herald Angel Sing" at the end of his talk.

After a buffet lunch, Prof. Phil Rogaway (UC Davis) gave a fascinating insight into the cultural aspects of cryptography research, sharing with us his views on how and why academic cryptography research has developed in the way that it has, and reflecting on why the academic community's reaction to the Snowden revelations has been so muted.

Our third speaker was Chris Gavin, Vice President for Information Security at Oracle. Chris gave an account of Oracle's approach to information security, emphasising the need for appropriate positioning within the organisation and the way in which policy, rather than technology, dictates how security is handled within Oracle.

We are, as always, very grateful to HP for sponsoring this extremely successful event. We are looking forward to holding our silver anniversary colloquium in December 2014.

STAFF PROFILE: KOSTAS MARKANTONAKIS

> Dr Kostas Markantonakis is a Reader in the ISG.

///

How did you become interested in computers, and specifically in Information Security?

I need to briefly guide you through three distinct incidents in my life, so allow me to take you a few years back.

The first incident started with an Amstrad CPC6128. I was fortunate enough during the mid-1980s, as a teenager, to receive from my parents a home computer. My main aim was to play computer games, however I started experimenting with developing my first commercial computer programs in Locomotive Basic. I was particularly interested in finding efficient ways to protect my programs from being copied. This really sparked my interest and, as a result, I studied Computer Science at Lancaster University.

The second incident revolves around my undergraduate degree. I chose an elective course on "Design and Analysis of Coding Systems" by Dr J A Llewellyn during which we conducted a group project where we had to research and present the state of the art in symmetric key cryptography. This course revived my interest in Information Security. I started looking for masters programmes in this field and came across a fantastic building in a university that was also hosting an MSc in Information Security.

I will never forget the third incident. This was a conversation with my father when we were discussing the various MSc offers I had received. He concentrated in asking me questions about the MSc in Information Security from Royal Holloway. He said, "Kosta, computers are here to stay… their protection will gain more and more importance. How about we go for this MSc in Information Security at Royal Holloway?"

///

You have a long association with the ISG and Royal Holloway – tell us about it.

After accepting Royal Holloway's offer, I arrived in September 1995 to study my MSc in Information Security. I remember that there were 32 students attending the course that year. I will never forget Fred Piper's "magical" lectures, Dieter Gollmann with his unique lecturing style, Chris Mitchell successfully blending crypto and computer security, and Pauline Stoner always available to help with any issues. My MSc project received some interest from a smart card manufacturer and the opportunity to stay on for a PhD was offered to me with Dieter as my supervisor.

I rejected an interesting job offer and, following my desire to find out more about smart cards and information security, I embarked on my PhD in September 1996. It would not have been possible for me to complete the PhD without Fred's help in arranging sponsorship from Mondex International, so thank you very much Fred! I submitted my thesis in January 2000 and was eager to leave academia and work in industry. This was mainly motivated by the desire to explore further how information security theory meets practice in the real world. At this point, I thought that I would never return to academia, although I must admit that there was a powerful and unexplained force pulling me towards the ISG.

///

What brought you back into academia from industry, and to what extent did a spell outside academia benefit your career?

I accepted an offer from Visa International EU to work as multi-application smart card manager for Southern Europe. This proved to be a great experience for me. Following on from Visa, I joined SDG (Steer-Davies-Gleave), responsible for advising transport operators, city councils and banks on the use and deployment of smart card technology

While I was working in industry, I came back to Royal Holloway to deliver a couple of MSc lectures on smart card security and multi-application smart card operating systems. The idea of coming back to the ISG was becoming more and more appealing. At that time, I realised that in my limited free time I enjoyed working around unanswered research questions, following on mainly from my PhD research, which resulted in conference papers. Furthermore, the interaction with high profile clients was intense and rewarding, but having the opportunity to lecture information security to students was electrifying. In the summer of 2002, I applied for an open position in the newly-established ISG Smart Card Centre. I was really honoured to be offered a position from which I could develop my research and teaching ambitions. After all, this is where it all started for me and, as they say, it's always nice to come home!

My involvement in the industry has provided me with invaluable experience, contacts, and has shaped my career in a profound way. It particularly gave me insights on how information security is applied in the real world and how to work in diverse environments, adapting my professional output according to client demands. All the knowledge I acquired throughout my journey has provided me with the means to enrich my lectures with practical experiences that aim to bridge theory and practice.

///

What are your main research areas of interest?

My main current area of research is cyber-physical systems. This includes a number of different technologies, such as smart tokens, mobile devices and the so-called "internet-of-things". I am particularly interested in the security of RFID tokens, smart cards and secure elements in mobile phones. The underlying hardware and operational requirements of these platforms create specific security challenges. These typically involve secure application deployment and management, secure application execution, and using side-channel leakage for platform identification purposes. Finding the right balance between adequate levels of security and acceptable performance and implementation degradation is a focus of my current work.

///

Much of your work has an applied focus – how important is it to you that the results of your research have potential application beyond the academic community?

I am a firm believer that both theoretical and applied information security research is necessary in order to provide more secure and operational systems. I am particularly interested in the information security challenges imposed by real world applications and usage scenarios, and how these can be met in the most efficient, reliable and secure way by the available information security primitives. This requires an on-going effort to maintain a close and trusted relationship with a number of industrial partners.

///

What are the emerging technologies that most excite you and what security challenges will they bring to society?

This has to be the "internet-of-things" and its instantiation by devices all around us (RFID tokens, secure elements in mobile devices, embedded systems in user devices and appliances). There are issues around the ownership of these devices, as the traditional issuer-centric models might be challenged by user-centric architectures. Additionally, secure updating and firmware patching is a major challenge due to the underlying limitations in the security functionality provided at the hardware level. In the payments industry, the scenery might also be heavily influenced by a rethinking of what might be considered as a PIN-entry device.

//

Do you think we will ever be able to regard mobile phones as secure computing devices?

This is a difficult question to answer. At the hardware level, we have secure processors that can execute an application securely along with underlying mechanisms that could attest whether the device is in a secure state or not, but these incur monetary and performance costs. At the software level, we have secure application management frameworks. Someone could claim these are important building blocks, but it can be equally claimed that we have a long road ahead of us. There are potential risks through the existence of a number of intermediate software layers and default functionality at the platform level, which might originate from handset manufacturers, network operators, etc. Equally worrying, but entirely understandable, is the attitude of mobile phone users in accepting whatever permissions are requested by an application to be installed.

//

You are governing the project component of our MSc programme - how important is a project to an MSc degree?

I think it is very important all round. It provides students with an opportunity to either further develop a project area in which they have prior expertise, or explore a new topic in which they would like to build up their knowledge and skills. The feedback we receive from potential employers is that it is also considered to be very important for them. This is because it provides employers with a strong indication of someone's commitment, acquired experience, and achievement in engaging with a substantial piece of individual work. It is also important for academic supervisors, since we have the chance to supervise strong MSc projects that push forward the boundaries of knowledge in the field.

//

We have seen many information security students from Greece - why is our programme so popular in Greece?

I have wondered this myself on numerous occasions, but I am not sure there is a clear answer to it. We might just have to deduce that Greek students are instinctively curious about information security. We must not forget the effort placed by previous ISG staff (especially Dieter Gollmann and Mike Burmester) in delivering invited talks at Greek universities during the early years of the MSc programme, which strengthened our presence in the country. The ISG has also worked hard to recruit Greek students in recent years. The feedback that I receive from students who join us from Greek universities is that their professors recommend our MSc as "the best in the world". Word-of-mouth also plays an important role, as our Greek alumni are our best ambassadors and student recruiters. One thing is clear: according to our current MSc Programme Director Chez Ciechanowicz, "Greek students do well in the MSc, so let's find some more"!

