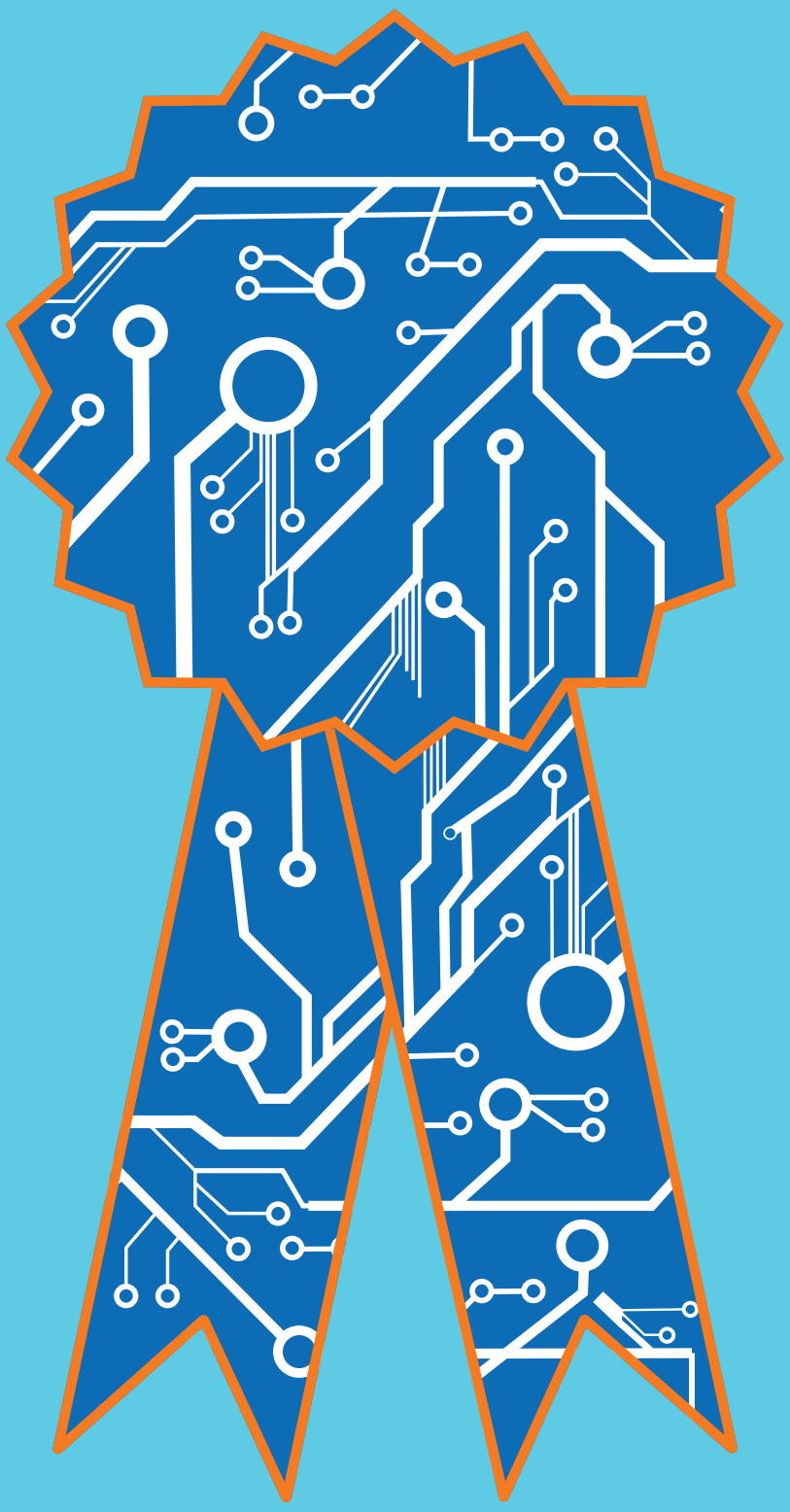
Information Security Group

Review 14/15



ROYAL HOLLOWAY UNIVERSITY OF LONDON

LETTER FROM THE ISG DIRECTOR

Every year seems to be an even better year than the one before to be in the field of cyber security. So much is going on that it is becoming almost impossible to keep track of it all. One advantage of being part of a multidisciplinary academic cyber security centre, such as Royal Holloway's Information Security Group, is that, through our diverse interests and activities, we can make a decent effort of keeping in touch with this fast moving field. This newsletter gives you a glimpse of some of the events and perspectives gleaned over the last year.

One of the highlights of 2014 was obtaining full certification from GCHQ for our pioneering MSc in Information Security. With over 3000 cyber security graduates from this programme around the world, we are justifiably proud of this major contribution to the international development of cyber security as a profession. We have recently learned that our Distance Learning MSc programme has also obtained full certification, which is great news.

Crucial to staying informed and delivering relevant teaching and research is the ISG's connections to the wider cyber security community. One of our longest partnerships, and arguably one of our strongest, has been with HP Labs in Bristol. December 2014 saw the 25th anniversary of the HP Information Security Colloquium, held every year at Royal Holloway. We celebrated this with a truly memorable event which brought together some legends of the past and emerging talent of the future.

Much is discussed about the lack of people skilled in cyber security. We have good news about the employability of our graduates but recognise that, for some of them, getting that first job can be challenging without "prior experience" on the c.v. In 2015 we are launching the MSc in Information Security with Year in Industry, which embeds a one-year placement within a two-year MSc programme.

Our EPSRC Centre for Doctoral Training in Cyber Security has been a major success and brought much energy and inspiration to our activities. We are also delighted with the formation of our new Systems Security Lab, welcome a new Director of Distance Learning to the ISG team, and have been running Cyber Security Residential courses for schoolchildren with the Smallpeice Trust. Don't forget to solve our resident puzzle wizard's latest challenge!

This newsletter gives you a flavour of what we have been up to. Do not hesitate to get in touch about these, or other, activities. We would be delighted to hear from you.

Professor Keith Martin

INDEX

GCHQ CERTIFIES OUR MSC IN INFORMATION SECURITY

Dr Chez Ciechanowicz

> Dr Chez Ciechanowicz, MSc Information Security Programme Director

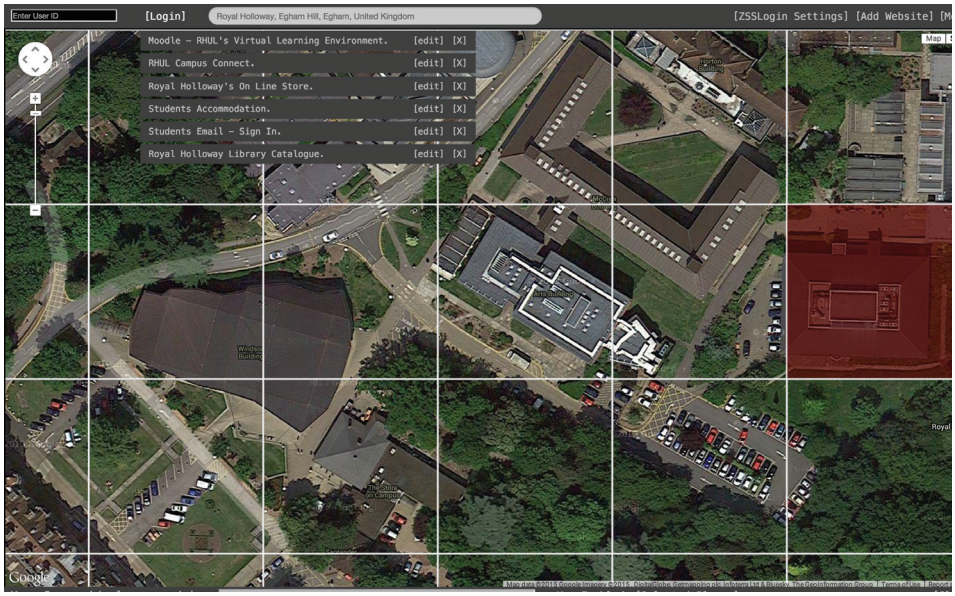
In November 2011, the UK Government issued its Cyber Security Strategy for protecting and promoting the UK in a digital world. As a result of this, GCHQ in partnership with other Government bodies launched a series of initiatives to achieve the objectives listed in the Strategy. One of the aims was to "Encourage, support, and develop education at all levels, crucial key skills and R&D".

Within the context of education, in Spring 2014 GCHQ launched a scheme for the certification of masters degrees that provided a general, broad foundation in cyber security. As pioneers of masters level education in this area (we introduced the world's first MSc in Information Security in 1992), we were heavily involved in the definition and establishment of this certification process. In particular, the ISG's former Director, Prof Fred Piper, has been advising GCHQ on what the standards should be.

Although I was personally responsible for putting together our certification documentation, I was overjoyed at the amount of help provided by my work colleagues, and managed to submit the application two hours before the submission deadline (without their help I would have failed abysmally in meeting this deadline!).

At the heart of the certification process is the Institute for Information Security Professional's (IISP) Skills Framework. Our MSc syllabus is aligned very closely with the framework. The IISP is an independent member-owned organisation that furthers the development of knowledge, skills and professionalism in Information Security and Assurance. In addition to professional accreditations, it also provides services for competency measurement, job role definition, benchmarking, and capability. Recently the IISP have introduced the concept of Academic Partners and Royal Holloway is proud to have become one of these. We are partners because we support the concept of career development and recognise that degrees are only the first stage in a long process towards gaining experience and becoming fully fledged security professionals.

At the beginning of August 2014, GCHQ announced that four universities had gained full certification, namely Royal Holloway and three other universities (Oxford, Lancaster and Edinburgh Napier). In earlier documents, GCHQ announced that certification was the first step towards the concept of becoming an Academic Centre of Excellence in Cyber Security Education (ACE-CSE). We are totally supportive of this initiative and it is our intention to apply for ACE-CSE status when the call document is circulated.



GEOGRAPHICAL PASSWORDS

By Dr Ziyad Al-Salloum

> Dr Ziyad Al-Salloum (zss@zss.net), ISG Alumnus, Founder & CEO of ZSS Ltd.

In 2011 LinkedIn.com announced the exposure of millions of its hashed passwords. It was a matter of days before these passwords became publicly known after cyber criminals recovered them. In another breach, fifty million passwords were stolen from the Evernote service, leading the cooperation to issue a rushed security notice to advise its clients to reset their "soon to be cracked" passwords. Twitter has also been under attack, with the encrypted passwords of around 250,000 of its users exposed to cyber criminals.

A study that analyzed 32 million publicly leaked passwords from the gaming website RockYou, showed that passwords were generally short, conformed to existing language patterns and showed a great deal of overlap. However, even passwords that have been constructed by highly-skilled experts have been exposed. Such incidents indicate that we need to revisit authentication approaches, in particular password construction. It has been claimed that an effective replacement for conventional passwords could reduce 76% of data breaches, based on an analysis of more than 47000 reported security incidents.

All studies (and indeed our own intuition) show that humans do not particularly enjoy memorizing characters and, when they have to, tend to apply minimal effort. This leads to a range of vulnerabilities, including:

- Using passwords that are vulnerable to dictionary attacks.
- Using passwords that are short enough to be vulnerable to brute-force attacks.
- Using the same password for different accounts.
- Constructing passwords using obvious information, such as birthdays or addresses, making the passwords easy to guess.
- Avoiding changing passwords according to a recommended time interval.
- In the event of changing a password, the new password selected not being very different from previous ones.

To address these vulnerabilities we propose the concept of geographical passwords, which are passwords that have been constructed based on geographical information. By "geographical information" we mean the knowledge acquired through processing geographically referenced data, which is data identified according to places on the Earth's surface. Geographical information (i.e. streets, buildings, rivers, mountains) is very familiar to humans, who show a remarkable ability to remember places they have visited, or wish to visit. Geographical passwords recognize this characteristic in humans and utilize it to establish access credentials.

We believe that if users are able to select geographical locations as their access credentials then many current problems can be addressed because geographical locations are:

- Easy to remember and hard to forget - especially if there are feelings and memories associated with the selected places.
- Diverse - there are many geographical locations where the user can select from.
- Hard to predict - since users can choose places based on personal preference.

Selecting a geographical area on a map can be done in many different ways and using different shapes. A user can place a circle around a favourite mountain, or a polygon around a favourite park. No matter how the geographical area is selected, information can be extracted from the area (such as longitude, latitude, altitude) in order to form the geographical password.

We have developed a geographical based access credential called ZSS Login to demonstrate one possible implementation of geographical passwords. We divide Earth into small rectangular geographical areas, each representing a geographical password. For ease of use, we divide Earth into different layers where each layer represents a zoom level which has a different rectangular geographical area size.

Each geographical area can be defined by two points, the south-west and the north-east, which consist of geographical coordinates (i.e. latitude and longitude). We use these two points to form our geographical password. In ZSS Login the order in which the user selects geographical locations is also taken into account.

Assuming there are 360 billion rectangular geographical areas on planet Earth that the user can choose from, the more places selected, the larger the geographical password space, which makes it more difficult to guess or brute force geographical passwords. To make it even more difficult, the geographical password space can be further increased using different techniques such as using the extracted geographical characteristics of selected places as input to a Message Authentication Code (HMAC) function where the key is a memorable string of characters, or better, a randomly generated key. ZSS Login uses a 256-bit randomly generated key to further strengthen the geographical password and mitigate shoulder surfing attacks, thus tackling many vulnerabilities associated with conventional passwords. Assuming 100 trillion guesses per second, it could take cyber criminals trillions of years to brute force ZSS Login's geographical passwords.

Geographical passwords should not be confused with graphical ones, since theycan be totally constructed without using any graphics at all. Nor should they be confused with user current geolocation authentication, since any location on planet Earth can be an access credential in a geographical password. For example your favourite camping spot in Spain can be your password to your office in London, even though you are not currently there.

