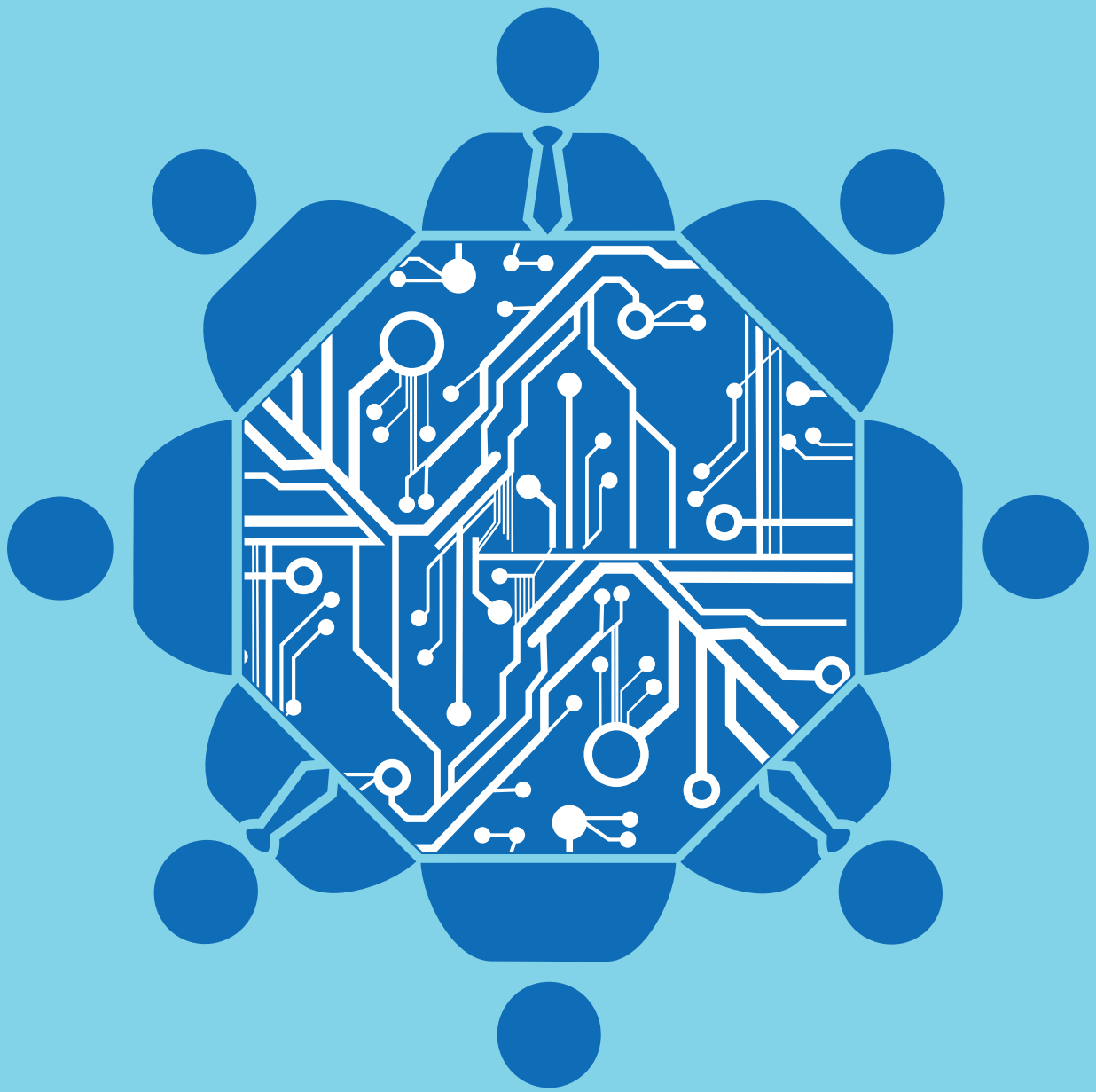
Information Security Group

Review 12/13

ACADEMIC CENTRE OF EXCELLENCE – CYBER SECURITY RESEARCH



Royal Holloway University of London

LETTER FROM THE ISG DIRECTOR

Welcome to our annual review of activities of the Information Security Group at Royal Holloway, University of London.

It has been a very exciting year to be an academic research group in the area of cyber security since there have been many opportunities to embrace as part of the UK's Cyber Security Budget filtered down to support academic research.

Perhaps most fundamentally, Royal Holloway was recognised as one of the first eight institutions to be awarded the status of Academic Centre of Excellence in Cyber Security Research (ACE-CSR). This award came about after careful scrutiny by an expert panel of our research activities, both in terms of depth, breadth and future plans. As the first institution in the UK to develop a dedicated research centre in this area we would have been horrified not to have achieved this award, yet it was still gratifying to have the quality of our research formally recognised.

There have also been several research calls dedicated to cyber security research from which we have successfully obtained significant research funding. The CySeCa project forms part of the Research Institute in Science of Cyber Security and you can read more about the project in this newsletter. We were also successful in bidding to host a Centre for Doctoral Training in Cyber Security Research. This £4M award will fund 30 PhD scholarships and represents an entirely new approach to PhD training, which we are extremely excited about. The newsletter contains further details, as well as a call for applications - if you know talented people seeking to develop a career in cyber security research then please draw their attention to this.

The past year has also seen the launch of Prof. Dusko Pavlovic's Adaptive Security and Economics Laboratory (ASECOLab). As well as big ideas, ASECOLab also houses the most comfortable sofa in the ISG, so it is well worth learning more about their plans in order to get yourself an invitation to come and sit on it!

Elsewhere in the newsletter you can read about new security standards for cloud security, the launch of a new open access Coursera course on malicious software, meet some of our staff, and learn more about some of our highlights from last year. Don't hesitate to get in touch if you want more details, wish to study with us, or seek to explore opportunities for working together.

Professor Keith Martin

INDEX

ACADEMIC CENTRES OF EXCELLENCE IN CYBER SECURITY RESEARCH

By Jason Crampton & Keith Martin

> Prof. Jason Crampton is ISG Director of Research
> Prof. Keith Martin is Director of the ISG

The quality of the Information Security Group's research in cyber security was officially acknowledged by GCHQ and EPSRC when Royal Holloway was awarded the status of Academic Centre of Excellence in Cyber Security Research (ACE-CSR). We are one of only eight higher education institutions in the UK to receive such recognition in the first round, although additional institutions will receive accreditation this year. ACE-CSR accreditation is based on several indicators of research strength and breadth, including research strategy, number of active researchers, scope and quality of research work, health of PhD graduate school, extent of research funding, and research environment.

Of course it was not a surprise that the research activities of the ISG made the grade in this assessment exercise, but it is nonetheless pleasing to have this formally recognised at a national level. We already regarded ourselves as a centre of excellence – it's just good to hear that some other folks agree!

The real question is: does obtaining the ACE-CSR "badge" really make a difference? The jury is out over the long term, but for now it really does matter. One of the intentions behind the ACE-CSR scheme is to identify research capability in cyber security in the UK, thus allowing money and other resources to be directed to those universities that have been able to demonstrate genuine expertise in this area. We have already seen the benefits of this, with a number of funding opportunities open only to ACE-CSR institutions, including some PhD studentships funded by GCHQ. We have also seen a closer working relationship forming between GCHQ and the ACE-CSR institutions, which will be to the good of both parties. We expect ACE-CSR status to strengthen our links with industry and, crucially, help us to obtain insights into the critical cyber security problems facing modern businesses.