RECENTLY COMPLETED PHD THESES & OTHER NEWS

Thomas Richard McEvoy
Context Based Anomaly Detection in Critical Infrastructures

Jihoon Cho
Cryptographic Approaches To Security and Privacy Issues In Pervasive Computing

Wei Zhang
Improvements and Generalisations of Signcryption Schemes

Calvin Chen
Secure e-Payment Portal Solutions Using Mobile Technologies and Citizen Identity Scheme

Eduarda Freire
Non-interactive Key Exchange and Key Assignment Schemes

Prof. Kenny Paterson has been awarded the Applied Networking Research Prize from the Internet Research Task Force (IRTF) for his research with PhD student Nadhem Al-Fardan. Their work uncovered a glitch in the way in which the Transport Layer Security (TLS) protocol terminates sessions, leaking a small amount of information to the attacker who can then use it to gradually build up a complete picture of the data being sent.

In January 2014 Chris Mitchell became Section Editor for Section D (Security in Computer Systems and Networks) of The Computer Journal, published by OUP on behalf of the British Computer Society. The Computer Journal, founded in 1958, is one of the longest-established journals serving all branches of the academic computer science community.

MEET THE CDT CYBER SECURITY

The Centre for Doctoral Training in Cyber Security at Royal Holloway welcomed its first intake of ten PhD students in September 2013. This £4M grant from the EPSRC and the Department of Business, Innovation and Skills, supports a programme of thirty PhD studentships with intakes from 2013 to 2015. The CDT students undertake an intensive first-year taught programme, before embarking on three years of research, which includes placements at external organisations.

We were delighted to recruit a strong and very engaging cohort of students for the first year of the project. It's time to meet them and find out how things are going. We are still recruiting for 2014, so if you are interested in exploring a research career in cyber security and have a strong academic background in any relevant discipline then please get in touch.

See: www.rhul.ac.uk/isg/cybersecuritycdt/ for more details.

JONATHAN HOYLAND

I recently graduated from Oxford, where I was awarded a Masters in Computer Science. Academically speaking my interests are model checking and formal verification in general, particularly as it applies to security protocols and primitives. Outside of the office (and much to the annoyance of my office inside too) I can often be found singing along to whatever music happens to be in my head. I love music in all its forms, performing and listening, and from opera to K-Pop, I love it all.

I'm really enjoying the CDT programme so far, having a year to consolidate all my learning has been great. The most surprising thing I've learned so far is just how broad a range of topics fall under the banner of cyber security. I would never have considered Geopolitics as something so rife with cyber security implications.

ROBERT LEE

Before joining the CDT I spent four years at York studying for my MEng in Computer Systems and Software Engineering. As part of that I completed a couple of security modules and a masters project in using GPGPU for cryptanalysis, gaining an interest in security and research at the same time as a degree. The CDT started at just the right time for me!

Having moved straight from school to university and to university again, I only have a few summer placements of real world experience, so I've really enjoyed our external speaker events when we get to hear about practice and not just theory.

I think that I've most been surprised by my course in smart cards where I have been amazed by the amount of technology and features that can be fitted into one smart card. Screen and buttons can even remove the need for a card reader for online banking.

CONRAD WILLIAMS

Before joining the CDT, I studied Pure Mathematics (Bsc) at Royal Holloway and graduated with a First Class Honours in 2013.

The most enjoyable part of the CDT so far has been the taught modules. Before joining the CDT I had limited information security knowledge, and I have thoroughly enjoyed expanding my understanding of all areas of information security and how important it is in the business world.

The most surprising thing that I have discovered so far is how aware information security professionals have to be of legal implications of systems that they manage and design. The professional duty extends far beyond making sure data is held securely and worrying about privacy; aspects like risk assessment and managing liability also have a huge role which I had not realized before.

DUSAN REPEL

I have a degree in Computer Science from the University of Plymouth and my interests lie primarily in operating system and application security.

The diversity and blend of different expertise in the CDT make it an interesting and unique working environment, like no other! With each of us addressing a cyber-security issue from a different angle, we often manage to have a 360 degree view of the problem.

Not much really surprises me about cyber security. For me, personally, cyber security has always been defined by exploration rather than expectation. Every connected person is a co-creator of cyberspace and it largely remains an uncharted territory composed of complex behaviours. This makes securing cyberspace both challenging and exciting.

SAM SCOTT

Originally, I studied mathematics for my undergraduate degree. However, when I was exposed to some of the ways that maths was used in cryptography - modular arithmetic, elliptic curves and lattices to name a few - I was immediately interested in exploring these interesting, practical uses of mathematics. Currently, I am trying to get an understanding of the many different aspects of cyber security in order to understand where else advanced mathematics might play a role.

I love problem solving, and one of the most interesting parts of being in the CDT are the industry events, which allow us to consider real-life issues and discuss how we might go about solving them. However, some of these problems might not have obvious solutions. Recently I was surprised to learn that one of the issues facing the core infrastructure of the internet is caused by sharks attempting to eat underwater cables!

THYLA VAN DER MERWE

Prior to starting at Royal Holloway, I worked for an engineering firm in South Africa. I hold a BSc (Hons) in Mathematics and an MSc in Mathematics from the University of Cape Town, as well as an MSc in Information Security from Royal Holloway. I also currently sit on the ISO/IEC JTC1 SC27 standards committee where my activities involve the standardization of cryptographic mechanisms and protocols.

I have been impressed by the multidisciplinary nature of the programme and have thoroughly enjoyed the interaction with our industry partners as I feel that this has provided valuable insight into the need for cyber security professionals both in academia and in industry. I have found that being part of the CDT has helped to broaden my understanding of the current challenges in cyber security, some with far-reaching consequences that I had previously not considered, specifically, the issue of cyber warfare and the degree to which nation states need to invest in the protection of critical infrastructure.

STEVEN HERSEE

I'm a former RAF Officer, police analyst and private sector worker, with an interest in the militarisation and general securitisation of Cyberspace. I believe that Cyberspace will become a new domain of Warfare and that Cyber War Will Take Place (apologies to Thomas Rid!).

I have thoroughly enjoyed the variety on the course, the disparate composition of the students in the CDT, the exposure to great thinkers, the expertise of the ISG, and the access to interesting and thought-provoking material.

I have been surprised to discover that some people think that cyber war will not take place. I have also been surprised to discover that many people working within the sector believe that Edward Snowden and Julian Assange are heroes.

PIP THORNTON

I have a background in the Metropolitan Police and military, and have BA degrees in History and Politics (Liverpool), English Literature (Open), and a Masters in English (Kings). My interests lie in how the figure of the soldier is represented, perceived and (de)constructed in geopolitical and cyber spaces.

What I have enjoyed most so far is regaining the freedom of studenthood. As interesting and rewarding as my career (occasionally) was, the opportunity to spend my days thinking, reading/writing and discussing topics which really matter to me, has been a real privilege.

The most surprising thing I have discovered so far about cyber security is the potential it has for incredibly rich and relevant cross-disciplinary critical and creative research. I was also quite surprised to discover the ferocity of the territorial politics of Word v. LaTex in interdisciplinary word processing etiquette!

THALIA LAING

I received a BSc in Mathematics from Imperial College London, where my dissertation focussed on Elliptic Curves and their application to Cryptography. I then came to Royal Holloway and completed the MSc in Mathematics of Communications and Cryptography. My dissertation was in the area of Key Predistribution for Wireless Sensor Networks.

So far I have enjoyed the breadth of topics covered in the CDT and the challenge of being exposed to topics I otherwise would not have covered.