Finally, geographical passwords are adaptable as millions of conventional password based websites, do not need to change or integrate anything for their users to start using this UK patented technology, unless they choose to integrate it as part of their own servers. ZSS Login can be demonstrated at www.zss.net and a full paper is available at www.zss.net.

INTRODUCING S2LAB
By Lorenzo Cavallaro

> Dr Lorenzo Cavallaro is a Senior Lecturer in the ISG and Leader of S2Lab.

On August 2011, I came to Royal Holloway to be interviewed for a Lectureship within the ISG. I remember vividly one of the questions from the interview panel being: "Work in your research area really requires a lab - what if you don't manage to establish a lab in your subject?" I, of course, played it cool and reassured the panel that I would succeed – they just had to take a leap of faith (and, most importantly, believe in my plan).
Fast forward to September 2014 and I was delighted to announce that the Systems Security Research Lab (S2Lab) at Royal Holloway became a reality!

The research carried out at S2Lab focuses on devising novel techniques to protect systems from a broad range of threats, including those perpetrated by malicious software. In particular, we aim to build practical tools for, and provide security services to, the community at large. Our research is generously supported by the UK Engineering and Physical Sciences Research Council (EPSRC), the European Council Framework Programme 7 (EU FP7), Intel Security (McAfee Labs UK), and Royal Holloway, University of London. S2Lab's research activities are also supported by a number of collaborations with academia (including Universita` degli Studi di Milano, Politecnico di Milano, IMDEA Software) and industry (including Intel Security and HP Labs Bristol).

The research in S2Lab crosses the boundaries of a number of different computer science related topics, such as operating systems, computer architectures, program analysis, and machine learning, making our challenging journey always exciting. We are currently covering topics that primarily focus on applying (novel) machine learning and program analysis techniques to improve the security of networks and systems.

These include:
- analysis and detection of botnets and Android malware;
- automatic generation of exploit for heap-based vulnerabilities; and
- machine learning-powered situational awareness.

I am proud to have the opportunity to be working with bright scholars, without whom S2Lab would not exist. In no particular order, these are postdoctoral research assistants Davide Papini, Zhi Wang, Santanu K. Dash and Guillermo Suarez-Tangil Po, and PhD students Kimberly Tam, Salahuddin J. Khan, Gibson Mba, Roberto Jordaney and Dusan Repel. This impressive team is guided by myself and Dr Johannes Kinder from the Department of Computer Science. I am very excited about S2Lab and I want to share with you what two of the other team members think about being in S2Lab.

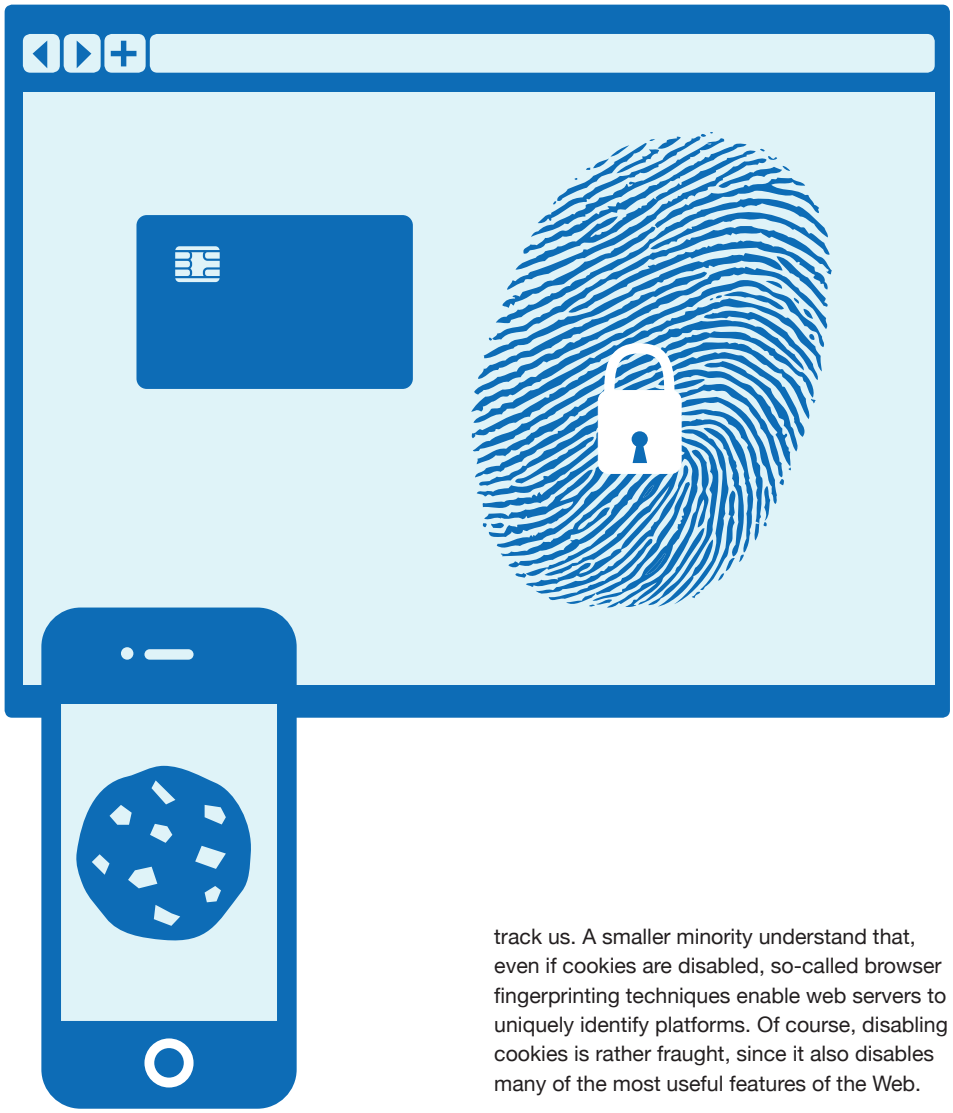
Kimberley Tam
It's great to have the S2Lab room where we can interact and collaborate whenever we want/need to, and I'm also very happy to see the S2Lab group growing in a multi-disciplinary sense as well as in members.

I think the mixture of projects was very well set up since the main projects are different enough that we are all working on something unique and new, but they still overlap, just enough, that we can very much benefit from each other's expertise. There is always something exciting to work on, whether collaborative or individually. The colours that S2Lab have been painted in are, hmmm…, audacious (perhaps a nice tribute to the university colours and clearly not boring). The particular shade of orange might also quantitatively increase productivity by deterring lab members from looking away from their computer screens.

Santanu Dash
Here is my attempt at a fun mission statement for S2Lab: We are Jedis, S2Lab is our Jedi Temple and with our lightsabers we shall vanquish all malware [Lorenzo: hey, the lab focuses on other security problems too, but nice, yeah; well, this shows how much we long for Star Wars Episode VII!] There are lots of exciting projects happening. Conformal evaluation, CopperDroid, and Skyrise are the coolest project-related buzzwords you'll hear in S2lab. Also, Dusan, one of our brilliant PhD students, is experimenting with vodka shots as a substitute for caffeine.

S2Lab is a special place to work because of the exposure it offers to the lab members. The projects that we work on cut across multiple domains such as security, machine learning, networks, program analysis and operating systems. It enables each of us to expand both the breadth and depth of our knowledge. We are a really diverse bunch: currently eight people, from five different nations. Pay us a visit to learn more!

Back to Lorenzo...
I am deeply grateful to the ISG and Royal Holloway for not only believing in the research I wanted to pursue, but also for having concretely contributed to the refurbishment of the space that has now become S2Lab.
For me, S2Lab represents the beginning of an exciting and hopefully fruitful journey. Follow S2Lab's achievements at http://s2lab.isg.rhul.ac.uk and pay us a visit in McCrea 343 on the Royal Holloway campus.



THE DISRUPTIVE EFFECTS OF USER PRIVACY

By Chris Mitchell

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

Introduction

We are all accustomed to the idea that what we do online is not very private. We may not know exactly who knows what, but we do know from personal experience that organisations connected to the Internet, e.g. websites we visit and Internet advertising agencies, monitor our activity and use it to target advertising. In this context 'activity' includes not only where we browse on the web, but our past purchases, the contents of our emails, and other factors we may not even be aware of.

The means by which we are tracked is not so clear, at least to most internet users. A minority of us understand how cookies can be used to track repeated visits to the same website, and also, through the HTTP referrer field and links embedded in web pages, how advertisers can track us. A smaller minority understand that, even if cookies are disabled, so-called browser fingerprinting techniques enable web servers to uniquely identify platforms. Of course, disabling cookies is rather fraught, since it also disables many of the most useful features of the Web.

Web browser fingerprinting techniques have existed for several years, but their use and effectiveness has only relatively recently become widely publicised, e.g. as described in an article published in December 2014 by Sophos. Indeed, such is the sophistication and maturity of the technique that many companies today offer browser fingerprinting products and services. Essentially browser fingerprinting involves a website using its interactions with a user platform (computer, tablet or smartphone), including through use of JavaScript programmes downloaded to a browser, to learn a host of details about the software and hardware of that platform. This might include what operating system and browser are in use and which versions, what the capabilities of the platform are, e.g. in terms of screen resolution, and what fonts are available. This information is sufficiently detailed to uniquely identify most platforms in use. Of course, IP addresses help with fingerprinting, but the use of anonymising routers does not stop fingerprinting.

Whilst our activities can be readily tracked using a variety of means, there is also great pressure to change this, including from legislators such as the European Commission, who wish to protect citizen's privacy; pressure groups of many types, arguing in favour of greater end user privacy; and standards and other guidelines, which set down codes of behaviour and best practices for websites. Supporting these demands for greater privacy are a range of technologies that help support privacy, e.g. including: encryption; good practice schemes such as the 'do not track' HTTP header field; anonymising routers; anonymous credential systems and other special cryptographic schemes; and homomorphic encryption, which potentially enables processing of encrypted data.

However, despite the plethora of technological aids, in practice we tend to largely rely on regulatory/legal compliance solutions to protect our privacy. Such an approach inherently assumes that those with access to our personal data will behave in accordance with law and regulation. Of course, this is a questionable assumption; moreover the level of legal protection for our privacy varies widely as we travel around the globe. As a result, some in academia and elsewhere advocate a purely technological solution, arguing that use of appropriate technology could prevent any misuse of personal data, however it might arise. However, the consequences of such an approach, if it could ever be realised (which is, of course, a big if), are profound, and this is the main focus of this article.

Possible privacy goals

Perhaps the ultimate goal of privacy advocates is to enable us all to leave no identifiable trace of our activities, if that is what we want. Some would suggest that such an arrangement should even be the default, given that many users have limited technical expertise. However, defining what no trace means is problematic.

To see why even defining the type of privacy we might want is difficult, it is necessary to observe that almost everything we do partly identifies us, e.g. we indicate our language, interests, etc. by where we choose to browse. In addition, some activities automatically reveal our unique identity, e.g. when we use a credit card for payment. Perhaps the key property we might wish to achieve is linkability of activities, or rather unlinkability. That is, we might reasonably wish for two distinct interactions with the same or different websites to be incapable of being linked by these websites.

These difficulties in definition highlight the difficulties in effectively anonymising personal data. Such anonymisation has clear benefits, allowing large data sets to be analysed, e.g. to identify new treatments for illness, new solutions to complex problems, etc. However, the risk of de-anonymisation (or re-identification) is always present, so anonymisation needs to done with great care. However, this is a subject for a different article.

Disruptive effects

The supposition for the next part of this article is that the privacy advocates are completely successful, and by default all our activities are unlinkable (except where necessary). That is,

suppose we can all use the Internet knowing that, unless we choose to reveal who we are, it is technologically impossible to link our various interactions with third parties. 'Hurrah!' we might all say, except that the potential impacts are far-reaching. Most obviously, the service providers would lose their ability to link one user interaction with another, severely limiting their ability to target advertising. Perhaps less obviously it would also affect both security (of users and service providers) and usability in a variety of ways. We next look at these impacts in a little more detail. Perhaps I should observe at this point that the observations made below are not new – many authors have been saying similar things for some time, but it perhaps helps us all to be reminded of the implications of pursuing higher levels of privacy.

No more free stuff?

Many of the free web services we use on a daily basis are funded through advertising. Examples of such services include search, cloud storage, social networks, messaging (email and instant), Internet gaming, and voice over IP. That is, it includes things that most of us rely on all the time in our daily lives, both at work and outside. It seems evident that loss of targeted advertising could severely impact advertising revenues for these service providers, as well as other possible revenues. With a potentially much reduced revenue stream there will presumably be fewer free services for us all to enjoy.

How might this affect us? Well, perhaps we will have to start paying for all these services. Alternatively, maybe some service providers and/or services will simply vanish, if it becomes uneconomic to provide them. In any event, we should expect a huge disruption in the economics of the Internet. Some would say this is a small price to pay for greater privacy, but others may disagree.

Less effective security

Security and privacy often push in somewhat different directions. We next highlight a few ways in which more effective, technology-driven, privacy provision could affect the provision of security, and might ultimately damage some end users.

Some Network Intrusion Detection Systems (NIDSs) examine DNS messages. As a result, if DNSsec encryption was to be widely deployed, which would, of course, enhance security as well as privacy, then such messages become opaque to the NIDS. That is, by concealing traffic, detecting intrusions becomes more difficult. It has also been widely suggested that DNSsec could make distributed denial of service attacks much more effective, although the degree to which this is true has been disputed.