Another benefit of the ACE-CSR branding is the plans to encourage meetings with and collaborations between ACEs. The inaugural ACE-CSR conference, attended by several representatives of each ACE, was held at Cheltenham in November. We were delighted that Royal Holloway's Nadhem Alfardan scooped the prize for best "elevator pitch" to a panel of government and industry judges on the subject of his recent research on the (in) security of the DTLS protocol. Further meetings of the ACEs are expected at Imperial in June and Royal Holloway in September.

The ACE-CSR scheme will provide ongoing validation of the quality of an institution's research in cyber security, with re-evaluation expected every five years. As long as the government runs the ACE-CSR scheme, we will make sure that Royal Holloway more than meets the necessary qualifying criteria.

GCHQ

EPSRC
Engineering and Physical Sciences Research Council

CENTRE FOR DOCTORAL TRAINING IN CYBER SECURITY

We were delighted to learn that Royal Holloway will host a new EPSRC Centre for Doctoral Training (CDT) in Cyber Security Research. The ISG-led bid for a research training grant of just under £4M will create funding for ten PhD scholarships in each of three annual intakes in 2013, 2014 and 2015. Two CDT grants were awarded nationally, one to Royal Holloway and one to Oxford University. The intention behind these awards is to boost the number of PhD graduates with skills relevant to the national need for cyber security expertise at all levels. James Quinault, Director of the Government's Office of Cyber Security, said "I am very pleased that Royal Holloway's strengths in this area have been deservedly recognised; we look forward to working with them to build the numbers of UK graduates working at the cutting edge in this field."

The ISG already has a healthy doctoral training programme, with around 40 PhD researchers studying at any given period. However, a CDT is "game-changing" in the sense that each intake of new students is regarded as a "cohort". They will attend one year of courses in advance of their three-year research programme, and will experience varied industrial placements during their studies. The intention is that PhD graduates have a well-rounded education in cyber security, as well as develop specialist skills in a research area of practical relevance.

As Alex Hulkes from the EPSRC explains, "The doctoral training that EPSRC funds should have the student at its heart. CDTs are an excellent way of ensuring this is the case as they provide students with a stimulating environment and a broader training than is often found in more traditional models of a PhD. When combined with excellent research this enhances graduates' employability no matter what their final destination. In particular, the inherently collegiate experience which comes from a CDT's cohort approach is of great value in any future career, whether research-based or not, as it reflects the realities of the modern workplace."

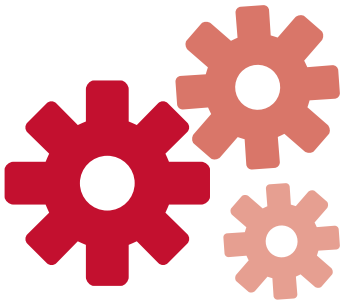
One of the most exciting aspects of the CDT award is that it integrates industrial engagement throughout the programme. The ISG is delighted to have the backing of around 30 organisations from across the cyber security sector, including IBM, McAfee, Thales, Vodafone, UK Payments, TfL and Logica. Igor Muttik, Principal Research Architect of McAfee Labs, is one of the cyber security research experts that the CDT will be developing projects alongside. He says: "We are at a point at which the explosive growth of computer technologies has resulted in a worrying increase in cyber attacks against individuals, companies, and governments. McAfee is extremely excited to join forces with Royal Holloway in fostering a cohort of new security warriors whose job will be to protect the global computing ecosystem of tomorrow."

Another unique aspect of CDT research training is that the projects funded through the CDT should be strategically chosen to cover the broad range of research areas related to cyber security. To assist with this strategic assignment of projects, the CDT has an advisory panel consisting of research leaders in both the UK and overseas. Prof. David Basin, Chair of Information Security at ETH Zurich is one of the panellists: "Cyber Security has become a central concern for governments and industry. This planned Centre represents a remarkable opportunity for faculty, doctoral students, and industry partners alike to join forces and work on different aspects of this problem. I look forward to sharing experiences, having run a similar centre here in Zurich for many years."

Prof. Keith Martin, Director of the ISG, is thrilled that Royal Holloway was successful in bidding to host a CDT in Cyber Security: "Royal Holloway has operated a graduate school in cyber security for many years and, although we feel that this is an area where we have an excellent track record, a CDT represents a significantly different approach to research training and we are really looking forward to engaging with it. With this award also comes a great responsibility to deliver the PhD graduates in a manner that benefits from the CDT cohort approach."

The Cyber Security CDT at Royal Holloway will be led by Dr Carlos Cid: "We are obviously delighted that our bid to host one of the Centres for Doctoral Training in Cyber Security was successful. One of the goals of the CDT is to contribute to the pool of UK-based doctoral-level cyber security experts, and we are aiming to recruit and train some of the most promising students to work in this field. We are looking forward to working with our industrial and academic partners to deliver training and research of the highest quality to the CDT students."

Royal Holloway's CDT in Cyber Security is recruiting now, so please pass on the word and encourage suitable candidates to get in touch with us.