I have been surprised with the role the social sciences play in information security; I had never personally considered cyber security from this viewpoint and have enjoyed becoming acquainted with the relevant issues and topics.

NAOMI FARLEY

I recently graduated from Royal Holloway with a First Class Honours degree in Computer Science and Mathematics. Although my current interests are related to cryptography and access control mechanisms, I am thoroughly enjoying learning more about other areas within cyber security.

In particular, I am enjoying the software exploit challenges that are included in the Software Security course that forms part of our first year training within the CDT. What I have found most surprising about cyber security so far is that it is incredibly difficult to make a system secure against all possible attacks.

A GLANCE OVER THE FENCE – ONE ACADEMIC'S PERSPECTIVE ON THE ISF CONGRESS

By Geraint Price

> Dr Geraint Price is a Lecturer in the ISG

The Information Security Group has been a member of the Information Security Forum (www.securityforum.org) since late 2010. In that time we have contributed to a few of their research projects, attended and sponsored their annual Congress, and engaged with their UK Chapter meetings. A number of ISG members have presented at both Congress and the UK Chapter meetings.Last year's annual Congress was held in Paris and I ventured over the Channel to represent the ISG.

For those of you not familiar with Congress, it is a very large event, with the 2013 edition hosting over 800 delegates from around the globe. Congress runs for three days, and has a wide variety of talks. There are two main parts to the programme: the keynote sessions of invited distinguished speakers and the parallel tracks of member-submitted talks. The former are usually global names from both inside and outside the security industry, while the latter is an interesting mix of "how we did…", personal experiences of dealing with particular problems, and more research-related looks at the principles behind the application of security across member organisations.

For the keynote sessions, as seems to be the custom, two non-security people were invited. The opening speaker this year was Sir Ranulph Fiennes, who shared some of the incredible tales of exploration for which he has become world-famous. One thing that he focussed on, which I hadn't anticipated, was the importance of getting the right team in place. When the chips are down, knowing that you can implicitly trust those around you can mean the difference between life and death. While this might seem obvious in hindsight, it was a rule by which he runs all his expeditions. The second guest speaker was Bruce Dickinson, the lead singer with Iron Maiden. He was no less engaging and it was interesting to learn how they have adapted their business model in light of the "download generation". A key message was to acknowledge the changes around you and learn to adapt to any new environment.

The bulk of Congress is made up of member-submitted seminars, which cover separate themes over the three days. There were 49 of these, which covered the following "tracks": Mobile, CISO, Privacy, Cyber, Securing the Supply Chain, Engaging with the Board, Managing Risk, Big Data, and Cloud.

What I found interesting about the talks that I attended was the level of innovation in some of the approaches taken. As an academic, I feel that sometimes it can be easy to forget that we don't have a monopoly on innovation. Specifically, there was a very interesting talk on how using simple "reminders" can influence human behaviour. It was refreshing to see that this research used similar techniques to the "grounded-theory" work that we are carrying out here at Royal Holloway in the Cyber Security Cartographies project. It was also very clear from this work that "one size does not fit all", which flies in the face of the way in which some security technology is presented to the market.

A few of the other talks I attended discussed the opportunities that Big Data presents to help security practice. These naturally related to the ability to bring together diverse and diffuse data sets. It was clear that this was a burgeoning area where development of the right tools in information science might help us to tackle some of the challenges presented by the rapid escalation of complexity within "cyber"-based systems.

If there is one thing that I've learnt from attending Congress over the past few years, it is that the scope for innovation and academic interaction with industry is immense. The main difficulty seems to come from framing questions in suitably tractable ways that academics can grasp, while still engaging with the genuine problems faced by industry. That may not come as ground-breaking news to everyone, but I came back from the 2013 Congress energised by the possibilities.

EVALUATING THE SECURITY OF TLS
By Jacob Schuldt

> Dr Jacob Schuldt is a Postdoctoral Research Assistant in the ISG

The ISG has a long history of analyzing cryptographic protocols deployed as part of the security infrastructure used on the Internet and in commercial systems. One protocol in particular has attracted a lot of attention from ISG researchers due to its widespread use and importance: the Transport Layer Security (TLS) protocol.

While the name TLS might not be immediately recognizable, almost everyone is familiar with secure HTTP connections, easily identifiable by the prefix “https://” appearing in the URL of the browser when a secure HTTP connection is in use. This type of connection, which is typically used when connecting to on-line banking systems or when submitting credit card details to an on-line shop, relies on TLS to protect the transmitted data. However, secure HTTP connections is just one area where TLS is used as a tool to provide security today - other examples include protection of email traffic, communication with embedded systems, and secure instant messaging. Today, TLS is arguably the most widely used security protocol, and has become the de facto protocol standard for secure Internet and mobile applications on the Internet.

In 2013, we initiated a project with the aim of evaluating the security provided by TLS in its most common configuration in securing HTTP traffic. The results of the project were both surprising and alarming, given the central role TLS plays in securing the Internet.

Brief overview of TLS

TLS was originally designed by Netscape in the early 90s under the name Secure Socket Layer (SSL). In 1999, the Internet Engineering Task Force (IETF) adopted SSL v3.0 under the name TLS 1.0, and it has since evolved through TLS 1.1 (2006) to the current version TLS 1.2 (2008).
The protocol consists of two consecutive phases: the execution of the TLS Handshake Protocol in which client and server establish a shared session key, followed by the TLS Record Protocol which implements a confidential and authenticated channel to transport application-layer data between client and server.
The Record Protocol provides three main combined authentication and encryption options for building the secure channel:

01 authenticating data using a message authentication code (MAC) followed by CBC-mode encryption using a block cipher such as AES;

02 authenticating data using a MAC followed by encryption using the RC4 stream cipher;

03 using a dedicated authenticated encryption algorithm, simultaneously implementing authentication and encryption, based on the GCM or CCM mode of operation of a block cipher.

The third option is only available in TLS 1.2, but this has seen a surprisingly slow adoption. A survey from June 2013 estimated that only 15.1% of websites supported TLS 1.2 and, at the time the results of the project were published, none of the major browsers supported TLS 1.2 in their standard configurations.

The first option has been subject to significant cryptanalysis. The best known attack is probably the BEAST attack which exploits a vulnerability in the variant of CBC-mode encryption employed in TLS 1.0. The Lucky Thirteen attack, which was also uncovered at Royal Holloway, further demonstrated that both TLS 1.1 and TLS 1.2 were vulnerable to a padding oracle attack, despite TLS from version 1.1 onwards providing countermeasures against this type of attack.

While all three versions of TLS can be patched to provide resistance against both the BEAST and the Lucky Thirteen attack, these attacks, coupled with the lack of support for TLS 1.2, led many commentators and some security firms to recommend the second encryption option based on the RC4 stream cipher. Indeed, the RC4 option was, until now, widely supported and used. For example, in a recent survey, the ICSI Certificate Notary performed an analysis of 16 billion TLS connections and found that around 50% of the traffic was protected using RC4 cipher suites.

The RC4 stream cipher has long been known to have a variety of cryptographic weaknesses. But no rigorous analysis of the security of RC4, as it is used in TLS, had previously been carried out. The aim of our research project was to provide such an analysis.

Attacking RC4 encrypted TLS traffic

Surprisingly, we uncovered two relatively simple plaintext-recovery attacks on RC4-encrypted TLS traffic. Both attacks are based on statistical analysis of ciphertexts and, unlike the BEAST and Lucky Thirteen attacks, do not require the adversary to inject messages into existing TLS connections or be located close to the client or server so that accurate timing results can be obtained. However, both attacks require a mechanism that will enable the adversary to obtain multiple encryptions of the target plaintext.