Browser fingerprinting has both positive and negative aspects. Clearly it negatively impacts user privacy. However, it is also widely used as a means of enhancing user authentication, by verifying that a user is working via a known platform. That is, if browser fingerprinting was made impossible (actually, very difficult to achieve for anyone other than an expert user) then user authentication would be made less effective.

As is well known, effective user anonymity makes ensuring that users are held accountable for their actions very difficult, if not impossible. That is, efforts to investigate security breaches may be made very much more difficult if all the activity records are unlinkable. More generally, criminal investigations could be made much more difficult. Legal interception may also be made much less valuable to investigators.

Less effective everything

We finally briefly observe how privacy might impact usability. Browser fingerprinting techniques are used by many websites to understand the capabilities of user platforms, thereby providing content tailored to that platform. For example, content sent to a smart phone can be tailored to display effectively on a small screen, as opposed to content sent to a desktop PC. Indeed, it is hard to see how some details of the end user platform can be withheld from content providers without seriously affecting usability.

Similarly, one of the features of cookies that most of us rely on is the e-commerce 'shopping basket'. We can get part way through our supermarket shopping on line and the contents of our half constructed order will survive even if the platform is rebooted. I know many of us regard this as an essential feature, without which e-commerce would be much less useful. However, this reliance on cookies automatically seriously reduces the degree to which we can stay private.

Concluding remarks

I should say at this point that, lest I be marked down on somebody's hit list as an enemy of all that is good and just, this short article is not intended as an argument against enhancing user privacy – it is just intended to point out some of the implications. In fact, implementing complete unlinkability is theoretically possible but very difficult to achieve in the real world. For example, our browsers leak vast quantities of information about us; however, the technologies required to fix this are not simple to use. Few of us even know what anonymising routers are or what the threat is that they address, let alone use them, and it is not very practical to expect users to start with a clean OS installation every time they browse the web.

One possible outcome of any significant reduction in the ability of web servers to track users is that we will be given more overt choices between a reduction in our level of privacy and making a payment for service. Whilst users say they value their privacy, in practice they appear to be reluctant to spend money to do so. For example, AT&T in the US allows gigabit service subscribers to opt out of deep packet inspection for a $29 monthly fee. Apparently most users do not pay the extra fee, although whether this is because they do not value privacy, or they do not trust AT&T not to track them even if they do pay the extra, is unclear! Such a pricing versus privacy approach is not universally popular, as, for example, an opinion piece in The Guardian on 21st February 2015 makes clear.

Another direction much discussed is giving the ability for users to choose, perhaps from one instant to the next, to what degree their privacy is impinged. That is, for some sites users might be happy to take a more relaxed view of tracking in return for free service, whereas for others they may wish to have their interactions remain completely unlinkable. Whilst this is possible in principle today, e.g. by running 'clean' browser instances in separate 'vanilla' virtual machines, for most of us this is not a practical option. Of course, this is precisely the sort of thing that HTTP 'do not track' is meant to allow, but it would appear that most websites ignore such a request.

A further issue is that if law enforcement and other government agencies cannot access data via interception, then they are likely to try other methods. These other methods may be even more intrusive. For example, there has been much recent discussion of malware distributed by western governments for user monitoring, including the recent damaging revelations about apparently government-originated malware infecting hard drive firmware. Whilst this particular malware appears to have been used only to target high-value individuals, use of such an approach could easily be extended to allow for mass surveillance. If course, it could reasonably be argued that such approaches are likely to be used by governments anyway, even if we fail to deploy better privacy technologies. Getting the balance right is clearly very difficult, so what can we reasonably expect to see happen? Even the most strident advocates of technological privacy solutions do not suggest the legal/regulatory/compliance approach should be abandoned, and this approach will surely continue, as will the development of best practice guidelines/standards. Privacy technology will also continue to advance, and some of it will no doubt be deployed. However, I fully expect security agencies and others to continue to develop ways round deployed technologies.

Of course, highly skilled and highly determined individuals can, as now, make their activities pretty private, but they are essentially irrelevant to the argument. So probably not very much will change, and the possible disruptions discussed above will not happen, unless, of course, legislators demand it. Nevertheless, the potential for huge disruption remains. Perhaps the best way of summing this up is to say that, in the words of the old adage, we should be careful what we wish for.

SMALLPEICE CYBER SECURITY RESIDENTIAL FOR SCHOOLS

The ISG has formed a partnership with the Smallpeice Trust to deliver three-day residential courses for 13 and 14 year old (Year 9) students that give them insight into the fascinating area of cyber security.

The first event ran in April 2014, with 50 students from across the UK benefitting from a unique hands-on learning experience at Royal Holloway. The course demonstrated to students how important it is to be aware of the risks we are taking in cyberspace, especially as we are increasingly spending a significant proportion of our lives there. Working in small teams, they got a unique opportunity to explore some of the threats to cyberspace and the techniques currently being employed to provide cyber security, by tackling a series of cyber security challenges. They also got to meet real-life cyber security professionals, learning about the challenges they face each day in securing cyberspace, while discovering some of the fantastic career opportunities on offer in this dynamic sector.

The second workshop ran in April 2015, where another 50 students embarked on a capture-the-flag challenge, which saw them defeating software vulnerabilities, opening safes and building lego cyber worlds. The 2015 event was sponsored by GCHQ and assisted by Sigmatak and the Cyber Security Challenge, as well as various friends of the ISG.

The UK National Cyber Security Strategy identifies the need for cyber security education at all levels of the curriculum. While we normally focus on students in higher education, it has been a real pleasure having so many budding cyber security specialists on our campus. We hope that some of them were sufficiently inspired that they will consider pursuing an educational pathway that leads to a cyber security career. We look forward to welcoming Smallpeice and another batch of students in 2016.

MY ROYAL HOLLOWAY EXPERIENCE
by Kacper Dudzinski

> Kacper Dudzinski is a pupil of Grey Court School, Richmond, Surrey

I loved the cyber security course and it was great fun. The course appealed to me because it looked fantastic and I knew that I would learn a lot of things that I would need later on, when I pursue a career in Computer Science. I didn't believe we would actually 'hack' anything, as that sounds like something which requires a lot of knowledge and experience. So I was surprised and impressed at the workshops this course had to offer.

I enjoyed the various lectures which included things such as cryptography, security visualization, malware and of course cyber security. In cryptography we learnt the three basic ciphers: Pig-pen, The Caesar Cipher and The Substitution Cipher. The Substitution Cipher is the most secure. Here, each letter becomes a random letter in the alphabet. Although there are millions of possible outcomes, it's not that hard to crack because of its context. For example, if the letter F shows up a lot you can assume it is the letter E, which is the most common letter in the English Language. Cryptography involves a lot of assumptions, guesswork and dead ends. We also had a chance to win some chocolate!

In security visualization we used Lego to create models. I found the malware lecture particularly interesting. In this lecture we learned about things such as Trojan horses, botnets (how they work and what dangers they pose), the internet and how it communicates between client and server and how the data being sent can be interpreted, we learned about cookies and sessions, proxies and about HTTP. My personal favourite was the software workshop, where we had to hack each website to continue to the next, harder one. We had to view the source code and try to find things hidden in it. We also got to use proxies to change the data that we were sending. It was a challenging but fun task, where teamwork was essential.

During the course we had an ongoing competition called capture the flag. The story behind it was that there is an evil computer system called Messy or MS42. When we completed one of the activities for example after hacking each website in the software workshop, we got a special code. We then entered the code into a website to shut down one of Messie's sub-systems. The team who shut down the most or all the sub-systems the fastest won a prize. I am pleased to say that it was our team that won!

The rooms we stayed in were amazing. We had a big bed as well as our own showers. Additionally at the end of the corridor was a kitchen where we chatted while having a cup of tea. There were recreational activities such as the Imagine Activities where you could watch a film, take a quiz, play various games or just chat while enjoying a cool drink. There was also the fantastic barbeque and disco, where we got to relax after a day of hard work. The staff were really nice and helpful, especially the student ambassadors who didn't hesitate to give us a hand or moral support when we were stuck.

We met and worked with different people and we made new friends, or strengthened existing bonds. It was a chance to learn interesting things in a more casual and relaxed environment. We also got a tour of the Royal Holloway, University of London great campus, visiting buildings like the library, the computer building and of course the quads, where we saw the statue of Thomas Holloway, the founder of the university and Queen Victoria. We saw and experienced university life. During our stay we also learnt a bit about the University and Thomas Holloway. In fact, we even made a presentation on him while practising our presentation skills. Did you know he made his fortune selling fake medicine?

At the end of the course we got to show off everything we'd learnt by making a presentation in front of the staff, our peers and our parents in the beautiful picture gallery. We developed skills such as teamwork, co-operation, communication as well as perseverance.

Now that the course had finished, I am even more convinced that a career in Computer Science is what I want. I also learned more about cyber security and how to keep my computer safe from malware and other attacks that may harm it. Simple things like an anti-virus, firewall and secure passwords keep you safe every day. For example if you have one password for all your accounts, if they get into one, they can get into all of them, leaving you totally exposed. That's why you should have different passwords for all your accounts.

I loved every second of this course and I would recommend it to anyone who is interested in computer science or cyber security, or just anyone who is looking for a fun and interesting course.

STAFF PROFILE: PETER KOMISARCZUK

> Dr Peter Komisarczuk is Director of Distance Learning in the ISG

Tell us a little bit about your background

Well I have been in the networks/telecoms world since 1984. By 2014 I had spent half my working life in industry and half in academia, working mostly in R&D roles, but with a foray into consultancy and academic management as well.

I started out in pure and applied physics and, I have to say, it was a great choice. I really enjoyed the mix of physics, programming, electronics and operational research. My first job was in the electricity supply industry. Unfortunately they had too many control and transmission engineers, so within a few days of joining I was embedded in the corporate network team – leased lines and modems, followed by circuit switched data and X.25 packet switched networks. I have since worked for Ericsson, Fujitsu, and Nortel in various R&D roles, picking up my PhD along the way. I switched back to academia in 2003, with eight years at Victoria University of Wellington in New Zealand and then Professor of Computing at the University of West London, before joining the ISG at Royal Holloway at the start of this year. Most of my work has been based around telecommunications, the Internet and its protocols, and technologies, including security, which were applied in product R&D, standardisation, research and consultancy activities.

What attracted you to come to Royal Holloway?

The ISG of course! The potential to engage in a more research-oriented environment and gain more expertise was key to my decision. The breadth of research and enterprise engagement undertaken within the ISG is fantastic. In my previous role I had an enterprise development hat on, which I am keen to keep wearing.

I am currently a co-investigator working on an inter-disciplinary project funded under the EPSRC CEReS initiative, looking into identifying and modelling victim, business, regulatory and malware behaviours; which is a tall order. A decade ago I would have focused primarily on the technical aspects of cyber security but the reality is that the Internet and cyber security are many-faceted and also comprise economic, business, political, psychological and sociological dimensions. I think there is potential to develop further work relating the mathematical sciences and the interdisciplinary nature of cyber security. Being part of the ISG could allow me to help to develop that further.

How did you get into the area of cyber security?

From an industry perspective I gained knowledge around network management systems security and then around Internet infrastructure and Internet access protocol architecture, as well as solutions such as L2TP, PPPoE, RADIUS etc. It was in 2004-5 that I began a more academic exposure to security with collaborator Dr Ian Welch at Victoria University of Wellington. It came about as a couple of fortuitous engagements.

The first was with Dean Pemberton, then a network engineer based in Wellington, who wanted to undertake an MSc and had access to an unused /16 address space! A network telescope was created and ran for some 18 months; it picked up a bunch of backscatter and reconnaissance scans which created a huge dataset and has been used in a couple of projects.

The second was when Dr Christian Seifert joined us in 2006 to work on a PhD in the area of honeypots. Specifically this resulted in the creation of several client honeypot technologies that were then employed to analyse drive-by-download attacks on computer systems, which was a new area in 2006. We created the low interaction client honeypot HoneyC and then a Windows XP behaviour analysis tool, Capture-BAT, that led to the development of the high interaction high capacity client honeypot Capture HPC. It was these that got us working with the Honeynet Project in particular, and Christian developed the New Zealand chapter in 2007-8. As part of this work we developed a scan of the.nz domain for InternetNZ which ran for about two years.

This work led to an invitation to join the NZITF (originally the NZ Botnet Task Force) resulting from a brief encounter on disembarkation at Wellington airport in 2007. The NZITF is an organisation comprising industry, government and academia that have a mandate to improve the cyber security posture of New Zealand. I was academic liaison for a couple of years until coming back to the UK in 2010, which was a real privilege.

Can you tell us more about the Honeynet Project?

The Honeynet Project is based out of the US and is a non-profit, all-volunteer organization that aims “To learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned”. The organisation is made up of a core board of directors and chapters from all over the world and is a bunch of great talented people. It has developed a set of useful open source tools from honeypots through to analysis tools; they span server, desktop, virtualised and mobile platforms. Christian Seifert created the New Zealand Honeynet chapter and Dr Ian Welch and myself took over the chapter in 2009. Unfortunately my involvement with the Honeynet Project has been severely reduced since 2011-12 as my day job became more intense and not related to security; and being based in the UK meant it was difficult keeping things going with collaborators in New Zealand. As part of the Honeynet project we were involved with tool development and data gathering plus other activities such as participating in several rounds of the Google Summer of Code (GSoC) from 2009-2011. In GSoC students would work over the summer on development of open source tools (and get paid by Google) which would aid the extension of existing data gathering or data analysis tools or sometimes create whole new tools.

I would like to get some ISG students involved in Honeynet Project related activities in the next few years. There could be GSoC opportunities in 2016 as well as MSc and BSc projects using or developing the tools from the Honeynet Project.

What’s your first impressions of the distance learning MSc programme?