ROYAL HOLLOWAY LAUNCHES RESEARCH THEME IN SECURITY AND SUSTAINABILITY

By Klaus Dodds

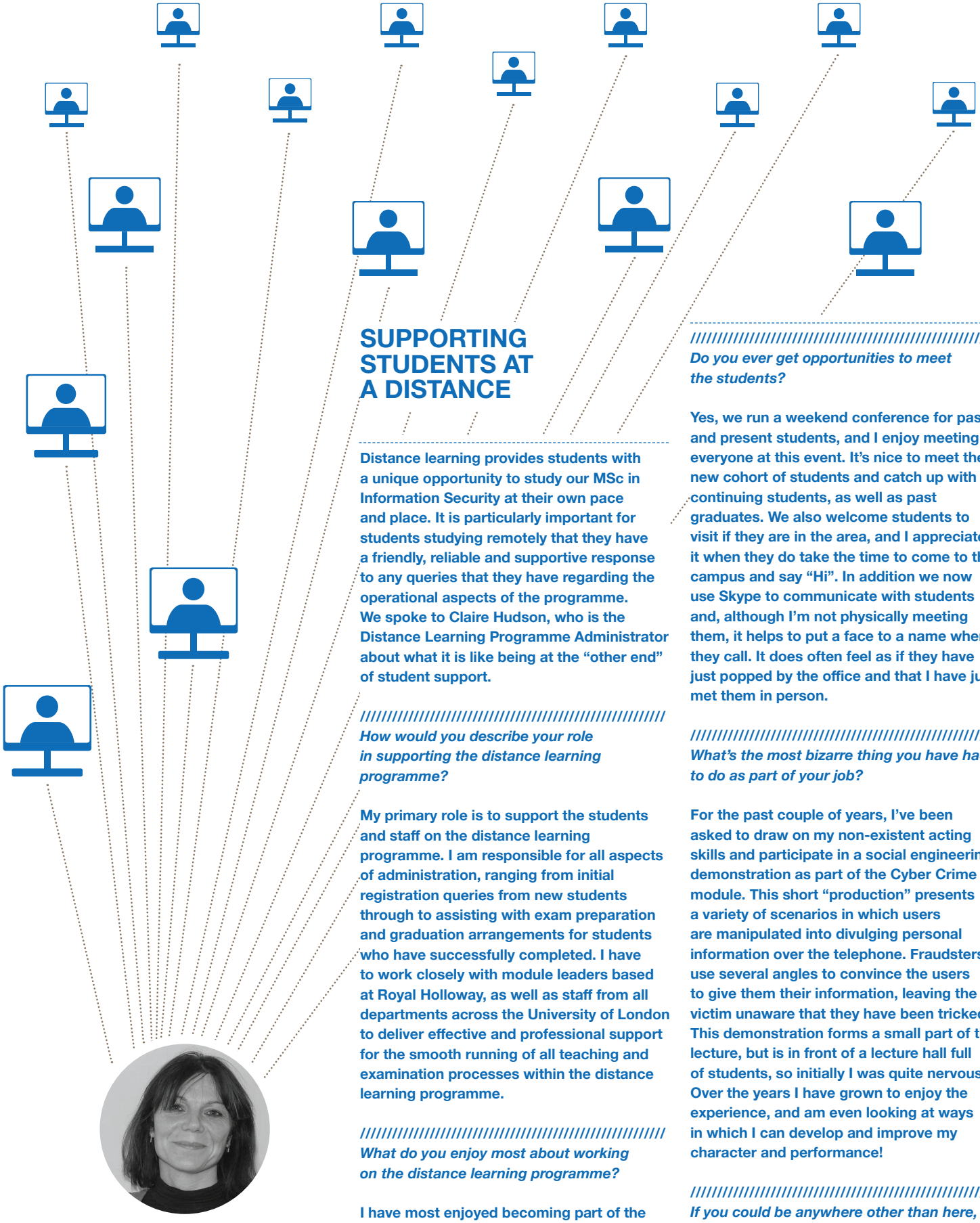
> Prof. Klaus Dodds is Professor of Geopolitics and Research Theme Champion: Security and Sustainability

In February 2013, Royal Holloway launched five new research themes, one of which was "security and sustainability". As a Professor of Geopolitics, I was appointed the "champion" for this research theme and part of my mandate over the next three years is to encourage inter-disciplinary and inter-faculty research initiatives building on existing and potentially new areas of research strength. The idea of the research themes is to provide a strategic focus for Royal Holloway and to act as a catalyst for future activity. Moreover, we hope that the research themes not only guide and support colleagues throughout the different faculties and departments of Royal Holloway, but also help to further promote our work within the academy and beyond.

The Information Security Group manifestly represents one of the most important areas of security-related research that Royal Holloway undertakes, with an enviable reputation for research and teaching excellence and a track record for engaging with academic and non-academic communities. I hope this research theme will act, in part, as a way of recognising the achievements of colleagues in ISG. Indeed without the ISG, alongside other pockets of excellence in security and sustainability-based research across the faculties, we would not have been able to creditably launch such a theme in the first place.

Looking forward, I want to do a number of things as research theme champion. First, I want to better understand the full range of research that we undertake at Royal Holloway. In part this enables me not only to learn about particular areas of interest but also better judge where we might take advantage of inter-disciplinary research calls and networking opportunities. I would like, where appropriate, to help bring research teams together to address these opportunities. Second, I hope this theme will encourage more interaction between security and sustainability-based researchers. For example, in the field of information security I could well imagine that a great deal of the research, say on security services, has to confront issues pertaining to logistical, financial, and political sustainability. And for researchers concerned with sustainability, questions regarding security are never far removed. How we make our lives more sustainable will in part depend on how we make judgements regarding what needs to be securitised or not. Third, with the launch of cross-theme funded PhD studentships, we have an opportunity to sustain a community of new researchers who will have supervisors drawn from two academic departments. The ISG is well placed to renew and establish new contacts with colleagues throughout the university.

As an example of the kinds of initiative that I want to seed, I recently had the pleasure of working with colleagues in Biological Sciences, Criminology and Geography on a project relating to social media usage and the British armed forces. In a nutshell the team were examining how the Ministry of Defence will need to review its social media policies in the light of changing technologies and user habits. They pitched the proposal to an ESRC/DSTL competition on Science and Security and have recently heard that they have been successful. I look forward to working with ISG colleagues to cultivate interdisciplinary projects of this type and would be delighted to hear from any potential partners who would like to get involved.



SUPPORTING STUDENTS AT A DISTANCE

Distance learning provides students with a unique opportunity to study our MSc in Information Security at their own pace and place. It is particularly important for students studying remotely that they have a friendly, reliable and supportive response to any queries that they have regarding the operational aspects of the programme. We spoke to Claire Hudson, who is the Distance Learning Programme Administrator about what it is like being at the "other end" of student support.

How would you describe your role in supporting the distance learning programme?

My primary role is to support the students and staff on the distance learning programme. I am responsible for all aspects of administration, ranging from initial registration queries from new students through to assisting with exam preparation and graduation arrangements for students who have successfully completed. I have to work closely with module leaders based at Royal Holloway, as well as staff from all departments across the University of London to deliver effective and professional support for the smooth running of all teaching and examination processes within the distance learning programme.

What do you enjoy most about working on the distance learning programme?

I have most enjoyed becoming part of the ISG team and getting to know the students and academics. It's particularly satisfying if I have been involved with a student's initial application, and then see them join the programme and really embrace the course through the distance learning mode of study. I have also enjoyed the range of tasks that I have become involved in since these vary depending on where we are within the academic year.

Do you ever get opportunities to meet the students?

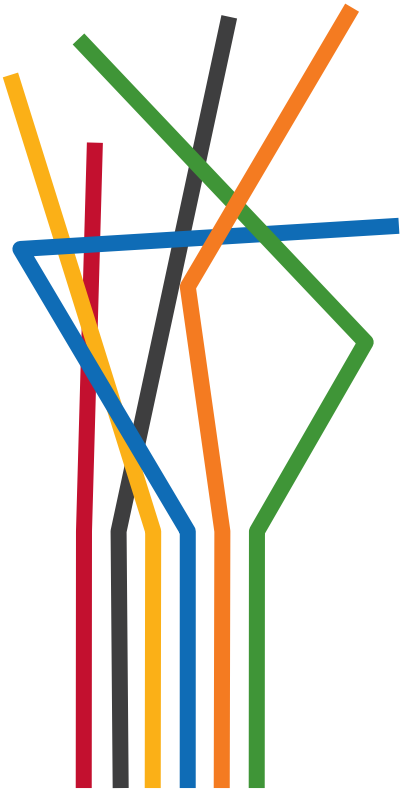
Yes, we run a weekend conference for past and present students, and I enjoy meeting everyone at this event. It's nice to meet the new cohort of students and catch up with continuing students, as well as past graduates. We also welcome students to visit if they are in the area, and I appreciate it when they do take the time to come to the campus and say "Hi". In addition we now use Skype to communicate with students and, although I'm not physically meeting them, it helps to put a face to a name when they call. It does often feel as if they have just popped by the office and that I have just met them in person.

What's the most bizarre thing you have had to do as part of your job?