A candidate target for the two attacks is recovery of secure HTTP cookies. These are typically used to authenticate HTTP requests. For example, after a user has authenticated himself to a secure website, he will typically be sent a secure cookie, which will be stored by his browser. This cookie will then act as an access token, and will be attached to every subsequent HTTP request to ensure that the request originated from the authenticated user. To prevent a secure cookie from being exposed, the browser will ensure that the cookie is only sent over a TLS-protected connection to the website from which the cookie originated.

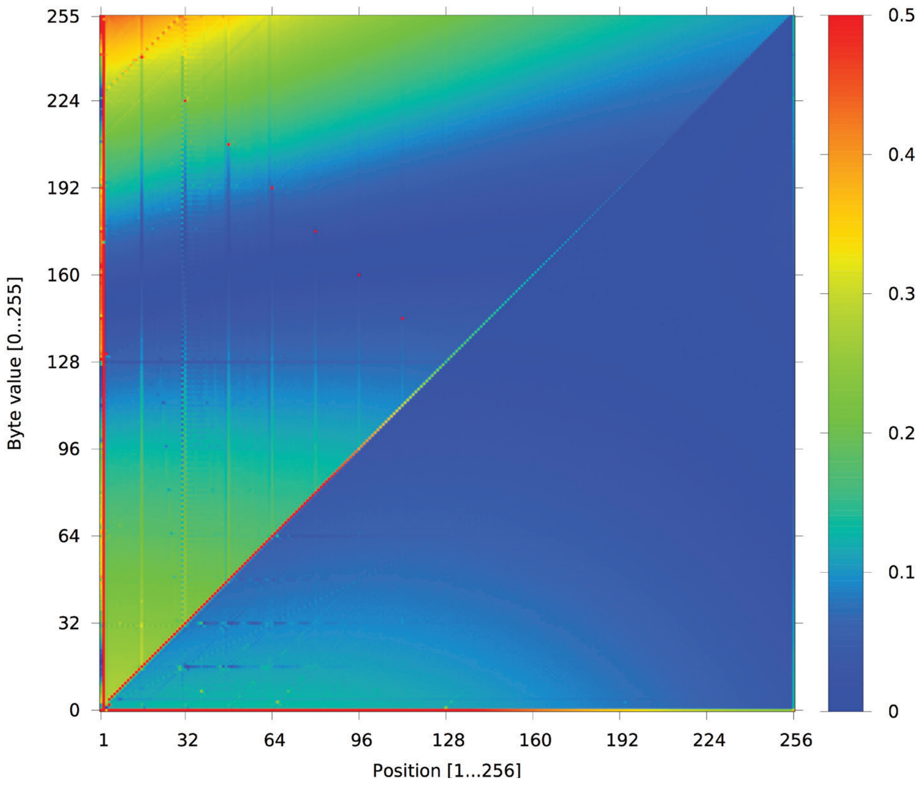
However, in this setting, the secure cookie would automatically be encrypted and sent for every HTTP request. This provides the multiple encryptions of the target plaintext that are needed for success in the statistical plaintext recovery attacks that we developed. We also identified a simple but more efficient mechanism for obtaining multiple encryptions of a secure cookie: if a user is lured to visit a malicious site, that site could serve a simple Javascript designed to asynchronously send multiple HTTP request to the target website. This would enable the adversary to control the rate at which requests are sent, but also influence what part of the RC4 keystream the cookie will be encrypted with, which will allow the attacks to be made as efficient as possible.

Our first attack

Our first attack targets the initial 256 bytes of plaintext in a TLS session, and is based on biases in the RC4 keystream; i.e. deviations from uniform in the distribution of the bytes at certain positions in the RC4 keystream. While a few biases in the RC4 keystream had been previously reported and theoretically analysed, our attack is based on an empirically generated description capturing all biases in the initial part of the keystream. This not only allows the attack to be optimized by simultaneously taking into account all existing biases, but also led to the discovery of significant biases which had not been identified previously.

However, because of the nature of the keystream biases, our first attack requires that the targeted plaintext be positioned within the first 256 bytes of the encrypted content, and that the plaintext is encrypted under many different RC4 keys. Assuming the client and server support TLS session resumption, the latter can be achieved by forcing the client and server to repeatedly resume the given TLS session, causing the RC4 key to be refreshed. Alternatively, the TLS session could be disrupted by other means, for example by interfering with the underlying TCP connection, which would likewise lead to renewal of the used RC4 key.

This first attack is on the verge of practicality. Specifically, experiments show that the first 40 bytes of TLS application data can be recovered with a success rate of over 50% per byte, using 226 sessions. With 232 sessions, the per-byte success rate is more than 96% for the first 220 bytes.



Pictorial representation of biases in RC4 keystreams for random 128-bit keys, for different positions (x-axis) and byte values (y-axis). The colouring scheme encodes the absolute biases, i.e., the absolute difference between the occurring probabilities and the (expected) probability 1/256, scaled up by a factor of 2^{16}, capped to a maximum of 0.5.

Our second attack

In contrast to our first attack, the second attack can target plaintext positioned anywhere in the TLS application data stream, not only in the first 220 bytes. Furthermore, our second attack does not require the target plaintext to be encrypted under many different RC4 keys (but works equally well even if this is the case). While the attack requires slightly more data to obtain similar success rates as the first attack, the above properties might make this attack easier to mount in practice compared to the first attack.

The second attack is based on double-byte biases, i.e. deviations from uniform of the distribution of consecutive byte pairs. These double-byte biases appear throughout the entire RC4 keystream, and not just in the initial 256 bytes. Our experiments confirmed the existence of double-byte biases previously identified in the literature, and furthermore showed that there are no other double-byte biases of similar size.

When targeting a 16-byte cookie, this attack is able to recover the entire cookie with a recovery rate of more than 50% based on 5 x 230 encryptions of the cookie, while a recovery rate of 98% is achieved for 8 x 230 encryptions.

Impact of attacks and the future of TLS

While our attacks require a large amount of ciphertext data to be successful, they clearly illustrate that the security provided by RC4 in TLS is far below the level of security suggested by the 128-bit key. Furthermore, it should be kept in mind that these attacks only set an upper bound for the security provided; optimizations such as exploiting language models for the targeted plaintext or combining both double-byte and single-byte biases, which might significantly improve the attacks, remain to be explored.

Several countermeasures to the attacks were suggested after our attacks were made public. Among these are discarding the initial RC4 keystream bytes, fragmenting the initial HTTP request so that the initial RC4 keystream bytes are used to protect the very first few bytes of a message, and adding random padding to HTTP requests. However, the first two countermeasures are not effective against our second attack, and the third will only increase the complexity of the attacks rather than defeating them. The only viable solution seems to be to abandon the use of the RC4 option in TLS.

Phasing out the underlying cryptographic primitive used in more than 50% of the TLS connections on the Internet is not easily done, but many vendors have already taken steps to prevent the use of RC4. For example, Microsoft have disabled the RC4 in TLS in Windows 8.1, and Google, Mozilla and Apple have now implemented and enabled TLS 1.2 and AES-GCM in their Chrome, Firefox and Safari browsers. Furthermore, the IETF is now developing new standards for alternative stream ciphers to replace RC4 in TLS.

So where do all these attacks on TLS's options for authenticating and encrypting data leave us?

Recall that the first option is based on a MAC followed by CBC-mode encryption. This is currently considered secure if patched to provide protection against the BEAST and Lucky Thirteen attacks. However, confidence in this option has been weakened due to the attacks, and completely eliminating the Lucky Thirteen has proved to be quite challenging for implementers.