First impressions are positive; the course has a good number of students and content

that is well-aligned with the campus course. The support team is an impressive mix of ISG staff and researchers, alongside professional practitioners. The MSc syllabus as envisaged for September 2015 provides some coverage of 12 out of the 13 skills groups within the IISP Skills Framework, which is fantastic.

//

What are your plans for taking the programme forward?

The key to the future is to get more students onto the programme and provide an even better student experience. Engaging with the students and understanding what they really want, as well as establishing what their study experience is like, will form the basis from which the programme can be taken forward. There are some themes around practical work and syllabus coverage that I will be exploring with the students. Additionally we are working with the University of London to further improve marketing and services.

Providing additional practical work within the degree wherever possible is one area I am keen to explore, however there is a tension between student workload and module coverage. The previous Director of Distance Learning, Colin Walter, had already begun the addition of more practical oriented content with establishment of a distance learning version of the campus module "Security Testing: Theory and Practice" which is planned to start in September 2015. I will be investigating other opportunities with the module teams over the next year to see what else could be provided.

In addition there are other modules on campus that could be provided to the distance learning students if there is sufficient demand and academic coherence. For example the Secure Business Architectures module led by Geraint Price would enhance some skills area coverage with its case studies in PCI DSS, BYOD, cloud and big data. Additionally the Software Security module led by Lorenzo Cavallaro provides practical coverage in some aspects of software and web vulnerabilities and attacks, which includes some hands-on hacking-oriented activities and would be a popular addition to the distance learning version of the degree.
This will keep us busy!

//

Do you think MOOCs are an important part of the future for higher education?

Certainly MOOCs (Massive Open Online Courses) have had a positive impact on broadening access and providing a taster of higher education and I would like to see this initiative succeed. Within our field I am keen to see how well the new MOOC offered by the Open University to introduce Cyber Security to the wider public has worked in developing general awareness and practice. There are also a bunch of MOOCs I am interested in taking around big data and analytics if I can find the time!

The MOOC financial model is still being developed and it takes a lot of effort to develop and run a MOOC, so we need incentives to do that. The potential to use MOOCs as a marketing technique is the key driver, thereby providing a stream of students onto degree programmes. I am keen to persuade the ISG to develop at least one further MOOC, following on from Lorenzo's successful Coursera MOOC on Malicious Software and its Underground Economy.

//

Edward Snowden: Naughty step or pedestal?

Quis custodiet ipsos custodes? Overall I think of Snowden primarily as a whistle-blower, but he is also a traitor. Some aspects disclosed make his crime more palatable, so I would describe myself as more "on the fence" and would not put him either on a pedestal or the naughty step. It is good for us to have gained some of these insights into aspects of the NSA and GCHQ surveillance that overstep the mark, however his leaks have a negative impact too and so counter-espionage and anti-terrorism efforts have probably been affected. The leaks, I hope, will lead to surveillance activities becoming more transparent and controlled, with enhanced accountability in place, but it will take time and effort by key advocates and organisations to champion rights and bring such activities to account.

//

What should we all know about you that you haven't told us already?

I enjoy watching rugby and support the All Blacks and so I am looking forward to the World Cup this year!

THE REAL WORLD CRYPTOGRAPHY MOVEMENT
By Kenny Paterson

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

Something is stirring in the space between theoretical and applied cryptography. In January 2012, Nigel Smart from the University of Bristol and I jointly organised a workshop at the Issac Newton Institute in Cambridge, provocatively entitled “Is Cryptographic Theory Practically Relevant?”. The workshop was intended to ignite the process of reuniting theoretical and applied Cryptography, which Nigel and I felt had drifted too far apart.

Holding the workshop as part of the celebrations for the centenary of Alan Turing’s birth seemed entirely appropriate to us. After all, Turing is not only one of the most famous applied cryptographers of all, but his work was also built on solid theoretical foundations. Apparently Nigel and I were not alone: participants filled the Newton Institute’s 100-seater lecture theatre to hear a rich variety of speakers from academic and industry talk about their conception of the gap between theory and practice, and about whether - and how - it should be bridged.

Follow-up events were held at Stanford in January 2013 and in New York in January 2014, with the numbers of attendees growing steadily and the beginnings of the “Real World Crypto” movement starting to taking shape. Along the way, we were joined by Dan Boneh, Tom Ristenpart, Tom Shrimpton and Aggelos Kiayias to form an organising committee, the domain www.realworldcrypto.com was commandeered, and sponsorship was secured.

The latest event in the series, RWC 2015, was held at the London School of Economics in January this year, with myself as local organiser. Planning for the event began almost six months earlier, with the team starting the process of selecting the invited speakers and drumming up the financial support necessary to keep the event as cheap as possible for participants: in contrast to most cryptography conferences with registration fees as high as £350, the registration fee for RWC 2015 was a nominal £50, cheap enough for everyone to participate. Everyone did participate - or so it felt. Registration closed at 400 people, and the LSE’s biggest lecture theatre was packed for every session. The “contributed talks” sessions were three times over-subscribed, and the lightning talks session saw a queue of 20 eager speakers form at the foot of the stage to give two-minute pitches about their work. There was a poster session which allowed students to show off their latest results in an informal environment, with wine and snacks.

And, of course, there were the 26 invited talks, given by a huge range of speakers from the industrial, academic and government sectors. Highlights included talks from Akamai and CloudFlare - major content distribution network providers - and Twitter, all addressing the problem of handling TLS at astonishing scales, from Facebook on the problems of managing hundreds of millions of users and their passwords, and from insurgent startups like Cryptosense, Certivox and Sharemind showing us what the future might look like. These were complemented by academic speakers talking about their latest research, carefully selected by the organisers to ensure a balance of topics close to the applied/theory boundary. Industrial and EU sponsorship enabled the RWC team to support the participation of around 40 students from all corners of the world; EPSRC funding made it possible to invite some outstanding speakers; and funding from the EU CryptoAction project covered the cost of venue hire.

The popularity of the 2015 event - with an attendance larger than any mainstream cryptography conference in 2014 - shows that something is afoot here. Arguably, RWC is serving a latent demand that was created by the IACR’s flagship cryptography conferences having steadily narrowed their focus to concentrate on theoretical (and sometimes overly esoteric) aspects of cryptography - research that is foundational and that one can hope might be useful for the long-term, but that has very little to do with the practice of cryptography today. Of course, those conferences can only reflect the scientific work that researchers decide to submit for publication. At the same time, though, there is plenty of great research going on in applied cryptography. But this genre now seem to find a more appreciative audience at the leading security conferences. And it seems hard to reverse the trend: now that the applied cryptography community has moved off to other venues, it’s not obvious what the leadership of the IACR can do to bring them back.

It remains to be seen how RWC will evolve and how it will shape the cryptographic community. Up till now, it has been a low-cost, high-quality workshop with carefully-selected invited speakers and a frothy mix of participants from industry and academia. This seems to be a winning formula - the organisers conducted a survey after the London event, and received almost uniformly positive responses. The response rate to the survey was nearly 50%, notably high in a world that is saturated with on-line surveys. This is a sign of the strength and engagement of the community that the RWC team is building. Planning for RWC 2016 is already underway. The event will be held at Stanford again, in the first week of January next year. The programme is starting to take shape at www.realworldcrypto.com/rwc2016, and you can follow developments at @realworldcrytpo on Twitter.

There are many ways you can get involved in the RWC movement - register early for RWC 2016; nominate speakers via the website; consider becoming a sponsor, associating your brand with the most exciting crypto event on the planet; maybe even start up an RWCx event - if you do, we’ll be glad to hear from you.

SMART CARD CENTRE OPEN DAY

After a one year absence for the organisation of ESORICS 2013, the ISG Smart Card Centre (SCC) Open Day Exhibition made an impressive return to celebrate its 12th Anniversary in September 2014. There were 12 industry/government exhibitors and a record number of SCC student exhibitors (9 PhD, 14 MSc). The event prizes went to Rowena Harrison for her MSc project investigating obfuscation and mobile app reverse engineering, and to CESG for its display on lightweight cryptography solutions. There were a number of short industry/government presentations and a guest lecture that highlighted the real world relevance of the SCC research area and training activities. This theme was echoed by the College Principal, Professor Paul Layzell in his opening address, which emphasised the ISG's pivotal role in 'filling industry's needs'.

The event was supported by SCC sponsors; Transport for London, the UK Cards Association, Visa and ITSO as well as the event sponsors; Comprion, Cubic, Giesecke & Devrient (G&D), Infineon and the Underwriters Laboratory (UL). Invited presentations were from Vodafone (Steve Babbage), Mastercard (Dave Roberts), MAOSCO (Chris Torr) and CESG. The guest lecture was from G&D (Klaus Vedder). Prof. Keith Mayes, Director of the ISG Smart Card Centre, was very pleased with the day. "The SCC Open Day was a great success and I was very pleased to see so much active participation. The principle of combining SCC students with industry and government in this event as well as the underlying research projects and internships is as relevant today as it was 12 years ago.

These days SCC projects are less often about traditional smart cards and more about other forms of embedded and implementation security. The student exhibitors covered topics including smart phones, Near Field Communication, Smart Tickets, RFIDs, the Internet of Things, Trusted Execution Environments, Host Card Emulation, as well as overall application/system security solutions and attacks against them. The future may not be as secure as we all would like, but it will certainly not be dull in the SCC!"

We are Anonymous
by Parmy Olson

This is a fascinating insider look at the group Anonymous. I found it highly intriguing to be given an insight into the lives and mind sets of some of those involved in the Anonymous movement. This book is much more of a social study than a technical discussion, but gave a really good qualitative assessment of the motivations and thinking behind those involved in some pretty ground breaking activity. A really excellent read.

Steven Hersee

Communication Theory of Secrecy Systems
by Claude Shannon

I have been reading this classic paper as part of writing the introduction to my PhD thesis. Although this paper covers a huge range of topics, it's particularly interesting because it hints at several ideas from modern cryptography (like key-alternating ciphers and algebraic attacks) even though it dates from 1949.

Gordon Procter

A Practical Guide to Trusted Platform Module 2.0
by Will Arthur and David Challener with Kenneth Goldman.

The TPM is designed to improve the trust in computing devices by offering certain functionalities. This book is written with the intention of lowering the learning curve. It gives the history, describes concepts and detailed implementation and offers use cases and coding examples. The authors of this book did an excellent job of explaining TPM 2.0 and added value by writing about application development for TPM 2.0. The coding examples and debugging tips are especially useful.

Jiun Yi

Critique of Security
by Mark Neocleous

This book challenges the reader to question some of the assumptions we make about security, in particular that security is a social good. It grounds the topic in the history and traditions of security thought and then presents critiques of this tradition. Certain forms of security are critiqued as not being focused on the protection of the individual, as is espoused, but on the order and control of the individual - this point is made about domestic national security policy and about social security but could be made about employee access control systems. The book concludes with a call to reconceptualise security to include social responses such as networks of solidarity and resilience. I found it uplifting to read a book that questioned the validity of security concepts that our area of study so often takes for granted. Some of the questions that the critique raises are uncomfortable for "security people": particularly the question of whether as an industry the goal is insecurity rather than security, because insecurity stimulates demands for security technologies and services. I think it is valuable to present an alternative perspective and have made this one of the course books for our security management module.

Lizzie Coles-Kemp

Bitcoin: The Future of Money?
By Dominic Frisby

Actor, comedian, financial journalist and author (a rare combination!) Dominic Frisby takes a hard look at the Bitcoin project and comments on what the outlook is for cryptocurrencies. He is of course too sensible to commit either way, but I liked his very real engagement with the Bitcoin project. He meets some of the pioneers, the traders, the believers, and also cast some of his own financial expertise into putting cryptocurrencies in perspective. You won't find many details of how Bitcoin works in this book, but you will get drawn into the whodunit thriller that lies behind the launch of the Bitcoin project. Did I log on to an exchange and immediately purchase some Bitcoins after reading this? Err.. no.. But maybe I am too cautious by nature.

Keith Martin

WHAT I HAVE BEEN READING RECENTLY

Ghost in the Wires: My Adventures as the World's Most Wanted Hacker
by Kevin Mitnick

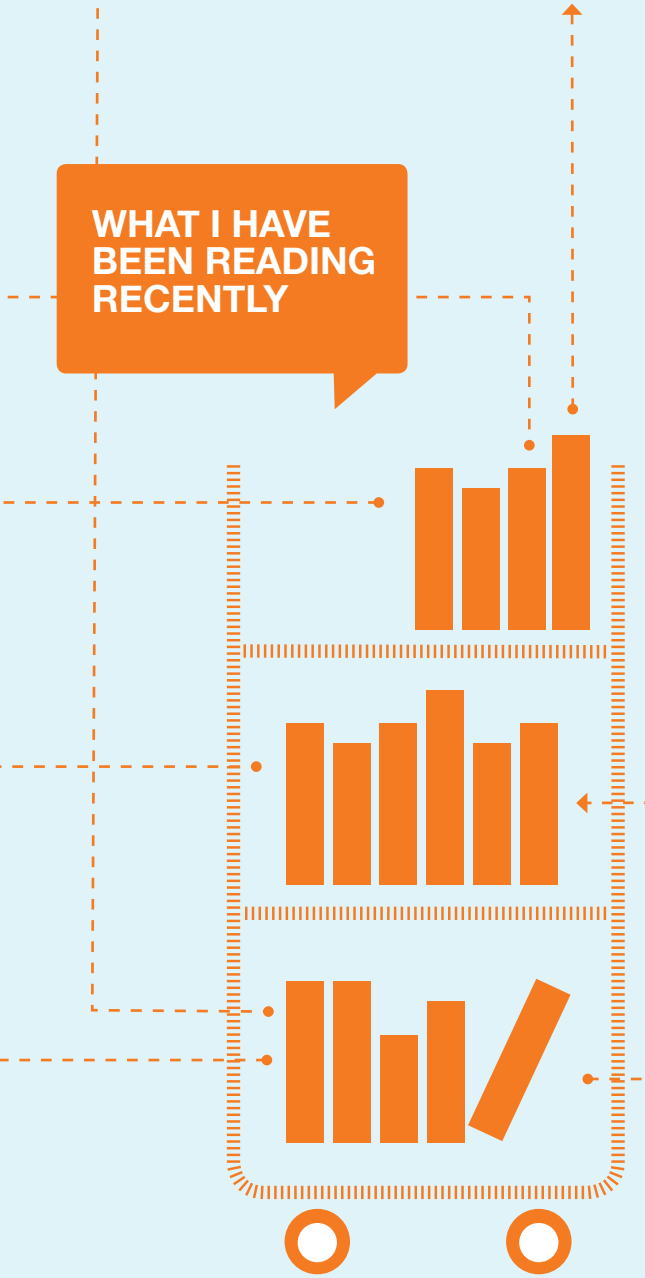
Ghost in the Wires is Kevin Mitnick's autobiographical account of his early years as a hacker. The story covers Mitnick's initial forays into phone phreaking, detailing the development of his social engineering skills, his natural progression to computer hacking, and his subsequent high-profile incarceration. The book is a fascinating read, providing insights into both the mindset and activities of one of the pioneers of hacking. Mitnick writes engagingly and the story moves along at a steady pace, regularly stopping to delve into technical details regarding specific telephone and computer systems. Highly recommended.