For the past couple of years, I've been asked to draw on my non-existent acting skills and participate in a social engineering demonstration as part of the Cyber Crime module. This short "production" presents a variety of scenarios in which users are manipulated into divulging personal information over the telephone. Fraudsters use several angles to convince the users to give them their information, leaving the victim unaware that they have been tricked. This demonstration forms a small part of the lecture, but is in front of a lecture hall full of students, so initially I was quite nervous. Over the years I have grown to enjoy the experience, and am even looking at ways in which I can develop and improve my character and performance!

If you could be anywhere other than here, answering these intrusive questions, where would it be and what would you be doing?

I would love to return to Avenches, which is a small village just outside Bern, Switzerland. Ideally, I would enjoy a couple of hours of horseback riding around the picturesque mountains, and would then finish the day with friends and family enjoying a good bottle of red wine.



ISG SMART CARD CENTRE EXPANDS RESEARCH INTO TRANSPORT TICKETING SECURITY

By Keith Mayes

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

The year 2012 was momentous for the ISG Smart Card Centre (SCC) as we reached our tenth anniversary. This was celebrated at the SCC Open Day Exhibition on the 11th September 2012, which was sponsored by Orange Labs, The UK Cards Association, Transport for London (TfL), ITSO, Collis, Comprion, Cubic and Visa. A record 15 organisations and 20 MSc/Phd students exhibited and the day concluded with a very interesting guest lecture from John Walker (SiVenture/Cisco) on physical attacks against hardware security. As befitted a birthday celebration, there were balloons and a rather splendid cake with an icing QR code linking to the SCC website! However, the most exciting part of the birthday was the gift supplied by TfL.

Anyone who has followed the history of the SCC will know that it has been active in the area of transport ticketing security and systems, and that TfL (and also ITSO) have been staunch supporters over many years in their roles as Associate Members. The TfL birthday gift was an agreement to increase its membership / contribution to the highest level and commit this for a minimum period of three years. This was a fantastic endorsement of the SCC and its activities, and shows (along with the huge support for the Open Day) that SCC research and student projects continue to be relevant and of interest to both public and private organisations. The extra funding will enable us to expand our research in transport ticketing security in a direction that promises real/practical impact to systems in the UK and overseas.

If you have never given much thought to modern transport ticketing security then now is a good time to turn your attention to it, especially as there is now funding to support a couple of PhD students. Advanced transport ticketing systems involve almost all the security topics that an alumnus of the Royal Holloway MSc in Information Security would recognise from their studies: smart cards, algorithms, keys, protocols, PKI, HSMs, mobile phones, back offices, applications, sensitive data, e-payments, databases, IT/Web security, access control, payment scheme interfaces, forensics and so on. The financial value of transport ticketing also provides a great incentive for attackers to target transport ticketing security and attempt physical tampering, side-channel and fault attacks, as well as the human aspects of fraud/ criminality. This provides a very broad and interesting playing field for research, which will only get more intriguing as we see more regional and national smart card tickets, as well as options to pay via EMV “touch and pay” cards and mobile phone wallets.

It is worth pointing out some of the recent game-changing developments, as well as the diversity in national and international solutions. Most legacy chip-card transport ticketing systems have an electronic wallet containing travel credit; when a traveller uses the card at a terminal or gate, some of the credit is exchanged for ticket/travel permission. This requires the terminal to be able to support the cryptographic protocol for card communication as well as the business and fare rules to buy tickets and manage wallet contents. This all has to be conducted at great speed (to avoid user inconvenience and station congestion) and card transactions typically complete in a few hundred milliseconds, which rules out an online, real-time response from a back office system. The offline operation normally uses symmetric key cryptography and thus introduces a key management and protection responsibility for the terminal devices.

However, all this is being radically challenged in London as it is now possible to take a bus ride (and eventually a train ride) using your contactless EMV payment card, even though it has no transport wallet and uses asymmetric cryptography in the card-to-terminal protocol. A journey is then no longer really a sequence of wallet transactions, but rather a collection of fixed location authentications that are later resolved into a journey and payment by the back office. The speed of authentication is still a challenge, although not so problematic as once thought. Significantly, the system has changed from pre-pay to post-pay and the back office has to work harder to ensure correct payments are charged and received, and that suspicious cards are blocked from the transport system. From a technical perspective one might imagine that the terminals will become simpler without the need to store secret keys, however the reality is that they are more complex. The reason is that for some years the legacy Oyster cards will need to be supported as well as the EMV cards, and commuters into London will eventually also have ITSO standardised cards. ITSO cards are intended for high value national travel in the UK and are based on the traditional wallet and stored travel credential approach.

If we bring mobile phones into the equation then we have a lot more issues to investigate. Near Field Communication (NFC) enabled phones can be used to emulate transport tickets and payment cards, or indeed the terminal devices. There have been numerous proof-of-concept trials of NFC ticket emulation, including one in London some years ago. However, due to the slow rollout of compatible devices, the many different security options, and competing rather than collaborating industry parties, a mass-market fit-for-use solution is still some way off. The solution also needs to be desirable, keeping in mind that a user with an EMV contactless payment card or an Oyster card with auto-top-up can already travel around London without the need to go anywhere near a ticket office or top-up machine.

We are starting to see phones that offer EMV contactless emulation, albeit as a tight co-operation between individual mobile network operators, banks and a limited set of handsets. These phones might eventually be used for travel in London, however there are few of them, and banks are deploying bridging technology in the form of EMV “stickers” that you can attach to any phone. Technically this is not exciting, since it is similar to sticking your existing bank card onto your phone, however it may help to change user behaviour and encourage the use of the phone as a touch-and-pay device.

If we consider the international situation, there is sadly not too much harmonisation and compatibility of strategy or solutions. For example, in Scandinavia there are un-gated smart card ticketing systems and some practical smart phone (non-NFC) tickets for national travel. Furthermore, in Germany you can find a system where a smart phone is used as a terminal/reader emulator and the cards/ tags are fixed at stations. The EMV payment card (and phone emulation) is currently the most likely route to an international roaming solution, however its payment limits currently restrict it to low value local fares.

I hope this short overview of one of our current research areas will excite interest. If you are interested in research in this area then please get in touch.

ORGANIZATIONAL PROCESSES FOR SUPPORTING SUSTAINABLE SECURITY
By Alf Zugenmaier

> Prof. Alf Zugenmaier is a Professor in Informatics and Mathematics at Munich University of Applied Sciences (currently visiting the ISG)

The journey from Royal Holloway to Dagstuhl seemed to take us further and further away from civilization. It started with a flight to Frankfurt subject to severe delays due to adverse weather, then a train, and finally a taxi through a winter fairyland of snow. Schloss Dagstuhl is so secluded that it is hard to believe that this spectacular castle is one of the most eminent places in computer science research. There must be something special about this place that inspires computer scientists to make such long and complex journeys in order to reach it...

At Dagstuhl, the German Leibniz organization runs a famous conference centre, where world renowned experts in computer science meet for dedicated seminar series in order to advance the state of research. Lizzie Coles-Kemp from Royal Holloway was one of the organizers of a Dagstuhl seminar on organizational processes for supporting sustainable security. She invited approximately 35 researchers and practitioners, set the agenda, and started us off on our discussions.

First, a set of short “provocations” framed the problem space to be discussed. The provocations dealt with how security is handled in different organisations. “Provocateurs” described the day-to-day problems they were facing with organizational security in their business environments. The cases were diverse.