The second option is based on a MAC followed by RC4, the target of our attacks, and should now be considered insecure.

The third option is offered only by TLS 1.2, and is based on using dedicated authenticated encryption algorithms. Here, implementations have not yet been fully evaluated with respect to resistance to side-channel attacks. However, with major players like Google moving to support TLS 1.2, it seems TLS 1.2 might finally become widely adopted, some six years after its standardization.

The general movement towards TLS 1.2 provides support for the argument that publication of concrete attacks is the most significant driving force behind the adoption of improved security standards. In turn, this underlines the value of conducting this type of research.

The research reported in this article was published as:

N.J. AlFardan, D.J. Bernstein, K.G. Paterson, B. Poettering and J.C.N. Schuldt. On the Security of RC4 in TLS. In USENIX Security Symposium 2013.

For more information about our results regarding TLS and RC4 see http://www.isg.rhul.ac.uk/tls/

MEGAMOS CRYPTO, RESPONSIBLE DISCLOSURE, AND THE CHILLING EFFECT OF “VOLKSWAGEN AKTIENGESELLSCHAFT VS GARCIA, ET AL”

By Robert Carolina & Kenny Paterson

> **Robert Carolina is a Senior Visiting Fellow in the ISG**

> **Prof. Kenny Paterson is an EPSRC Leadership Fellow in the ISG**

(A longer paper on this subject is available online and from the authors.)

On 25 June 2013, the High Court of Justice in England issued a preliminary injunction that restrained publication of a cryptographic academic research paper on the grounds that this is necessary to protect a crypto algorithm claimed as a trade secret. In this article we will review the facts of the case as presented in the decision, and provide a number of reasons we find this decision troubling.

The case focussed on a paper prepared by three university researchers, peer reviewed, and accepted for publication. It describes a weakness in the cryptographic algorithm used in certain types of Megamos automobile immobilisers. The Megamos system is designed to act as a deterrent to theft by placing the automobile in an immobilised state until a properly coded hand-held device is brought within close proximity of the vehicle.

The researchers provided advanced disclosure of the weakness using their best understanding of “responsible disclosure” protocols commonly used in the Netherlands, where all three co-authors worked during the research phase. Disclosure was made more than nine months before intended publication to a party in the supply chain who manufactures and sells the crypto package. Volkswagen (one of the companies who purchased and installed the immobiliser product in their automobiles) learned of the proposed publication many months later and brought this lawsuit. The case was brought in England where one of the researchers (Garcia) had moved to a new academic post between the time of research and publication. The lawsuit also names Garcia’s university employer in England, his two co-authors, and their university employer in the Netherlands.

The paper includes details of the crypto algorithm, but the algorithm itself is claimed as a trade secret. Normally the law does not prohibit publishing or otherwise using a trade secret that is uncovered through legitimate reverse engineering techniques. Although the researchers obtained the algorithm through a reverse engineering analysis, they did not reverse engineer the immobiliser. They reverse engineered a third party product called Tango Programmer that can be used to program immobilisers, including Megamos.

How did the algorithm find its way into Tango Programmer? The court decided that the designer of Tango Programmer (who was not a party to this case) most probably obtained the algorithm through some sort of improper activity – not through a legitimate reverse engineering study. Thus the court concluded that the researchers had obtained the secret algorithm from someone who (the court believes) probably has no right to publish it.

Applying human rights law, the court decided that the infringement of free speech created by a temporary injunction before trial was outweighed by the need to maintain the security of millions of automobiles fitted with the immobiliser.

We were disappointed by the court’s decision for a number of technological and legal reasons.

First, we were surprised by the court’s willingness (without explanation) to attribute significant value to the crypto algorithm’s secrecy, per se. The science of cryptography normally assumes that an attacker can discover the algorithm, and an algorithm that is so widely distributed in consumer products will not likely remain secret forever. The court even appears to accept that the algorithm had been successfully reverse engineered by others, but remained strangely wedded to the principle that secrecy is tremendously valuable in this case.

Second, when balancing free speech rights against intellectual property rights the decision does not provide a searching analysis of the degree of risk created by publication. There is no detailed discussion of the practicality of the attack, or if the immobiliser is defeated how difficult it would then be to steal a car. We believe it should not be sufficient to say (as the court does) that the academic publication will decrease security. A risk analysis (especially an analysis that will be used to decide the outcome of a free speech case) should explain how far that security has been lowered.

Third, we do not understand why the court was so willing to conclude that Tango Programmer was created using a misappropriated – not reverse engineered – algorithm. The court draws a major inference from evidence that the manufacturer is aware that its product is sometime misused for criminal purposes. This conflates two issues: how the manufacturer created Tango Programmer, and how Tango Programmer is (sometimes) used. The court does not acknowledge that legitimate security products can (and do) find their way into the hands of criminals as well as legitimate locksmiths.

Fourth, it may have applied the wrong legal standard in making preliminary assessment of the academics’ responsibility. The court concluded that Tango Programmer was made using a misappropriated trade secret and that the academics “ought to have appreciated that”. Just a few weeks before this decision, the UK Supreme Court decided in Vestergaard Frandsen A/S et al v Bestnet Europe Ltd et al, [2013] UKSC 31 (22 May 2013) that a higher standard should apply to this question – that the academics should be found liable for infringement of trade secret rights only if they had actual knowledge or so-called “blind eye knowledge” of misappropriation. The latter requires a finding of “dishonesty” – not a finding that they merely “ought to have known”.

Fifth, it is not clear why it has taken so long for the owners of this allegedly confidential information to enforce their rights. The court accepts that the Tango Programmer software has embodied the allegedly secret crypto algorithm since 2009, and suggests that the device is used (at least sometimes) by criminals. The product’s web site offers the device for sale throughout the EU, including a UK sales channel. The decision does not report on any past efforts to enforce trade secret rights in the UK or elsewhere against those who manufacturer, import, or sell, Tango Programmer.

Sixth, the court does not demonstrate a clear understanding of the phrase “responsible disclosure” as that term is used in security research. This misunderstanding is especially unfortunate, as the court is not shy in using this phrase to criticise the researchers.

We are concerned that this decision will have a chilling effect on security research in the UK. It could jeopardise the ability of UK academics to form multinational research efforts. Collaboration partners outside the UK might not wish to face the risk of a High Court injunction.

As a final comment, we are confident that the judge in this matter – who was required to hear this application and make this decision in a very compressed time frame – is an extremely able jurist. But judges, no matter how able, cannot be experts in all subjects. It is usually the responsibility of others to explain to the court key elements of technology that are under review. Perhaps for no reason other than the compressed timetable leading up to the hearing and decision, it appears to us that this process of explaining complex technical facts and practices from an otherwise abstruse specialist field has somehow broken down.

ANNUAL STUDENT CONFERENCE – CYBER SECURITY FOR THE NEXT GENERATION

On June 25/26 2013, the ISG had the pleasure of hosting the International (and final) Round of Kaspersky Lab's Annual Student Competition "CyberSecurity for the Next Generation".

Kaspersky Lab's Annual Student Competition is a unique event, which aims to bring together young researchers, IT security experts, and university professors from around the world, to present and discuss hot topics in information security research.

The International Round represents the competition final, bringing together the very best students. Winners of regional (European, Russia & CIS, Asia Pacific & MEA, and the Americas) rounds are invited to compete against each other in a collaborative, fun and creative environment.