Andreas Haggman

Security De-Engineering: Solving the Problems in Information Risk Management
by Ian Tibble

This book claims that there are two main types of information security professional. First the "hackers" who are highly technical but do not have any "business" understanding. Then there are the "Checklist and Standards Evangelists" who have limited technical knowledge and follow processes without real underlying understanding. Tibble argues that we really need more professionals with both skills. He also explains why some of the tools that we have been using are not as effective as some people think they are. I found this a somewhat pessimistic book, but it helped me to understand what can go wrong with practical information security. Since I was already aware of some of these problems, this book helped me to contextualise aspects of my own information security career.

Lazaros Kyrillidis



No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State
by Glenn Greenwald

This book starts by describing the fascinating story of the encounter between Edward Snowden, Laura Poitras and Glenn Greenwald. Along the way, Greenwald gives an account of his interview with Snowden and the events in Snowden's life that motivated him to become a whistle blower. The focus then shifts on the leaked documents and their significance. The final sections of the book discuss the role of the media in relation to the government, and the impact of government surveillance on a nation's democracy. This book combines a thrilling narrative with a compelling discussion on the ethical aspects of the surveillance state. It is a must read for anyone interested in understanding the issues relating to surveillance and the sociopolitical implications of Cryptography and Cybersecurity in general.

Jean Paul Degabriele

PLUS CA CHANGE: 25 YEARS OF THE HEWLETT-PACKARD INFORMATION SECURITY COLLOQUIUM

By Kenny Paterson

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

Things continually change in our field of cyber security - not only the buzzwords, but even the name of what we do (Information Security, Information Assurance, Cyber Security,....). But some things remain resolutely constant. One of those constants is the Hewlett-Packard Information Security Colloquium, HP Day to its friends.

Every December since 1990, the ISG has gathered its wide circle of friends from government, industry and academia to hear eminent speakers give their views on the current state of the field. Over the 24 years from 1990 up to 2013, we have heard from a total of 71 different speakers on a huge range of subjects, covering every aspect of Information Security: technical, legal, managerial, psychological and more.

The continuous sponsorship by Hewlett-Packard over this long time period is remarkable in these times of constant change. It reflects the stability of the company, the long-term view taken by its research staff, and the strength of the relationship between HP and the ISG. We deeply value their support.

A few cosmetic things have changed along the way. The sit-down lunch in the College's Picture Gallery has been replaced with a more dynamic (and less post-prandial sleep inducing) stand-up buffet; posters showing the best of the ISG's research have been introduced; the HP and ISG staff have aged mostly gracefully; we now use a modern teaching space in place of the creaky old Main Lecture Theatre; there's been a regular refreshing of the attendees as new friends enter our sphere and old ones depart.

To mark the event's silver anniversary, we decided to do something a bit different for the 2014 edition of the colloquium. We invited back 12 former HP Colloquium speakers to give short talks reflecting back on their original talks from today's vantage point. What emerged was a kaleidoscopic view of the field, but one in which, while the buzzwords and terminology have changed, the fundamental issues remain very much the same. We were also delighted to have short introductory pieces from Prof. Fred Piper and David Dack, the originator and original funder of the colloquium.

To get a fresh, forward-looking view, we handed over a chunk of the day's schedule to the next generation of leaders in the field: the students from our Centre for Doctoral Training in Cyber Security. They did not disappoint, putting on a thought-provoking and sometimes hilarious piece of theatre showing how Information Security might look in 2039, when reflected through the prism of a daily news programme.

The future, as envisaged by our CDT students, looks very different to the past. But the basic problems are still the same - some things really don't change. So here's to the next 25 years.

Hewlett–Packard Colloquium on Information Security

December 15th 2014

09:45 – 10:00
Introduction, award of David Lindsay prize, opening remarks from Fred Piper and David Dack

10:00 – 10:20
Prof. Andrew Odlyzko (1994)

10:20 – 10:40
Robert Carolina (1995)

10:40 – 11:00
Dr. Burt Kaliski (1996)

11:30 – 11:50
Prof. Peter Landrock (1997)

11:50 – 12:10
Dominic Steinitz (1997)

12:10 –12:30
Prof. Paul Dorey (2000)

12:30 – 13:30
lunch, posters, networking

13:30 – 14:20
Students from the Royal Holloway Centre for Doctoral Training in Cyber Security present "News Time 39"

14:20 – 14:40
Chris Potter (2007)

14:40 – 15:00
Graham Edwards (2001)

15:00 – 15:20
Dr Kieron O'Hara (2005)

15:20 – 15:50
Tea (and 25th anniversary cake)

15:50 – 16:10
John Austen (1992)

16:10 – 16:30
John Meakin (2005)

16:30 – 16:50
Colin Whittaker (2009)

16:50 – 17:00
Closing remarks

MY MSC INFORMATION SECURITY STORY
By Katherine Woods

> Katherine Woods is recipient of the 2014 Most Outstanding MSc Information Security Student Prize

I didn't come from a particularly strong technical background, having completed my BSc in Psychology at Royal Holloway in 2002. Working in business roles within a security solutions organisation provided me with insight into the industry and technologies and, importantly, enabled me to develop an understanding of some of the security concerns and challenges that businesses face.

Supported by my employer, I chose to take Royal Holloway's MSc in Information Security in order to formalise my security knowledge and to strengthen my technical understanding. I was interested in the choice of both business and technical modules offered as part of the course, as I view the ability to bridge the gap between the technical and business worlds as important. Traditionally information security is perceived as a technical discipline, but to ensure robust support for an organisation's strategy and objectives there needs to be an understanding of the wider business context. There is often a need for consultants to discuss security issues with people at different organisational levels, all with their own priorities and appetite for risk; therefore there is a need for the information presented to be relevant to the audience.

Information security involves focusing on a combination of the technology, processes and people and this was reflected throughout the course. People and processes are key aspects that can be overlooked by some organisations, in favour of technical controls. However, if the people and processes are neglected then even the most advanced technical solutions will prove ineffective. Many modern attacks include the psychological manipulation of people through social engineering, for example using phishing to target users. Despite this, security training and staff awareness activity is often lacking.

I took the course part time over two years, while working within the industry. The modules were conveniently grouped to enable me to continue working full time, with one day a week at university and with the option to complete some modules in block mode. I completed my MSc in 2014 and took my final exams while on maternity leave with my young daughter - it was a challenge, but well worth the effort.

The project is looking to extend analysis, partner with owners of data, and begin the modelling to combine the different strands of the project into a probabilistic framework.

PREDICTING AND LIMITING IMPACT OF CYBERCRIME
By Peter Komisarczuk

> Dr Peter Komisarczuk is Director of Distance Learning in the ISG

Identifying and Modelling Victim, Business, Regulatory and Malware Behaviours in a Changing Cyberthreat Landscape is an EPSRC CEReS project, now in its second year. The project aims to more fully understand what causes cybercrime and how to best predict its occurrence, and limit its impact upon the UK economy and society, using methods and concepts from a range of disciplines, including criminology, psychology, economics, mathematics and computer science. The research consortium is led by Cardiff University and includes City, Durham, Plymouth and Royal Holloway.

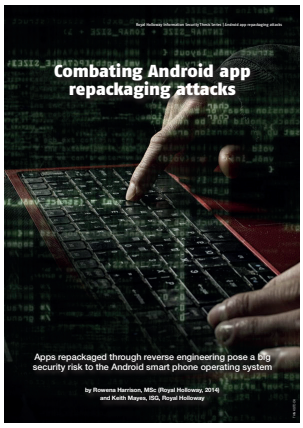
The key objectives of the project are to identify, understand and predict:

01 The behaviour of malware and human cyber perpetrators within and outside of cloud environments;
02 Business risk assessment practices, threat awareness levels, and adaptive behaviours as related to cybercrime;
03 The response of criminal justice agencies to cybercrime and business trust in the regulatory system;
04 Business and criminal justice cyber security practices (e.g. information sharing) in relation to issues of privacy, accountability and civil liberties.

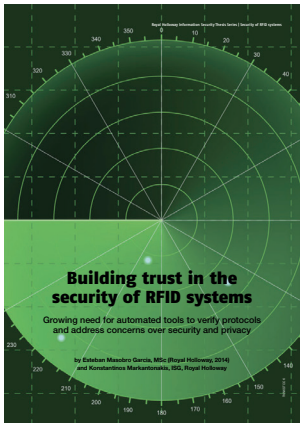
The project has six work packages covering

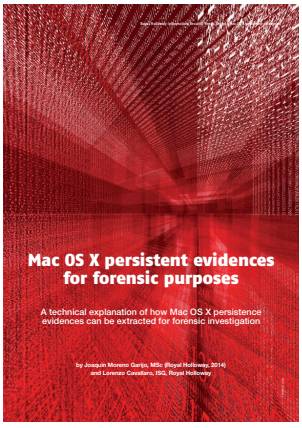
01 Modelling and monitoring cyber attacks;
02 Developing trust models for open distributed environments;
03 Identifying and modelling human behaviour in network communications;
04 Determining threat awareness, risk perception, adaptive behaviour and eCrime costs;
05 The cyber threat landscape and business confidence in the criminal justice system, and;
06 Developing a probabilistic framework combining the outcomes of the other five work packages.

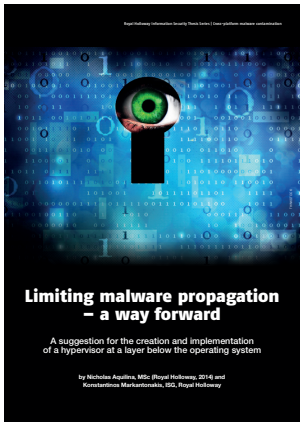
The outcomes to date include several research papers and a system to analyse log files from next generation firewalls for malware in networks, an analysis of Service Level Agreement models for the cloud computing eco-system, a survey of cyber security students regarding security behaviour and their personality profile, a business survey which is to be launched in June 2015, and an analysis of cybercrime convictions in the UK.

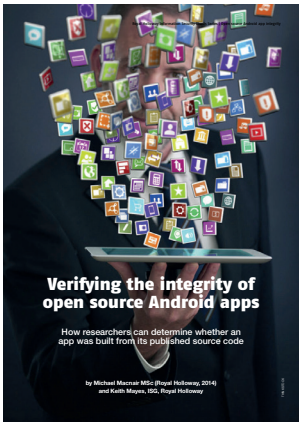


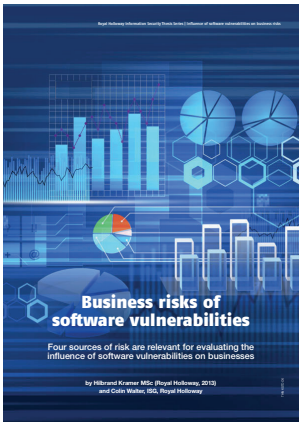
COMPUTER WEEKLY AWARDS

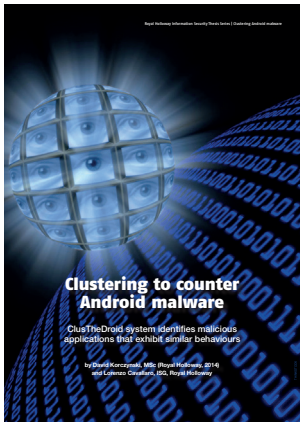












COMPUTER WEEKLY ROYAL HOLLOWAY INFORMATION SECURITY MSC THESIS SERIES

By Siaw-Lynn Ng

> Dr Siaw-Lynn Ng is a Senior Lecturer in the ISG

Founded in 1992, the ISG's flagship MSc Information Security programme has now produced over 3000 graduates from more than 100 countries in the world. The success of this MSc programme was recognised in 2014 when Royal Holloway became one of only four UK universities to gain full GCHQ certification of their Cyber Security Masters programmes.

One core part of the MSc programme is the MSc project, which is a major individual piece of work aimed at demonstrating an understanding of a specific area of information security. Because our students come from a range of different backgrounds, from new students seeking a foundation for a professional career in information security, through to experts in their subjects seeking to widen and deepen their knowledge of information security in general, the topics of our MSc projects are wide-ranging, from dealing with high-level subjects such as how to deal with insider threats, to detailed technical exposition such as forensic evidence in the Mac OS X operating system.