One case described a university research group which decided to move from a share-all access control policy to a more restrictive setting. The problem arose when one of the research group members decided to copy all of the documents to their hard drive before the new policy was put in place. This showed how tightening of security procedures can lead to unanticipated problems, including a sudden build-up of distrust between team members. A second case described security issues of information systems in health care and, more worryingly, security issues with information technology in health products. A third case presented an information security challenge with genuine life-and-death consequences: the dilemma social media poses to the military. As much as the military supports use of social media in order for soldiers to feel connected to home, there is a danger of soldiers unwittingly putting out seemingly benign information that might compromise operational security. Interestingly, despite the supposedly “complete” control of the military over their soldiers, this problem defies an easy solution. The discussions following up on these provocations got our minds set towards security problems faced by organisations, many of which go beyond technology.

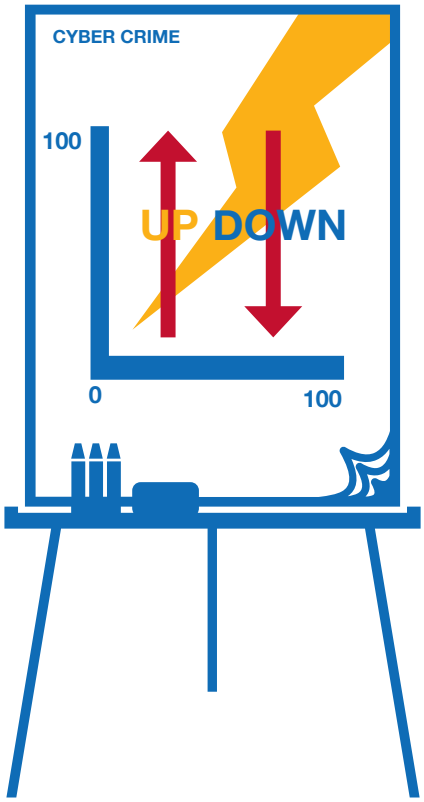
Following the provocations, much of the workshop was dedicated to a series of presentations and discussions on issues such as modelling frameworks, technical tools and research methods that can be used to tackle the organizational aspects of security policy lifecycle. These dealt with all aspects of socio-technical views of security, from policy setting through to verification, enforcement, and compliance.

My own presentation was based around a research project that I am conducting during my visit to Royal Holloway which deals with the importance of user authentication in the UK’s new universal credit benefit system. The problem with user authentication in this setting is that the users’ environment is not closely controlled. All security processes thus consider that the user could be under duress, potentially resulting in an insider attack either against the user’s own interests or against the interests of the benefit system. Designing security processes for this setting is not straightforward because, as benefits are time-critical, any security procedure that denies or delays benefits to eligible applicants will entail a cost that has to be borne by society. My research is based around the fact that there seems to be a current lack of understanding of how security policies can be tailored to address users potentially operating under duress. In this setting it is clear that the security policies need to be carefully chosen in order to minimize total cost to society, while ensuring maximum impact of the resources. During the subsequent discussion in Dagstuhl I received many valuable pointers from the audience, for which I am very grateful.

To emphasize the workshop character of this Dagstuhl seminar, participants were also asked to break into small groups and try to design organizational processes for security problems described in the provocations. In a second breakout session we then tried to design interventions to realize those organizational processes. When the results of these breakout sessions were discussed in front of the whole group, some time was spent addressing potential solutions to the individual cases. However, it became clear that we are still missing an arsenal of methods to tackle these problems more generally.

While many of us would love to have remained at Dagstuhl and attempted to solve some of these fascinating research problems, sadly the taxis arrived to take us back to the train station, from which we returned home to less secluded places and their many day-to-day distractions. My takeaway from these three days of intensive discussions in Dagstuhl, often continuing late into the night, is that while the problem space itself is reasonably well understood, what is missing are generally applicable scientific methods to arrive at, and to evaluate, potential organizational processes for supporting sustainable security.

For those of you wishing more information, the organizers intend to produce a paper summarizing the outcome from the seminar. Look out for further news about an interdisciplinary workshop and a possible special journal issue in order to document future progress.



UPSY-DAISY IN CYBER CRIME

By John Austen

> John Austen is Director of QCC InfoSec Training Ltd. and Consultant to the ISG

The figures for computer misuse offences (CMAs) within Greater London (known as the Metropolitan Police Area) were 12,817 in the year ending November 2012. This, a slight rise from the preceding year, was proportionally represented in the other 42 Police areas in England and Wales, the eight in Scotland and the one in Northern Ireland. Within London, 997 people were charged and 342 cautioned with these offences. This was a drop in cases from 2010 and 2011. Perhaps even more peculiar is the decline in the (police-recorded) Internet fraud and forgery offences from 2,519 to 2,240 and overall the non-CMA offences involving the Internet saw a decline from 3,096 to 2,686. So the question is: is Cyber Crime on the up or on the down? Let us look at some of the arguments and make sense of the police figures.

CMA offences fall into the categories of unauthorised access (otherwise known as computer hacking), unauthorised impairment to the operation of a computer (usually by some type of malware) and the supply or obtaining of tools or articles in order to commit these offences. Fraud and forgery relate directly to those cyber crimes that directly relate to financial gain.

A closer look at the figures begs the question as to whether or not this is a true reflection of Cyber Crime. The answer is probably not. Firstly the figures recorded by police have always been a marginal record of this type of criminality. Unlike other crimes, such as murder, there is no mandatory statutory requirement to report them to the police or to any other authorities. Secondly, insofar as computer hacking is concerned, the victim does not always realise that they are just that - a victim. Detecting intrusion into one's system or detecting Trojans or spyware is really a game for those who invest in up-to-date versions of the latest detection software; something usually far outside the means of individuals. Computer hacking is a strange crime; it is usually committed from a geographically (but not electronically) vast distance. The tools of the hacker are stealth, secrecy and anonymity. Only when they are caught does the true enormity and breadth of the crimes appear. In 1991, some 22 years ago, following the arrest of a three-member hacker group, an examination of their stored data revealed in excess of 10,000 successful intrusions into commercial systems – almost equivalent to the entire police figures for 2012. And that was just three hackers two decades ago, when commercial use of the Internet was much lower than today. Then we look at the recent surveys. The 2012 DTI and PWC Information Security breaches Survey showed historically high figures for intrusions into systems. Conducted on a (relatively small) survey of just 1,000 organisations, 93% of the larger ones reported a successful breach and intrusion into their systems. If that is the case for just that catchment, one wonders what the true UK-wide figures would show.

Whilst statistics are invariably open to interpretation, there is a yawning gap in our knowledge of the true extent of cyber crime. Recent comments from the Foreign Secretary on the threats of cyber crime to the U.K. National Critical Infrastructure and the substantial government monetary investment into combating it tell their own story. The notion that cyber crime is a periphery crime, demanding few investigative resources (as indicated by the police figures) is a flawed prognosis.