The 2013 competition final at Royal Holloway saw participants from USA, Mexico, Ecuador, Armenia, Russia, Indonesia, South Africa, Philippines, UK, and Germany alternating cybersecurity talks (including cryptanalysis at Bletchley Park, what's driving malware development and cybercrime investigations), with practical hacker-oriented hands-on sessions (including live malware analysis), cybersecurity-related challenges (such as a cyberwar game and a cybersecurity quiz), and fascinating social events featuring a boat trip along the Thames, an etiquette master class in Windsor (Guildhall), dinners in great settings, and a tour of London.
It was a very interesting and fun two-day conference, which we enjoyed very much being part of. We are particularly pleased that one of the winners, Dusan Repel, has commenced a PhD at Royal Holloway!

More information about the event is available at:
http://academy.kaspersky.com/cybersecurity/cybersecurity-for-the-next-generation-conference-final-2013/

An interesting video summary of the event is available at:
http://www.youtube.com
watch?v=bdbejnHTDsM#t=1

All photos © Kaspersky Labs

OUTREA

As well as providing education programmes and delivering research that is targeted towards the cyber security industry, the ISG believes strongly in the duty of higher education institutions to engage with the wider public on matters relating to academic expertise. This not only helps to inform the wider public of cyber security issues, but aims to inspire young people to consider a career in cyber security. Although significant effort is required to do this well, the results tend to be highly rewarding. Here are just some of the outreach activities that the ISG has been involved in over the last twelve months.

COMPETITIONS

The Cyber Security Challenge is a series of national online games and competitions organised in order to test the cyber security abilities of individuals and teams from every walk of life. It is designed to excite and inspire anyone considering a career in cyber security. The ISG is a sponsor of the Cyber Security Challenge and provides a range of expertise in the development of the competitions, as well as in judging and providing prizes.

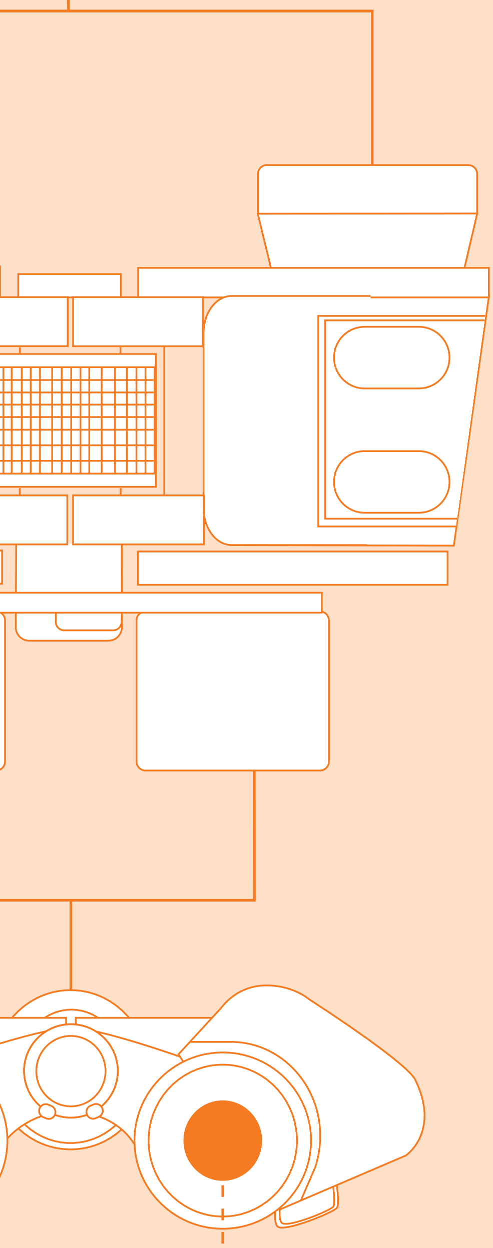
The ISG provides support and judges for the Sigmatak Film-making Competition, organised by Royal Holloway alumnus Tahir Alvi. This competition is open to children between 11 and 16 and aims to raise awareness of the importance of internet security through children producing their own films highlighting security and safety concerns. The ISG also hosted and provided judges for the finals of Kaspersky Lab's international CyberSecurity for the Next Generation Competition (see full report elsewhere).

WORKSHOPS

In April 2014 the ISG is hosting a three-day residential cyber security workshop for fifty Year 9 students. Pupils will engage in a series of group tasks, each exploring different aspects of cyber security as diverse as wireless networking, security awareness, and cryptography. This event is organised by the Smallpeice Trust, which is dedicated to promoting engineering careers to young people.

As part of the ISG's contribution to the Research Institute on Science of Cyber Security, we also facilitated a workshop on cyber ethics that was attended by a wide range of industrial stakeholders.

ACH ACTIVITIES



MEDIA

ISG staff are regularly called on by the media to comment on cyber security issues. In the past 12 months we have provided interviews for several international television stations, radio stations, and provided comments and articles for many print journalists.

OPEN DAYS

The ISG supports the annual Science Festival, when Royal Holloway opens its doors to members of the public.

At the Science Festival we have run cipher challenges, exhibited displays of historical cipher machines, provided an expert to be quizzed about careers in cyber security, and worked with artists to promote awareness of personal privacy and surveillance issues.

TALKS TO SCHOOLS

Members of the ISG regularly give presentations to school groups in order to promote early interest in cyber security. Prof. Keith Martin and Prof. Kenny Paterson gave presentations on cryptography to over 4000 school pupils at a series of events hosted at the Institute of Education by the Training Partnership. Keith also took part in a series of Christmas Cyber Security Lectures for Scottish Schools, reaching over 3000 pupils in events held across four cities. Dr Lorenzo Cavallaro gave an introduction to malicious code as part of Royal Holloway's Science for Schools Lecture Series. Dr Lizzie Coles-Kemp worked with a primary school using collage to explore children's attitudes to internet safety. Several ISG members have presented in recent years at Royal Holloway's annual Exploring Mathematics (EXPOMAT) day.

NEW TECHNOLOGY PROTECTS AGAINST PASSWORD THEFT AND PHISHING ATTACKS

By Chris Mitchell

> Prof. Chris Mitchell is a Professor of Computer Science in the ISG

Introduction

New technology launched recently by the ISG will help protect people from the cyber attack known as 'phishing', believed to have affected 37.3 million of us last year, and from online password theft, which rose by 300% during 2012-13. A common type of phishing involves cyber criminals creating fake websites that look like real ones and luring users into entering their login details, and sometimes personal and financial information. In recent months, the Syrian Electronic Army (SEA) has successfully launched phishing attacks against employees of the Financial Times to enable them to post material to its website, and mass attacks were launched within Iran using a fake Google email, shortly before the elections.

Our new system, called Uni-IDM developed jointly with my PhD student Haitham Al-Sinani, will enable people to create electronic identity cards for each website they access. These are then securely stored, allowing owners to simply click on the card when they want to log back in, safe in the knowledge that the data will only be sent to the authentic website. A key feature of the technology is that it is able to recognise the increasing number of websites that offer more secure login systems and present people with a helpful and uniform way of using these.

Uni-IDM is also expected to offer a solution for people who will need to access the growing number of government services going online, such as tax and benefits claims. The system will provide a secure space for these new users, many of whom may have little experience using the Internet.

In the remainder of this article we provide a little more detail on how the system works.

Authentication

Authentication of human users is a fundamental security requirement; indeed, it could be argued that it is the fundamental requirement. Despite its importance, it is almost universally acknowledged that providing user authentication remains a huge practical problem. In practice, as many observers have noted, we are still using passwords almost universally. Again as widely acknowledged, the use of passwords has many shortcomings, not least because users today have so many Internet relationships, all requiring authentication. In such a context, password re-use and use of weak passwords are almost inevitable.