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

This year we have fourteen articles covering topics from risk assessment to automated malware analysis. These articles are distilled from the full project reports and necessarily omit many details. Readers interested in particular articles can obtain the full reports from the ISG website.

Cesar Augusto Bonilla Alvarez proposes a protocol for users to authenticate taxicabs in the street in the article "Authenticating taxicab services". The aim is to ensure the user's safety and to provide an assurance of quality of service. The scheme uses smart cards located on the taxicabs and users' NFC-enabled devices.

In "Adversary modelling: evaluating the feasibility of a symbolic adversary model on smart transport ticketing systems" by Sheung Chi Chan, formal symbolic adversary modelling approaches are analysed and a new approach is proposed in order to prove the security properties needed in this contactless communication environment.

In "Building trust in the security and privacy of RFID systems" Esteban Masobro Garcia looks at automated tools that can formally verify the security and privacy level provided by RFID protocols and suggests a number of improvements to better capture the requirements of security protocols for low-cost RFID tags.

In "Verifying the integrity of open source Android apps" Michael Macnair introduces AppIntegrity, a service that enables researchers to verify that each version of an app that is published on the Play Store was actually built from its published source code.

In "The Android Labyrinth: combating application repackaging attacks", Rowena Harrison investigates the effectiveness of obfuscation tools against Android apps repackaging: legitimate applications are reverse engineered, modified to include malicious code, repackaged, and then distributed on app stores for download.

The article "Current trends in packing and obfuscation: how they fit into today's landscape of advanced persistent threat and cyber crime as a service" by Paul Moon examines the use of these tools in modern malware and what measures can be taken as defence.

In "Cross-platform malware contamination: limiting malware propagation - a way forward", Nicholas Aquilina puts forward a suggestion for the creation and implementation of a hypervisor at a layer below the operating system to monitor and intercept malware.

As the volume of new malware grows, we need automated tools for detecting new malware. In "ClusTheDroid: clustering Android malware", David Korczynski presents a system for clustering Android malware that exhibit similar behaviours.

Attacks from intruders and malware on Mac OS X have also increased during the past few years. In "Mac OS X persistent evidences for forensics purposes", Joaquin Moreno Garijo gives an explanation of Mac OS X persistence forensics evidences and develops an open source tool to extract these evidences.

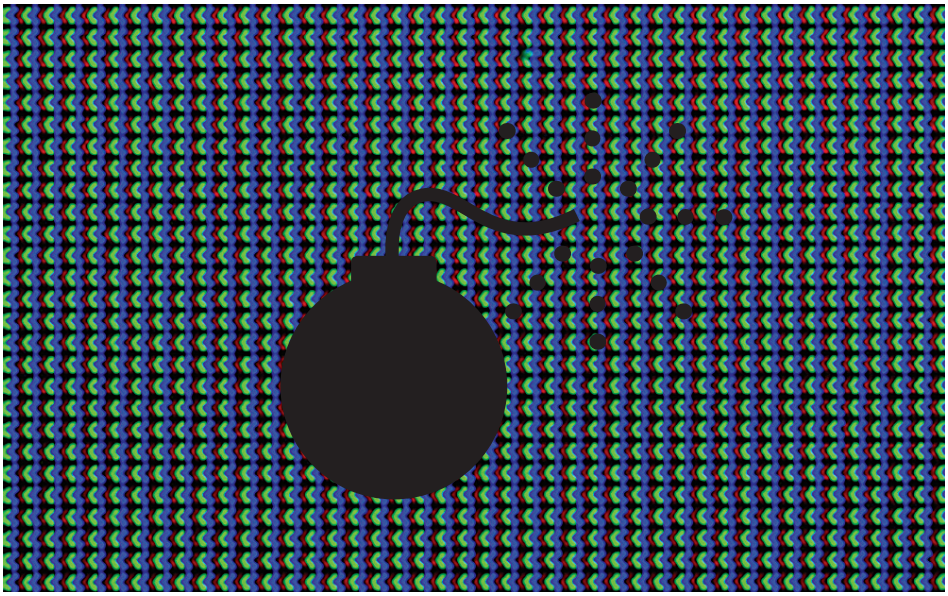
With the rise of online shopping, retail supply chains are seeing an increasing pressure to maintain high availability of products and fast deliveries while keeping prices low. Distribution centres lie at the heart of this, and the article "Information Security at the heart of the retail supply chain" by Katherine Woods discusses particular challenges to secure the retail supply chain and how they may be overcome.

"The value of threat modelling" by Timothy D. Williams gives an overview of the value of threat modelling and describes some common modelling techniques. These techniques enable better understanding of the underlying causes of risks and allow more effective risk management solutions.

Software vulnerabilities are often stated in rather technical language. In "The influence of software vulnerabilities on business risks: four sources of risk relevant for evaluating the influence of software vulnerabilities on business risks", Hilbrand Kramer presents the development of a method that management can use to understand and prioritise software vulnerabilities.

Another hard problem in information security is the insider threat, which eludes many traditional and advanced defences. The article "Mitigating cyber threat from malicious insiders" by Jason Anthony Smith looks at an insider attack as a sequence of phases and proposes a practical 10-step programme for mitigating malicious insider threat.

In "Analysis of the Linux Audit System" by Bruno Morisson, the mechanism by which the Linux operating system keeps track of events was also analysed and found to be wanting.



CYBER WEAPONS DON'T GO BOOM
By Andreas Haggman

> Andreas Haggman is a student in the EPSRC Centre for Doctoral Training in Cyber Security

In recent years, cyber weapons have shot to the top of the agenda of military planners, policy makers and academics alike. While previous incidents and operations hinted at the potential for using cyber to wage war, it was the discovery of Stuxnet in 2010 that really revealed the power of the digital domain.

Stuxnet was ground-breaking in that it crossed the boundary between the digital and analogue worlds – it was a piece of weaponised computer code which directly caused real-world physical damage. Stuxnet stealthily infiltrated a secure Iranian nuclear facility at Natanz, bypassing a range of physical and logical defences, and infected the Programmable Logic Controllers in systems that controlled spinning centrifuges. It then overrode built-in safety parameters to instruct the centrifuges to spin at rates which caused them to crack, thereby rendering them inoperable. All this was achieved while remaining undiscovered, a feat made possible by feeding false information to the safety monitoring systems, making it look like everything was normal. Whoever created Stuxnet (the evidence points to a joint United States-Israel effort, but neither have accepted responsibility) would have initially had to conduct a comprehensive and detailed survey of the facility's physical and logical systems in order to find vulnerabilities which Stuxnet could exploit. In short, Stuxnet was a complex and impressive endeavour.

It is perhaps little wonder, then, that Stuxnet is so endearing to military planners. In a world dominated by boys clamouring for fancy toys, Stuxnet represents a next-generation "must-have". Stuxnet is a Robosapien in a world of Furbees, a Bugatti Veyron in a world of Ford Fiestas, an AES algorithm in a world of Caesar ciphers. But this insatiable lust for the latest and greatest is only a superficial explanation of the allure of cyber weapons. Returning to Stuxnet's capabilities, as outlined above, reveals a more nuanced understanding of why the military is investing so heavily in cyber weapons. It is not the actual destructive capabilities of cyber weapons – indeed, the evidence provided by Stuxnet suggests that this is limited – but instead their immense capacity for stealth. Stuxnet bypassed defences and carried out its mission undetected and, crucially, was not attributable to an actor. Unlike, say, a cruise missile or fighter jet, Stuxnet had no traceable trajectory, no identifiable (or at least verifiable) point of origin. Such capacity for stealth makes cyber weapons attractive in two respects.

Firstly, from a warfare planning perspective, stealth is desirable because it helps maintain the element of surprise. If the enemy does not know an attack is imminent, or does not know what kind of attack will be used, they will not know what to defend against, thereby ceding the momentum to the attacker who is able to manoeuvre and strike at will. Secondly, the difficulty of attributing cyber attacks endows the attacker with a veil of anonymity. In operating under an anonymous shroud, states can conduct warlike operations without paying incumbent political costs such as declaring war, garnering support from the civilian populace, or in any way justifying their actions.

The theoretical attraction of military planners to cyber weapons is readily apparent and reasonably well-documented. What remains a point of contention, however, is the actual utility of cyber weapons in warfare. Limited empirical examples (Stuxnet is the only one of its kind) renders it difficult to make a judgement about the applicability of cyber weapons to combat and modern war. It shall below be posited that this is an area of study which has so far eluded significant analysis, yet is central to how war is conducted, and which could potentially place severe limitations on the utility of cyber weapons.

War is not merely about destroying the enemy. In Clausewitz's immortal words, "war is an act of violence to compel our opponent to fulfil our will." Influencing and convincing the enemy into acting as you wish is clearly a central component of war, but although Clausewitz talks about acts of violence, such acts alone are insufficient to compel. More often, it is intimidation and threats which incite certain behaviour. Indeed, the entire strategy of nuclear deterrence is based on not actually deploying nuclear weapons, but instead waving them around like some kind of apocalyptic menace.

This is where the stealth capacities of cyber weapons potentially begin to limit their utility. How does one wave around a cyber weapon without actually using it against an adversary? Cyber weapons do not come packaged in rocket-shaped hulls to be paraded on Red Square, nor can they be detonated on some remote Pacific atoll to demonstrate their awesome power. On a more tactical level, how does one influence or convince the enemy without the sights and sounds of war? In combat, an M16 rifle probably looks a lot more intimidating or reassuring (depending on which end of the gun one is standing) than some imaginary, and hypothetical, ones and zeroes zipping about in cyberspace. It seems that, at some level, cyber weapons are incompatible with the enduring nature of war.

The obvious antithesis to this is to consider them as tools of information or psychological warfare. Imagine, for example, an aerial bombing raid or missile attack on any modern capital city. The inhabitants immediately seek shelter in the city's underground rail stations. The attacker then uses a cyber weapon to take control of every station's tannoy system and uses it to broadcast political messages, or to play some particularly menacing music. Wagner's Flight of the Valkyries would be a tried and tested choice for psychological warfare. Cyber weapons might not by themselves be loud and brash, but they can seize control of things that are. Research into such uses of cyber weapons appears conspicuously absent, at least in the academic literature.
This seems a shame, for though Stuxnet opened many eyes to the possibilities of cyber warfare, the fascination with Stuxnet itself may have restricted thought and imagination. The stealth value of cyber weapons has been seized upon as their greatest asset, yet their silence and invisibility may well be counterproductive to the goals of war. Non-kinetic applications of cyber weapons must surely be considered as a significant area of use and this is something which deserves further close study.

Just because cyber weapons don't go "boom" doesn't mean they have to be silent. There are (many frightening) possibilities for cyber weapons beyond Stuxnet, and analysts and planners should think beyond this single tool when musing about how such weapons could be constructed and deployed.

FROM EGGS TO PONIES – A LESSON FROM THE STORY OF BOTS

By John Austen

> John Austen is a Visiting Lecturer in the ISG

In December 1993, with respect to Internet Relay Chat, Robey Pointer was developing applications that were trying to protect channels that had been disrupted. His successes, unwittingly, was the starting point for what turned out to be one of the scourges of the technology age.

IRC started in 1988 and, as a forerunner of social media, provided discussion forums for those who joined. While most discussion groups formed around genuinely constructive interests (at the time these were mostly of a technical nature), there were some formed by people out to cause trouble. By 1993 some of these "mischief makers" were taking over the channels, mostly using a technique known as "net splitting", which resulted in the so-called IRC Wars.

This was not the first time that mistrust, jealousy and a gang-like culture had disrupted network services. In the late 1970s the "phone-phreakers", forerunners of computer hackers, started their own wars. "Wars" is probably an inappropriate term as there was no physical violence, but merely the blocking of communications in their own forums and networks. Cyber criminals work remotely, most often alone in their own space, but have always needed forums and discussions groups to generate and pass on ideas and targets safe in the knowledge that they can maintain anonymity. The early 1980s "phone-phreaker wars", most notably between the so-called Legion of Doom and the Masters of Deception were followed by the formation of hacking groups who started their forums known as bulletin boards and which had fanciful names such as The Pirates Chest. It wasn't long before they started to fall out and technically invade and block each other's communication space.

The result of Robey's work in 1993 was to produce a software application that could link users together whilst keeping IRC channels free. These applications were called "web robots" (better known as "bots") which were able to run automated tasks over the Internet in a simple, structurally repetitive and higher rate than it would be possible for a human alone. When these IRC bots were linked they became their own network (a "botnet") which could be controlled from a single server. This server was known as the "master" and the bots were referred to as "slaves". This innovative idea was called the Eggdrop Bot, based on the analogy of being able to drop an egg (a network) without breaking it.

This turned out to be one of those developments that had the best of intentions, and indeed worked, but had unpredicted negative consequences. Some of the "troublemakers" whose activities had provoked the design of the Eggdrop Bot in the first place started a process to use it for their own ends.

Botnets really caught on in the world of cybercrime and the first major group to realise the potential of a botnet were the spammers. Spam was originally known as direct marketing or direct mailing. In itself, of course, this activity is not necessarily illegal (after all, Royal Holloway was built in the late 19th century from the proceeds of direct mailing of cure-all pills, so perhaps one should not demonise it too much!) After a first (minor) appearance on Arpanet in 1978, by 1994 internet spam was escalating. The late 1990s saw the introduction of Spambots which, at that time, just gathered information from Usenet forums but were not used as the delivery mechanism for the messages. This was soon followed by fully-fledged spam botnets, which had huge delivery systems. For example, by 2004 the Bagle botnet had 230,000 hosts and could deliver 5.7 billion messages per day. By 2009 this one botnet was responsible for 10% of spam sent around the world. Ordinary users, suffering from plagues of unwanted messages, might well ask how this volume of traffic could happen. The answer of course revolves around the issue of infectious bots, which are delivered in several ways to home computers, the favourite today being the "drive-by-download" (the unwitting infection of a machine by a bot at web-sites and other points of internet contact).