So why is there an acceleration in cyber crime? Obvious reasons include the proliferation of opportunity, targets, motivation, anonymity and the chances of success. In using an analogy: car theft was hardly a burning issue in the 1950's; fewer cars, fewer drivers and fewer trunk roads meant fewer car thieves. As an equivalent, in 1981 the ARPANET (forerunner to the Internet) expanded to a 213-node network with, naturally, no incidents to speak of. Today the Internet, expanding at breakneck speed, already connects more devices than there are people on Earth, even though just 2.4 of the world's 7 billion population are online. This vast communication system has provided a platform for a subdivision of cyber criminals, namely the politically motivated hackers - otherwise known as 'hacktivists'. A recent survey by Verizon estimates that at least 50% of hacking attacks in 2012 were by these groups. More opportunity, higher rewards, and, with the advancement of botnets, greater anonymity, have all contributed towards the creation of a cyber criminal's paradise.

And that is not all. Internet scams together with card fraud are at unprecedented levels. The Banks and Law Enforcement now admit that a 'no man's land' has emerged in which organised crime commit low-value frauds that generally go unrecorded, will never be investigated and are not even reported as crimes. Law enforcement have identified at least 1,000 crime gangs in 25 countries dedicated to committing cyber-fraud with at least 300 of those specialising in attacks targeted at Britain. Corroboration of this comes in the reports from The National Fraud Intelligence Bureau of 431,000 victims in 2012, a 9% increase on preceding years, with losses estimated at £185 million. Some cyber criminals are having a really profitable time. Their methods go across the cyber crime spectrum; Trojans to collect passwords, identity fraud from illegally accessed documentation, social engineering and phishing scams are the main weapons in the armoury.

Worse still, they are attacking a divided society; not necessarily divided by wealth, class, nationality or racial stereotypes, but a society divided in terms of technical knowledge and security awareness. Everybody uses email; everybody activates personal financial transactions in one form or another; and most use Facebook or other social networks – a mine of information for the unscrupulous. Unfortunately few actually understand how the technology works and the dangers that lie within it. This is a prime methodology of the cyber criminal, to attack the line of least resistance and target the most vulnerable.

Perhaps we really are 'In the Night Garden'.

ARTISTS AND DESIGNERS IN RESIDENCE

The end of the social research project Visualisation and Other Methods of Expression (VOME) marked the beginning of a new phase in the ISG's social and organizational research programme, building and extending the knowledge learned during VOME Lizzie Coles-Kemp has now started two new funded projects: TREsPASS, an EU funded project on quantitative risk assessment, and CySeCa, an EPSRC/GCHQ funded project on decision support for control selection.

Both projects see Lizzie leading research teams that use visual research methods and develop innovative ways of exploring and communicating the cyber landscape. Two new researchers have joined the ISG staff in order to extend our expertise in this area. Claude Heath is a visual art practitioner and researcher, and Makayla Lewis is a user experience researcher interested in accessibility design and creative research approaches. Here is how they describe themselves and their role in the ISG:

//

Makayla Lewis:

I have a passion for inductive Human Computer Interaction research. I completed a PhD in Human-Computer Interaction (HCI) at City University London's Centre for HCI Design in 2012, where I was funded by EPRSC to research online social network experiences and challenges, specifically change management, from a perspective of end users with motor impairments, especially cerebral palsy. Not only do I believe that the web should be accessible for all, it should also be secure for all. I was drawn to the CySeCa project because I'm not only passionate about user-centered research, but also about alternative ways to display this information using data-driven visualisations. I shall be using my user-centered design skills to draw out an understanding of how people influence the management of their data and how they use social networks to extend and maintain this influence. With this understanding we hope to map the organization in different ways and combine this view with a view of technical controls to better support the security management decision making in the cyber era.

I am a live *"sketchnote"* practitioner and have been producing and publishing sketchnotes about topics related to cyber security since I joined the ISG. My sketchnotes from the Hewlett Packard Colloquium were recently reviewed by Sketchnote Army who commented:

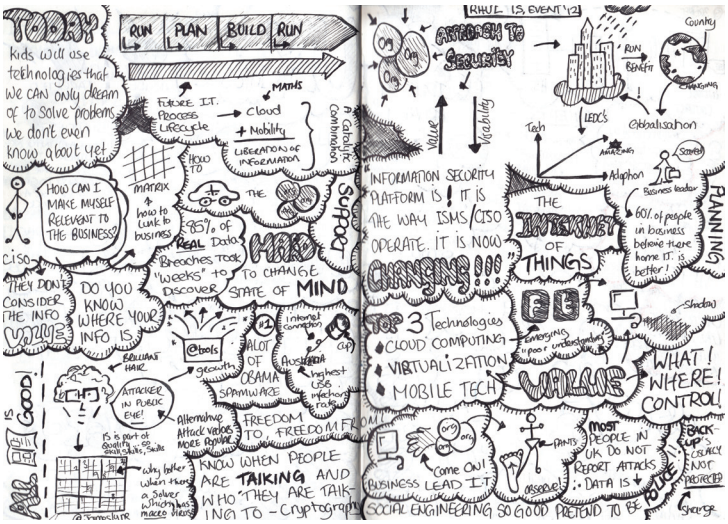
" I like the density of her sketchnote work and her use of the cloud separator for elements of information."

My sketchnoting is now making a regular appearance at ISG events including our weekly seminars and it complements a number of my other visualisation practices, including the use of rich pictures in organisational and community research. Lizzie's a keen supporter and comments

" Sketchnotes make a great tool for breaking down barriers between disciplines and communicating security-related concepts between academic and non-academic communities."

(http://sketchnotearmy.com/blog/2013/1/30/hewlett-packard-23rd-colloquium-on-information-security-sket.html)

Examples of my sketchnotes can be found at: http://www.flickr.com/photos/makaylalewis/sets/72157633090981769/



Claude Heath:

For me, the exciting prospect of joining the ISG at Royal Holloway is becoming part of a large team working on a difficult subject, that of security visualisation. The TREsPASS project, one arm of which is based at Royal Holloway, aims to break new ground in the field of security visualisation and threat navigation. My background is in visual art practice, specialising in drawing, while my first degree was in philosophy at King's College, London.

We are hoping that we can find some small way to inject fresh questions into the arena. Working with the 17 EU-based partners of the TREsPASS project, and engaging wherever possible with ISG members who work on these questions, the hope is that we can develop visual research techniques to help us on our way.

I come to Royal Holloway from Queen Mary, University of London, where I was based in the Cognitive Science Group in the Department of Electronic Engineering and Computer Science (EECS). This group specialises in the study of human interaction, and I have been looking at how drawing has been used in the social sciences, both as a means of recording and of discovery.

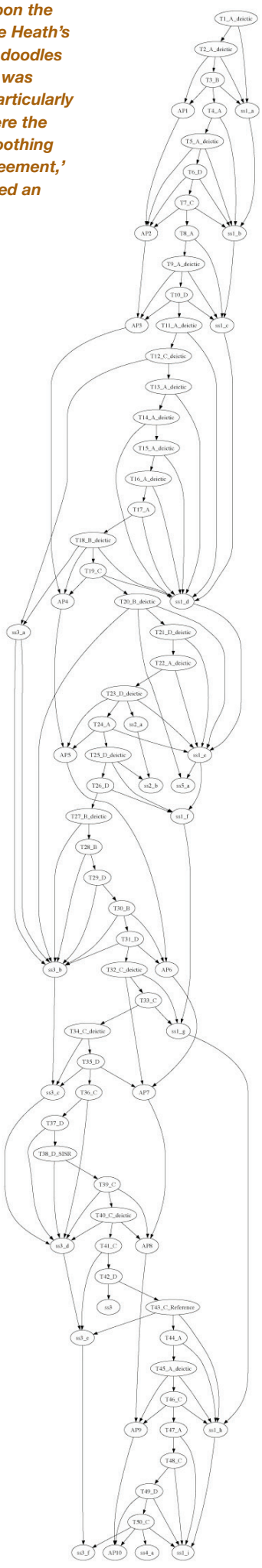
When looking at ethnographic data, my aim was to test out drawing strategies that add something to our understandings of shared space in human interaction. This data contained complicated and layered spatial interactions between collaborating architects, where establishing agreed meaning is crucial to their job, and shared space is an important means of achieving this.