A common approach to addressing this problem is to propose yet another new way of achieving user authentication, possibly involving a Public Key Infrastructure (PKI). However, there are already many good technological solutions. Perhaps the real problem is the insufficiently broad adoption of the solutions we already have. If so, this is partly a business and sociological issue, but perhaps it is also a problem which requires new technical thinking.

It is easy for those of us providing technological solutions to claim that this is not our problem. We provide the technology, and the business and commercial world should just get on with adopting it. However, real life is not so simple. We should be thinking about how to devise technological solutions which are easier to adopt. As always, key issues for adoption are transparency, ease of use, and backward compatibility, and these factors have played a large part in the design of the system we describe here.

Identity management

Identity management systems have been designed to simplify user authentication. An identity management system enables an Identity Provider (IdP) to support authentication of a user (and assertion of user attributes) to a Relying Party (RP). Recent years have seen the emergence of a wide range of such systems. Each system has its own set of protocols governing communications between the main parties. As well as its own protocols, each system may also have a unique supporting infrastructure, including public key certificates, shared keys, passwords, etc.

Some systems have gained traction recently, e.g. the use of OpenID in some sectors (notably as supported by Google) and Facebook's adoption of OAuth (in the form of Facebook Connect). However, the systems that have been most widely used also possess the most significant security issues (e.g. phishing vulnerabilities), and no system has truly broad penetration into the user community.

Many identity management systems are susceptible to phishing attacks, in which a malicious (or fake) RP redirects a user browser to a fake IdP. The user then reveals to the fake IdP secrets that are shared with a genuine IdP. This arises because, in the absence of a system-aware client agent (i.e. software running on the user's computer which is aware of the identity management process), schemes rely on browser redirects.

A further problem faced by an end user is that the user experience of every identity management system is different. It is widely acknowledged that users fail to make good security decisions, even when confronted with relatively simple decisions. The lack of consistency is likely to make the situation much worse, with users simply not understanding the complex privacy - and security-relevant decisions that they are being asked to make.

Finally, when using third party IdPs which provide assertions about user attributes, there is a danger that a user will damage their privacy by revealing attributes unintentionally to an RP. In general, getting settings correct for systems handling Personally Identifiable Information (PII) is a non-trivial task.

A new approach

It is tempting to try to devise another new scheme which has the practical advantages of OpenID and OAuth, but yet provides robust protection against phishing and privacy loss. That is, we might wish to devise a client-based scheme with the user convenience of other systems, but which somehow avoids the fate of Microsoft's CardSpace®. However, it seems that a new solution is highly unlikely to succeed when others have failed, especially given that systems such as CardSpace® have had the support of a large corporation and incorporate very attractive features. Moreover, a new system is likely to create yet another different user experience, increasing the likelihood of serious mistakes by end users. This suggests that devising yet another new system may not be the right approach.

Our goal is to describe a new approach to the user authentication problem. It does not involve proposing any new protocols or infrastructures. The goal is to try to make it easier to use existing systems, and also to make their use more secure (including resistance to phishing) and privacy-enhancing, not least through the provision of a consistent user interface and an explicit user consent procedure.

The scheme we propose, which we call Uni-IDM, involves a client-based user agent. This is a single tool which supports a wide range of identity management systems yet provides a single interface to the user. The consistent user interface should maximise user understanding of what is happening and thereby reduce the risk of errors and increase user confidence. It also avoids the need for passive browser redirects, hence mitigating phishing attacks.

//

Uni-IDM

We now describe Uni-IDM, an architecture for a client-based identity management tool that operates in conjunction with a client web browser. A tool conforming to the architecture provides a user-intuitive and consistent means of managing a wide range of types of digital identities and credentials for web activities. Royal Holloway has filed a patent on the technology.

The Uni-IDM architecture is designed to support a wide range of existing identity management protocols, and can be used to replace existing identity management client software, including the CardSpace®/Higgins agents, Liberty-enabled client software, and client-based password managers.

It is important to note that Uni-IDM is not an identity management system, at least not in the normal sense of the term. Instead it is an architecture for a client system which enables the use of multiple identity management protocols with maximal transparency to the user, and also avoids the need to install multiple identity management clients. The Uni-IDM architecture is designed so that conformant tools are able to work with existing Internet RPs and IdPs without any changes to their current operation. That is, the system is transparent to third parties.

The Uni-IDM architecture is designed to be platform-independent, and a partial prototype implementation has been developed. Implementations should be capable of being deployed on Windows, Unix, Mac OS, and smart phone-based platforms with minimal changes. Key parts of the system can be instantiated as browser add-ons, e.g. written in C++ and/or JavaScript, thereby maximising portability.

As with any identity management tool, the primary purpose is to enable an end user to access a protected resource. Once installed on a user platform, Uni-IDM will execute whenever a user wishes to access a protected service using a web browser. It allows the user to select a particular identity management system from amongst those supported by the RP. It also allows the user to choose which set of credentials is to be used with this RP, where the network interactions with the RP and IdP will conform to the chosen identity management system.

Uni-IDM interacts with the user via a key component known as the card selector. This provides a visual representation of user credential sets in the form of virtual cards, referred to here as credential cards (cCards). The operation of this component is motivated by the CardSpace® identity selector, whose virtual cards are known as InfoCards or iCards. Higgins, which originated as an open-source implementation of a CardSpace® -like system, also uses the term InfoCards. A cCard can represent any of a wide range of types of user credential, including:

- ready-to-use tokens including password manager tokens containing a username-password pair, referred to as local cCards; and
- a pointer to a remote, credential-issuing party (an IdP), referred to as remote cCards.

Whilst Uni-IDM has a somewhat similar user interface to CardSpace® and Higgins, it is important to note some fundamental differences. Both CardSpace® and Higgins support just one set of protocols for web interactions between the user platform and third party systems. If future versions of these systems support additional protocols, then this is likely to require corresponding modifications to RPs and/or IdPs. Uni-IDM, by contrast, is designed to work with almost any conceivable identity management protocol suite, and its adoption does not require any changes to third party systems (including IdPs and RPs).

Uni-IDM is made up of a set of self-contained components interacting with each other in a pre-defined way, thus enabling modular implementation. Such an architectural design enables new identity management protocols to be supported in a simple way by adding new software modules to an existing implementation.

MINDING THE CYBER SECURITY TALENT GAP WITH PWC

With cyber security being one of the fastest growing sectors in the UK, many organisations are seeking to recruit in this area. One traditional approach is to seek already-trained individuals who have a wealth of experience and technical ability behind them. This approach might work well in the short term, but does not readily increase the national cyber security skills capability, and runs the risk of overlooking emerging talent.

A more visionary approach is to attract talented individuals into careers in cyber security by equipping them with the skills to succeed. This recruitment process involves identifying individuals with exceptional transferable skills, such as expert communication, analytical and people skills, coupled with a willingness to learn. These individuals can then be prepared for a career in cyber security through the provision of specialist training to accompany on-the-job learning. The ISG has always been supportive of organisations who wish to utilise our education programmes as part of their training regime.

One organisation that has been using Royal Holloway's MSc Information Security as part of their professional development programme is PwC. Mark Hanvey, Cyber Security Director at PwC explains why:

"At PwC we are making strides to bridge the talent gap within cyber security by providing the right training and support. We are currently supporting nine of our people to study for a Masters in Information Security at Royal Holloway, University of London. The high quality training the MSc provides enables our people to develop their skills and gives them a solid career foundation for an ever-evolving industry. I completed the Masters at Royal Holloway in 1995/96 and found the teaching to be truly inspirational. The skills I learnt have been hugely beneficial to my career development."