Botnets are the ultimate delivery system. They now launch spam, distributed denial-of-service attacks, adware, spyware, click fraud and other types of scams and exploits. They are easy to put together – it is a one-man job to put up a botnet, but it is a difficult and labour-intensive task to take one down. To give an example, in September 2011 the Microsoft Corporation (and others), armed with a court order, took down the Kelihos botnet (which at that time was delivering 4 billion messages a day), yet five months later it was resurrected and activating more bots that were on home systems that had caught infection from Facebook.

Naturally it was not long before organised crime saw the benefits of these networks. ZeroAccess and Zeus are examples of botnets that were specifically tweaked (or designed) to attack financial systems, and they have been successful. Organised crime now offers a variety of botnets to rent or hire by the day, month or year. In 2014 the Pony botnet was responsible for relieving digital wallet owners of around £200,000 of virtual currency in just three months.

Botnets are by no means the only well-intended idea that has been subsequently misused in this type of way. In 1995 at Purdue University, Dan Farmer and Vietse Venema developed one of the best vulnerability scanning tools ever seen. Their "Security Administrator Tool for Analysing Networks" soon became known as SATAN, living up to its name by becoming a primary breaking tool for the ever-growing band of computer hackers, even though its working life was relatively short-lived. We will undoubtedly see many different types of scams and exploits in the future. However, botnets provide a salutary lesson in the perils of developing technologies that might have unintended uses and consequences. I am not sure how we can stop this happening again, but it is something that security researchers and developers would be wise to keep in mind.

AN MSC INFORMATION SECURITY AT ROYAL HOLLOWAY: PASSPORT TO A WELL-PAID JOB

The ISG was founded to deliver its prestigious MSc Information Security in 1992, which now has over 3000 graduates throughout the world. From the outset the MSc Information Security aimed to provide not only a solid grounding in information security, but also to provide appropriately educated employees ready to take on challenging information security roles in both the private and public sector, industry and government.

There have always been jobs for well-trained information security specialists, all the more so in recent years when the term "cyber security" seems to feature almost daily in media headlines. There has also been much discussion of a "cyber security skills gap" and governments around the world have been encouraging universities to train more cyber security experts.

While this all bodes well for those considering a career in cyber security, the ISG has recently commenced an ongoing exercise to monitor employability of MSc Information Security students. We hope to use this information to continuously assess how we can best equip students for the cyber security workplace.

How well are we currently doing?

MSc Information Security graduate student information was analysed for the period 2005/6 to 2011/12. Here are the results.

Will students get a graduate-level job?

Yes! The analysis (see Figure 01) shows that Royal Holloway MSc Information Security students in graduate-level employment or higher study (as opposed to taking lower grade work or being unemployed) have not fallen below 90% over the period, were in fact 100% in two of these years, and have an average of roughly 97%. Note that Royal Holloway's university-wide aspiration is for 75% of its graduates to enter graduate-level employment or higher study.

How much are graduates earning?

The analysis (Figure 02) shows that Royal Holloway MSc Information Security students are commanding decent starting salaries. These are excellent results, especially considering how the world and its economy were changing over the eight year period.

Looking to the future

While these employability and salary statistics are impressive, the ISG is committed to remaining "ahead of the game" and preparing its graduates as effectively as possible for an exciting cyber security career. Here are some of the recent initiatives to make sure that future Royal Holloway MSc Information Security graduates continue to get quality jobs.

MSc Information Security with Year in Industry

Many MSc Information Security students currently engage with short work placements and internships during the MSc project by means of various ad-hoc arrangements ranging from a week or two unpaid placement to a longer paid stay with a host organisation. These activities will certainly continue. However both employers and students have been asking us about longer, more meaningful opportunities to connect students to potential employers.

We are thus delighted to launch (from 2015) the MSc Information Security with Year in Industry. This is a two-year version of the MSc Information Security, with the student industry-year commencing after the May exams and the student returning the following year to complete the MSc project. Placements are subject to performance on the taught programme and not guaranteed, but the ISG will assist students in finding host organisations.

For further details of this new programme, please see https: //www.royalholloway.ac.uk/isg/prospectivestudents/prospectivestudents-msc/mscininformationsecurityyearinindustry.aspx

Royal Holloway Passport Scheme

As well as the formal taught component of the MSc Information Security, the ISG offers students many opportunities to engage in work, training and responsibility-related extra-curricular activities. Activities beyond the basic call of an educational programme are highly valued by employers. The Royal Holloway Passport Scheme allows these activities to be documented and awarded points towards a Royal Holloway Passport Award.

External Syllabus Review

The ISG has just completed the latest External Syllabus Review of its MSc Information Security programme. This periodic audit involves a number of reviewers from industry and government conducting a thorough review of the current syllabus to ensure that it remains relevant for future graduates. This information feeds into our constant revision of the syllabus and provides assurance that a degree in MSc Information Security from Royal Holloway remains a highly respected award, and one with a good job at the end. This has also been emphasised by the recent GCHQ Full Certification of the Royal Holloway MSc Information Security.

Figure 01
The % of ISG MSc Graduates in Graduate Level Work

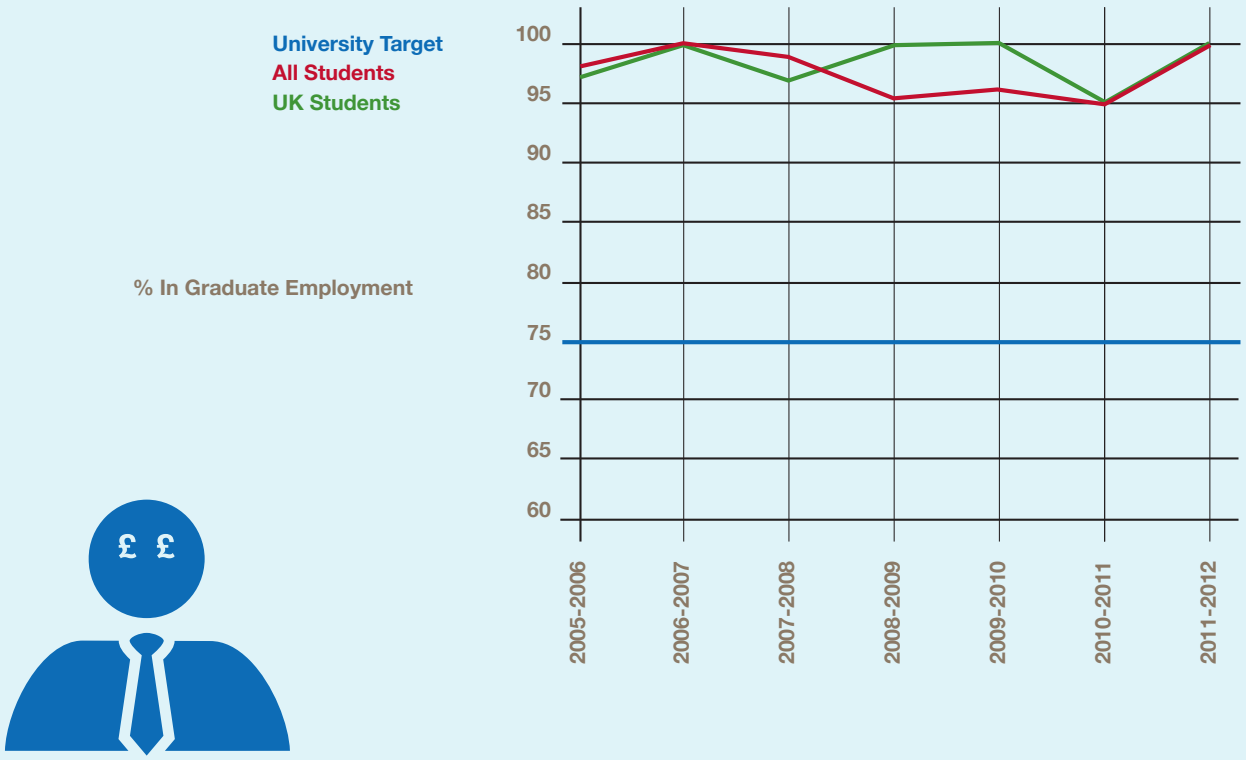
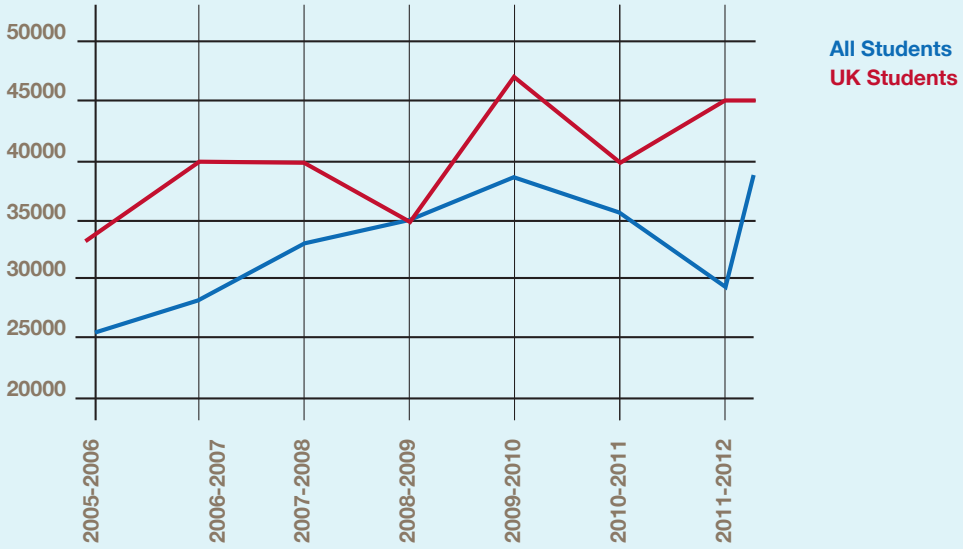


Figure 02
Median Salary for ISG MSc Graduates (UK £s)



CENTRE FOR DOCTORAL TRAINING UPDATE
By Carlos Cid

> Prof. Carlos Cid is Director of the EPSRC Centre for Doctoral Training in Cyber Security

The Centre for Doctoral Training (CDT) has just entered the third year since its launch in April 2013 and, despite its early age, we are delighted with its progress and to have so much exciting news to report.

The CDT currently has 19 students, divided into two cohorts. We have recruited students with a wide range of backgrounds and interests, making the cohorts particularly suitable to the multidisciplinary nature of the CDT. We are now recruiting for the third cohort, to start in October 2015. We expect that 12 new students will be joining the CDT later this year and we look forward to their arrival.

Students from the first cohort are now well into their second year of studies, and moving full steam ahead with their PhD research. They are producing interesting research output, with some already resulting in academic publications. Many are also looking forward to starting their industrial placements later this year. The second cohort has just concluded most of their first year of training, and students are now busy organising their summer projects.

The ISG has always placed strong emphasis on external engagement throughout its education and research programmes. Our external links have only strengthened with the launch of the CDT two years ago. In our original bid, we received the support and commitment from over 30 organisations from across the cyber security sector, to be involved in the CDT training and research programme; several new ones have since joined the list. CDT students are able to get a strong 'background' exposure to industry through various CDT activities. The growth in our industrial links – both in numbers and quality – is certainly a highlight from these first two years, one that brings many benefits not only to the CDT, but also to the ISG as a whole.

CDT NEWS

Andreas Haggman, first-year PHD student with the CDT, has been awarded 1st place in the International Institute for Strategic Studies 2015 Student Essay Competition on International Cyber Security with his entry 'The Dangerous Rhetoric of Cyber Deterrence'.

"I am delighted and honoured to be recognised in this way by such a prestigious institution," Andreas says. "This is a fantastic opportunity to not only get my work out in the public domain, potentially read by HM Government, but also to participate personally in the proliferating internationalcyber security debate."

The International Institute for Strategic Studies (IISS) is a world-leading authority on global security, political risk and military conflict. It was founded in the UK in 1958 with a focus on nuclear deterrence and arms control. Today, it is also renowned for its annual Military Balance assessments of countries' armed forces and for its high-powered security summits, including the Shari-La Dialogue.

For winning the essay competition, Andreas has received a cash prize and has been invited to join IISS's Academic Network in support of Her Majesty's Government on International cyber security policy.

Professor Klaus Dodds, Royal Holloway's research theme champion for security and sustainability, noted, "It is a tribute to Andreas and colleagues that such recognition has been secured, and is indicative of the kind of students being attracted to the CDT in Cyber Security in the first place."

Professor Keith Martin, Director of the Information Security Group, commented, "Andreas is one of three CDT students jointly supervised by the Department of Geography and the Information Security Group, and I am delighted that the resulting cross-disciplinary environment is fostering talented researchers who can make meaningful contributions to debates of contemporary significance.

Second year CDT student Dusan Repel won the 'best elevator pitch' competition at the Third Annual Conference for the Academic Centres of Excellence in Cyber Security Research. Dusan spoke about his work on malware analysis and saw off competition from students from each of the other ten UK Centres of Excellence. The conference itself brought together academic, industry and government representatives to discuss a number of themes, mainly based around exploitation of academic research and innovation. This is the second time in three years that a Royal Holloway student has won this prize.

A team of second-year CDT students won second prize in the "Universally Challenged" university cipher competition, organised by Cyber Security Challenge UK. This event saw teams from universities across the country pit their skills against each other before a judging panel of industry experts from BSides London, CERT-UK and GCHQ.

Teams were tasked to create a complex challenge cipher, which was then shared with the other teams to test their skills against. They were then challenged to break as many of the other ciphers as possible before the competition ended.