It has never been my goal as an artist, or researcher, to make merely aesthetically pleasing pictures, so it was a pleasant surprise to hear Lizzie say about her research group: "we don't want to make pretty pictures." Nevertheless, I have found that if a visual idea comes about with a mix of rigour and free experimentation, people will sometimes use aesthetic words in connection with it.

Experience has taught me that an art practice can lead in any direction, almost by definition I believe. Also, one can never be quite sure where pictures will end up, or the uses they will be put to once they leave the studio. For example, I can quote a review of my work by Laura Cumming in The Observer, ('The Government Art Collection: At Work', Whitechapel Art Gallery, London 2011, touring 2012):

Sir John Sawers, currently head of MI6, previously at the UN, used to invite hostile nations into his office to dwell upon the beautiful cobalt ground of Claude Heath's 'Ben Nevis on Blue', all dots and doodles and just shy of figuration. Which was extremely helpful during some particularly heated negotiations on Iran, where the painting was used as a kind of soothing time-out for eyes and mind. 'Agreement,' according to Sawers, 'was reached an hour later.'

Works can be seen at:
www.claudeheath.com



HOW THE OTHER HALF LIVES: SECURITY DESIGN INFORMED BY FAMILIES SEPARATED BY PRISON

By Lizzie Coles-Kemp

> Dr Lizzie Coles-Kemp is a Senior Lecturer in the ISG

In 2012 I was lucky enough to lead a team of artists who specialise in using participatory engagement methods to unearth the collective narratives of a community. As a group, we use these collective narratives to explore how these communities might be served or supported. The aim of this Arts & Humanities Research Council funded Connected Communities scoping study was to work with the community of families separated by prison using a participatory engagement process in order to identify why some families do not engage with the support offered, and to envision how support might be re-designed to encourage wider engagement by more families.

The hardships that these families experience are many and varied. As the quotes (below) illustrate, families in this community often have to manage both the practical and emotional aspects of a family member being imprisoned.

Quotes from Telling the Children by Action for Prisoners' Families:

"I try to deal with things myself- I don't like going in and burdening him. I tell him things when the time is right. I don't talk about money. I do have problems with debt but I try to hide that – like last month my phone was cut off."
Prisoner's partner

"She mustn't think we don't love her... if we don't keep in touch she will think we don't love her and she will harm herself again"

As a security specialist, I learned a number of important points about security design on this project. In particular I saw firsthand how choices about information disclosure and service engagement are dramatically constrained when people are placed under enormous emotional and financial pressure. I realized how many assumptions we make in our security designs about the stability of the environments in which services are used and the attitudes that service users have towards service providers. When service users are not in stable environments and have conflicted feelings about the service providers, security practices are not as we might expect. Above all I learned that how we as people see ourselves in relation to technology defines much of our technology practice. In the context of families separated by prison, many families do not engage with support services because they simply do not see themselves as support users. Perhaps the same is true for people who do not use security services and technologies; perhaps some simply do not see themselves as security technology users?

It was an extraordinary project to work on and I am extremely grateful to the Arts & Humanities Research Council for the funding. The story of families separated by prison is a powerful, moving and often humbling story. It's a community of families that is often invisible to society. As researchers we felt that we were lifting off a curtain to reveal a diverse and resilient community that often feels cut-off and isolated in its struggles. We used our skills to explore how it feels to be a family separated by prison and, with two participant groups, we created collage, film and puzzles to better understand why aspects of support feel inaccessible to some and to envision how this might be changed. We hope that the creative outputs that this funding made possible will help families to feel that their voices are a little more audible.

All illustrations and collage design from this project are by Alice Angus, Proboscis. Further details on this project and links to the outputs can be found at: http://proboscis.org.uk/tag/hidden-families/

STAFF PROFILE: GERHARD HANCKE

> Dr Gerhard Hancke is a Teaching Fellow in the ISG

Tell us a bit about your background and how you ended up joining the ISG.

My early academic background is in Computer Engineering - I completed both my BEng and MEng degrees at the University of Pretoria in South Africa. In 2003, I was fortunate enough to be awarded a Skye Foundation scholarship to study towards a PhD abroad and I headed out to the UK to join the Computer Laboratory at the University of Cambridge. I arrived at Royal Holloway in the latter stages of 2007 when I was hired as a researcher at the ISG Smart Card Centre to work in the area of RFID and contactless tokens. In 2011, I was appointed as a Teaching Fellow with the ISG and essentially swapped the laboratory in Founders for an office in McCrea.

What are the joys and challenges of teaching on the MSc Information Security programme?

I enjoy teaching as every class is different and the students keep you on your toes. We have some really bright students who come from a variety of backgrounds – some students have been working in security-related fields for numerous years. This brings about some interesting discussions, and it is often possible to learn something new during a lecture or project meeting. As a teaching fellow I have had the opportunity to be involved in a number of different modules. This is a good opportunity and has challenged me to get involved in areas of information security outside of my own core interests. Teaching itself is also a challenge and delivering a good lecture takes some effort. Teaching is something that I am relatively new to so I am continually working to improve.

What are your research interests?

My main interest is the security of embedded devices. These tend to be categorised into many different areas, such as Internet-of-Things, smart tokens, mobile devices and cyber-physical systems, but essentially these are the bits and pieces all around us with some computational capability. These devices all play a prominent role in our everyday lives but do not always enjoy the same security scrutiny as larger devices such as a PC or server. I look at system security as a whole but have a particular interest in vulnerabilities and security mechanisms at the hardware and the physical communication layer. That said it is a perk of any academic position to go off and take a chance on something new, so I am happy looking at topics outside my main interests, especially areas of security such as management and law that are outside my current technical comfort zone.

How do these interests tie into research being conducted in the wider ISG?

In some cases being a bit of a generalist is useful and I feel that I can contribute in a number of areas. The boundaries between the technical and non-technical areas of security in particular present some interesting opportunities. I am currently involved in the ISG project on Cyber Security Cartographies (CySeCa), where I am working on methods for integrating and visualising organisational and data network data in a way that can aid security managers in identifying security issues. This requires me to do some system engineering and design, some applying of my understanding of technical network concepts, as well as some understanding of the softer science involved in organisational research, and some aspects of security management.

Do you think it will ever be possible to have smart mobile phones that provide a comfortable level of day-to-day security?