This joint initiative between PwC and Royal Holloway has been working well. Matt Gregson, PwC Cyber Security Associate, is one of those on the programme and is inspired by the benefits to client relationships:

"The masters at Royal Holloway is a great opportunity to learn new skills in new domains of information security. The professors are world leaders in their field and offer great insight into current trends within Information Security. The course allows us to bring this knowledge and value to our clients at PwC."

Particularly satisfying is the ability to take ideas from the classroom and apply them in practice, Victoria Melvin is a Cyber Security Senior Associate with PwC:

"The Royal Holloway MSc in Information Security offers an engaging and rigorous curriculum that I can translate into my everyday work. A master's degree from such a well-respected institution lends greater credibility working in the cyber security industry."

However, one of the strongest features of the Royal Holloway programme is the quality of networking and group learning that can be achieved by studying within a sizeable cohort of like-minded students. Josh Higginbotham, a PwC Cyber Security Associate, has found this very much to his advantage:

"The infosec masters is a brilliant opportunity to learn new skills. In addition I have been able to network and build solid relationships with other people working in cyber security and IT. The course is structured very well and the availability of resources aids the learning process."

From the Royal Holloway perspective, having such a strong presence of cyber security consultants on the programme has been highly beneficial. Programme Director Chez Ciechanowicz is delighted at the success of this initiative:

"One of the great pleasures of teaching cyber security is running classes that consist of students with a wide range of practical experience. This allows newcomers to the field to share their educational experience with students who have practiced in different areas within the industry. We are convinced that our programme will serve PwC well in their exemplary approach to professional development."

A PRIZE CRYPTIC PUZZLE
by Skipjack

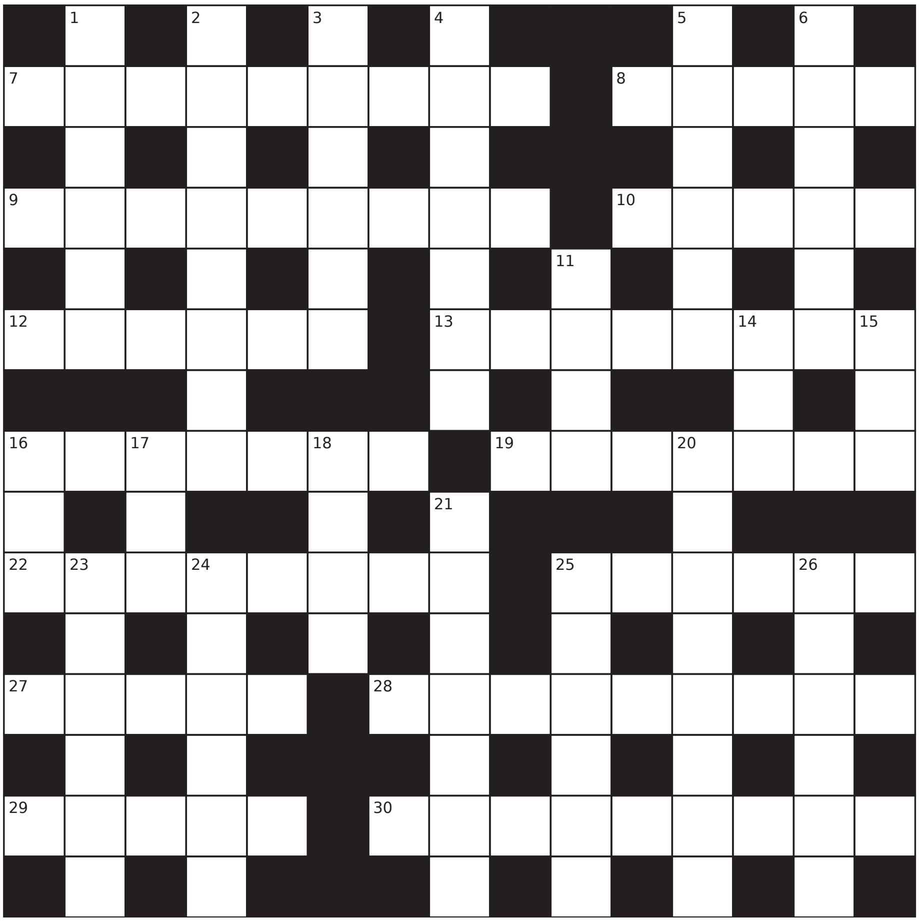
This is a cryptic crossword in the classical “British-style”. A mystery prize will be awarded to the winner. To be eligible for the prize you must complete the puzzle correctly and provide a cryptic clue for BLETCHLEY PARK. The winner will be decided by Skipjack on the basis of the clue; Skipjack’s decision is final.

To enter the competition, send your clue and a copy of the completed puzzle. Entries may be scanned and emailed to: jason.crampton@rhul.ac.uk

or sent by post to: Jason Crampton,
Information Security Group, Royal Holloway,
University of London, Egham Hill, Egham,
TW20 0EX, U.K.

All entries received by 31st July 2014 will be considered for the prize.

For those unfamiliar with cryptic crosswords, Jason has prepared a brief introductory guide to help you on your way:
www.rhul.ac.uk/isg/documents/pdf/crypticcrosswordclues.pdf
Jason also recommends Big Dave’s site:
http://bigdave44.com/crosswords/crossword-guide/3/#cluetype
alumniconference/2014/home.aspx



The asterisked clues have a connection with 6,15,1,3; these clues do not include a definition

Across

7 Third-party dealership ruined gear 27 (9)
8 Leader of opposition in close call (5)
9 In a fitting state? (9)
10 Suggest by just scratching head (5)
12 Hear author’s first verse (6)
13 Irish symbol is fake stone (8)
16* Guy from Underworld? (7)
19 Third-party identification? (7)
22 Defunct club is a waste of space (4,4)
25 Apply one-way function again to produce new text from old (6)
27 Move 15? (5)
28 Musical genre from Boulder? (5,4)
29 Clear type of text that needs 1,3? (5)
30 Hand green bananas to someone making no effort (9)

Down

1 See 6
2 Wasted sanction blocking encrypted leaks (8)
3 See 6
4 Close to leader this month (7)
5* Teacher clutches thigh (6)
6,15,1,3 Try ugly hack by cop; Piper develops way to secure the Internet (6-3,12)
11,14 At some distance from orifice, wiped bottom of delegate (4,3)
14 See 11
15 See 6
16 Concealed part of Jewish identity (3)
17 Trim the borders of bleak field (3)
18 Constituent part of cash machine contains nothing (4)
20 Stick religious books to disciple (8)
21* Free Mandela! (7)
23 Breathe out when former partner is well (6)
24* Providing fifth root splits cube...(6)
25*. . . remainder is divided by 4 (6)
26 Three-quarters discreet could be privacy-preserving (6)

2014 ALUMNI CONFERENCE

23rd – 25th June 2014

We are pleased to announce that we will be holding our fourth ISG alumni conference from 23rd – 25th June 2014.

—

The alumni conference webpage can be found at: http://www.rhul.ac.uk/isg/alumni/alumniconference/2014/home.aspx

—

Ticket price will be £85 per person. This includes all lectures and presentations, refreshments, dinners and WiFi connectivity.

—

The two keynote speakers for the conference will be Prof. David Nacacche & Prof. Andy Clark.

If you wish to speak at the conference, please contact Dr Kostas Markantonakis (k.markantonakis@rhul.ac.uk)

—

Any questions regarding the event can be directed to Emma via isg@rhul.ac.uk

—

We look forward to seeing you all in June!

Facebook:
http://www.facebook.com/ISGofficial

Twitter:
http://twitter.com/isgnews

LinkedIn:
http://www.linkedin.com/groups?gid=3859497

You Tube
www.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@rhul.ac.uk
W: www.rhul.ac.uk/isg