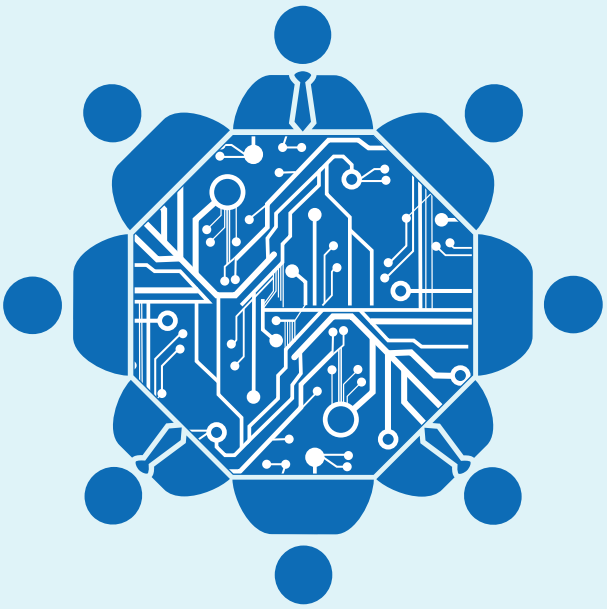
'Alice in Cyberland', the team from Royal Holloway, was officially announced as winning second prize at a ceremony in London in front of an audience of the UK's top cyber security experts. Dusan Repel, from the Alice in Cyberland team said, "It was a really enjoyable and fulfilling task to design a challenging puzzle that interviewed program analysis and cryptography. It was an honour to have been part of the team".

CDT EXTERNAL ACTIVITIES

External engagement is a key component of the CDT programme. As part of the first-year CDT training, we run a number of external engagement sessions in order to expose the CDT students to perspectives from different sectors of the cyber security industry.

In January 2015 we visited the Transport Research Laboratory to learn about the cyber security challenges being faced through increased automation in future road systems. These included issues concerning driverless cars and battery charging. In February we visited Intel Security (McAfee) to get a better understanding of how malware is developing and how alerts are managed. In March we visited KPMG to experience the life of a cyber security consultant. The CDT students were set a number of complex challenges and had to present their findings to the boardroom – glad to report that none of the students were fired!

We have also hosted several sessions at Royal Holloway. The National Crime Agency presented their view of the cybercrime landscape and tasked the students with addressing several of the ongoing challenges that the NCA faces during a set of lively discussions. Adeptica explained the complex cryptography behind smart metering during an engaging workshop which required students to apply their cryptography knowledge in a real world setting. A team from L-3 TRL ran a very interesting hands-on workshop in March, when students got some firsthand experience of key management in high graded cryptographic equipment. Finally, CDT students also spent two days with a former Radio 4 producer developing cyber security awareness podcasts.



THE EXPERIENCE OF A CDT STUDENT

Naomi Farley
Second-year CDT student

After a great first year of exploring a variety of topics within the area of cyber security, the second-year CDT cohort have now decided on their individual topics of interest and have started to carry out research into these full-time. Examples of research topics include access control, applied cryptography, malicious software and cyber warfare. Students are now busy working on articles to submit to journals or conferences (with some having papers accepted in the past year). We have also been able to attend academic events to both present our own work, and to keep up-to-date with new research in the field. As summer draws closer, several members of the second-year cohort will soon be commencing summer internships in various companies, such as HP Labs and Mozilla Foundation, whilst others will be looking to start similar internships in the near future.

Although we have started to specialise in our own areas in cyber security, we have been fortunate enough to still be able to participate in the external engagement sessions with the first year CDT cohort, such as a recent visit to Intel Security, as well as workshops held at the university. A recent industrial session run by L-3 TRL Technology, for example, enabled us to get hands-on with ECM equipment and learn more about the valuable research that the company does.

Despite the change in focus for second year CDT students, informal discussions and weekly PhD seminars allow both cohorts to learn about the research interests of individual students within each cohort and to keep up-to-date with research that is being carried out within the CDT.

SHORT NEWS BITES

ISG HOSTS AFCEA CYBER WAR DINNER AT ROYAL HOLLOWAY

The Information Security Group was delighted to host the London Chapter of the Armed Forces Communications and Electronic Group (AFCEA) for a black-tie Cyber Dinner in Royal Holloway's Picture Gallery on 15th April 2015. Prof. Thomas Rid from the Department of War Studies at King's College London gave a keynote talk in front of an invited audience on the subject of cyber war. His address was in response to three short challenges, delivered between the courses, targeted at the title of his book, "Cyber War will not take place".
These challenges were presented by Gp Capt. Andy Gudgeon (President of AFCEA London), Dr Alasdair Pinkerton (Dept. of Geography) and Capt. Mike Hawthorne (Vice President of AFCEA London and current Royal Holloway MSc Information Security student). Organiser Chris Yorke was delighted with proceedings and expressed his sincere thanks to Royal Holloway's catering team for "the quality of food and service in a stunning environment". It was a most enjoyable evening and Prof. Rid, who regularly presents at events of this type, expressed his humility at addressing such a prestigious audience of cyber security experts from the military, government and commercial sectors.

ISG RESEARCH ON FREAK ATTACK HITS THE HEADLINES

The work of ISG researchers Martin Albrecht, Kenny Paterson, Davide Papini and Ricardo Villaneuva-Polanca has been making headlines in the tech press in March. In the wake of the FREAK attack on TLS, the ISG team scanned the internet for servers offering export-grade RSA keys. These 512-bit RSA keys were a crucial component in the FREAK attack. The team made three discoveries:

- The number of servers offering these 512-bit RSA keys has declined very rapidly - from around 25% down to 10% in just a week.
- But the same RSA key is sometimes used by many different devices, more than 28,000 in the worst case. Since a 512-bit modulus can be factored for about $100 on a commercial cloud computing service, this reuse of keys makes the amortised cost of breaking the traffic for each device very low.
- 90 out of the 2.2 million 512-bit RSA keys that the ISG team collected were found to have non-trivial common prime factors with one another, making them trivial to break. Just 167 seconds of computation was needed on an 8-core system to identify and break these keys.

The work was picked up by Dan Goodin at Ars Technica and was then covered in The Register, PC World, Threatpost and more. Kenny Paterson, one of the team members said "This was a great 'Friday afternoon project' for us - we had just the right set of skills in the team to get it done quickly. We relied on great publicly available tools like zmap and fastgcd to do most of the hard work. We were pretty surprised by the results, and also by the extensive press coverage."

SSR 2014

The Information Security Group played host to another international research conference in December. The First International Conference on Security Standardisation Research (see the SSR 2014 webpage for further details, including copies of the presentations) was held on 16th and 17th December 2014 and attracted over 40 delegates from across the world to attend two full days of talks and a panel session, including two keynote talks from Charles Brookson and Marijke De Soete. The feedback from delegates was excellent. The proceedings of the conference were published in the Springer LNCS series.

CANADA-UK COLLOQUIUM ON CYBERSPACE

The Canada-UK colloquium is an annual event aiming to build up contacts between leading experts from both countries and contribute to the development of public policy in the UK and Canadian. The 2014 colloquium, which was held in November 2014 at the Fairmont Le Chateau Montebello Hotel in Quebec, set out to tackle The Challenges of Cyberspace: Living and Working in a Digital Society. Amongst a varied panel of politicians, academics, business leaders and civil libertarians, Prof. Keith Martin, Director of the ISG, and Pip Thornton from the EPSRC CDT in Cyber Security, were invited to join in the debate. After a briefing day in the parliament buildings in Ottawa, and a reception at the British High Commission, the UK delegation headed up the river to Montebello for the main two-day colloquium. Plenary sessions, with papers from delegates from each country, were held on The Challenges of Cyberspace, The Politics of Cyberspace and The Business of Cyberspace, as well as one on Cyber Risks and Cybersecurity. There then followed break-out sessions on Cyber and Privacy, Cyber and Social Media, Information Flows/ High Frequency Trading and Threats of the Balkanisation of the Internet/Cloud Computing.

A subsequently prepared written report on the group's findings will include recommendations to the UK and Canadian governments. "It was a real privilege to be invited as a post-graduate representative to such a high-profile event", said Pip. "The Colloquium covered some really important issues from some very diverse and sometimes conflicting angles, which I found fascinating. I also had the opportunity to meet some great people".

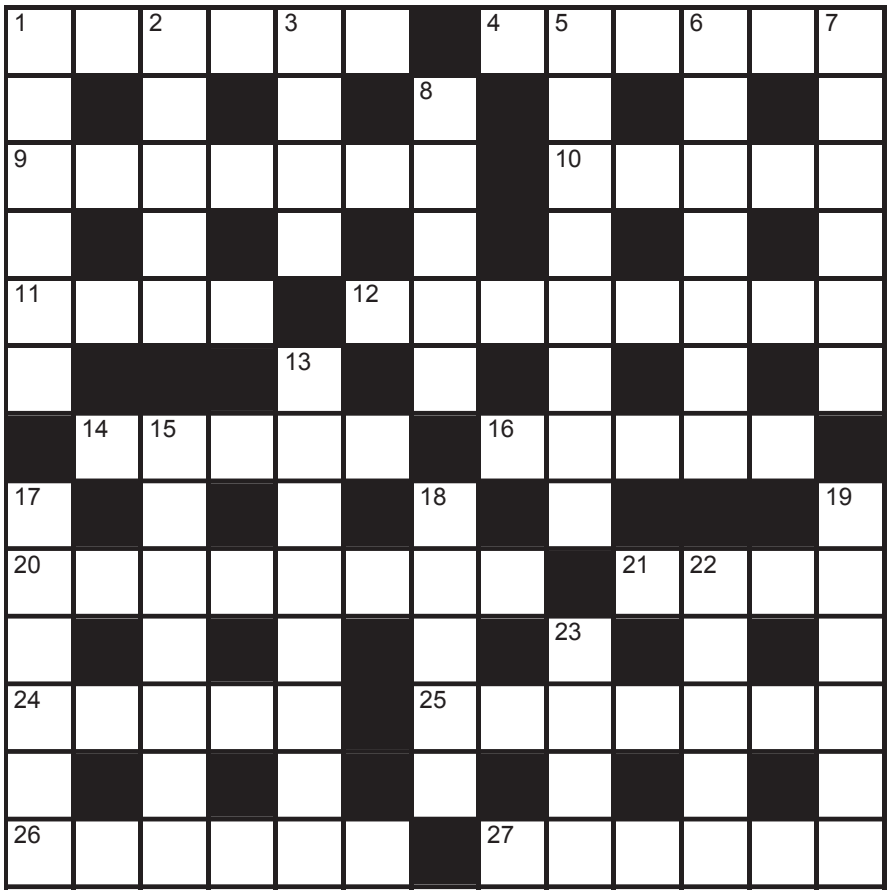
IMPACTING FUTURE PAYMENTS

The ISG has been carrying out a sequence of expert studies on payment authentication for the UK Cards Association. The association is the trade body for the card payments industry in the UK, representing financial institutions that act as card issuers and acquirers; and is also one of the sponsoring members of the ISG Smart Card Centre.

The studies have addressed attacks and countermeasures for current chip & PIN cards and the evolution of security protocols and technologies that will impact how we will all pay for things in future. The work has been led by Dr Kostas Markantonakis and the ISG expert team included Prof. Keith Martin, Prof. Keith Mayes, Prof. Fred Piper and Dr Geraint Price.

Dr Markantonakis commented: "We are really grateful for the support we receive from the UK Cards Association to encourage our research and so it is very gratifying when we can deliver something in return that could have significant impact on future payments in the UK." David Baker of the UK Cards Association said "The UK Cards Association is very pleased with the work carried out by the ISG. For us it is not only important to have access to the leading-edge expertise and experience, but also to work within a solution-oriented trusted relationship. We look forward to working with the ISG in the future."

CROSSWORD
By Skipjack



Clues are normal but solvers need to transform the answers to down clues before entering them into the grid. The answers in the top row provide a hint…

Across

1 Salad made with lettuce, Parmesan cheese and croutons (6)
4 A secret code (6)
9 Instrument for measuring angular distances (7)
10 Passage separating rows of seats (5)
11 Sudden blast of wind (4)
12 Chronic disease caused by deficiency of nicotinic acid (8)
14 Code of principles (5)
16 Forcibly remove (5)
20 Unaccompanied song in several parts (8)
21 Boastful bird? (4)
24 Painter famous for ballet scenes (5)
25 Evidence of disease (7)
26 Dissimilar (6)
27 Playground apparatus with a fulcrum (6)

Down

1 Comic actor of the silent era (6)
2 Criminal society originally from Sciliy (5)
3 Wading bird worshipped by the Egyptians (4)
5 Tranquility (8)
6 Vain bird? (7)
7 Computer infected with malware and controlled by third party (6)
8 44th US President (5)
13 Small Chinese oranges (8)
15 Go on strike (4,3)
17 Belonging to the people (6)
18 Nobel prize-winning English physicist (5)
19 Free from danger (6)
22 Striped animal (5)
23 Largest island in Micronesia (4)

RECENTLY COMPLETED PHD THESES & OTHER NEWS

Jean Paul Degabriele
Authenticated Encryption in Theory and Practice

Nadhem Alfardan
On the Design and Implementation of Secure Network Protocols

Eduarda Freire
Non-interactive Key Exchange and key Assignment Schemes

Robert Fitzpatrick
Some Algorithms for Learning with Errors

Christian Bonnici
On the Design of Legally and Ethically Effective Consent Management Schemes

Muhammad Saeed
Authentication Issues in Near Field Communication and RFIDDesign and Analysis of Security Ceremonies

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@royalholloway.ac.uk
W: www.royalholloway.ac.uk/isg