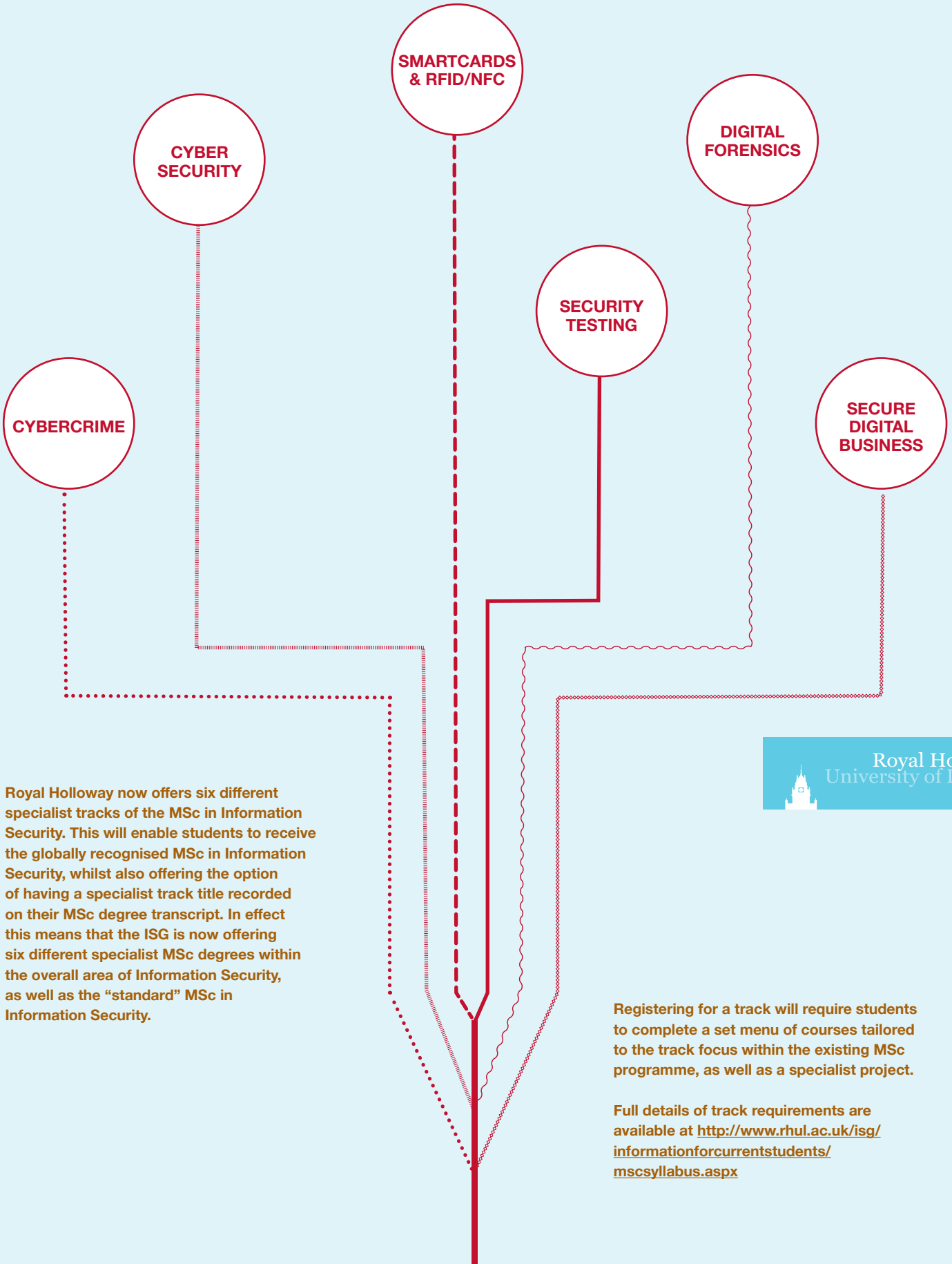
This is difficult to answer definitively – have we truly reached a comfortable level of security for devices that preceded mobile phones? I believe that mobile platform developers have a greater appreciation of security needs than their PC counterparts at a corresponding stage in the device lifecycle. This is positive and although it can definitely not be said that a complete solution exists, there is already some basic functionality in place which can be built upon for the future. What I think will happen first is that a comfortable level of security might be realised for specific applications. For example, some mobile payment applications already leverage a trusted execution environment, the SIM or a dedicated hardware module, within the mobile handset to implement security services under the assumption that the rest of the platform insecure. In the future, this approach could potentially extend to core security functions of the platform as a whole.

You have been looking after some of the ISG's outreach activities - how important do you regard this type of activity?

Outreach is our interface to the general public and it gives us an opportunity to make an impact on the wider society. At the moment we are primarily engaged in activities like school talks and participating in Royal Holloway's Science Festival, an open day where younger visitors can take part in a collection of science activities. Through these activities we raise awareness about security and we also promote security as a potential career path, along with STEM fields as a whole. We are looking at expanding our outreach activities to raise security awareness within a broader audience and this year we had our first public science lecture where Dr Lorenzo Cavallaro gave a great talk on malware and botnets. I hope this will become an annual event.

Tell us something about yourself that you think would surprise your closest colleagues!

South Africa is not known for anything cold but I have become a great fan of ice hockey. If you wander by my office you will sometimes see me catching up on NHL games (only during lunch and coffee breaks!). I support the Edmonton Oilers, who were really good around the time I was born and somewhat bad ever since, but they are my wife's hometown team so I'm not abandoning them yet. As an added benefit, games in Edmonton start around 2 am, which is great for working late and even better now that I have a few-weeks-old son.



Royal Holloway
University of London

Royal Holloway now offers six different specialist tracks of the MSc in Information Security. This will enable students to receive the globally recognised MSc in Information Security, whilst also offering the option of having a specialist track title recorded on their MSc degree transcript. In effect this means that the ISG is now offering six different specialist MSc degrees within the overall area of Information Security, as well as the "standard" MSc in Information Security.

Registering for a track will require students to complete a set menu of courses tailored to the track focus within the existing MSc programme, as well as a specialist project.

Full details of track requirements are available at http://www.rhul.ac.uk/isg/informationforcurrentstudents/mscsyllabus.aspx

CHOICE OF
SEVEN MSC'S FOR THE PRICE OF ONE!

MASSIVE OPEN ONLINE COURSE ON MALICIOUS SOFTWARE

By Lorenzo Cavallaro

> Dr Lorenzo Cavallaro is a Lecturer in the ISG.

FREE COURSE!

It all started with a big bang (for me). On a very hot day in July 2012, Keith Martin rang me up and left me a voice message: "We got to talk." Did I forget any malware running in the lab? Was I late with a deadline?

Fortunately, it was indeed a blast – and a positive one. It turned out that the University of London International Programmes had been approached by Coursera, a social entrepreneurship company that partners with top universities around the world to offer online courses for anyone to take - for free. Through this, Coursera, in its own words "hopes to give everyone access to the world-class education that has so far been available only to a select few; to empower people with education that will improve their lives, the lives of their families, and the communities they live in." As a result of this partnership, Royal Holloway has been selected to deliver two courses in June 2013. Emmett Sullivan (History) will deliver *The Camera Never Lies* and I have been given the honour to present *Malicious Software and its Underground Economy: Two Sides to Every Story.*

Cybercrime has become both more widespread and harder to battle. Researchers and anecdotal experience show that the cybercrime scene is becoming increasingly organized and consolidated, with strong links also to traditional criminal networks. Modern attacks are indeed stealthy and often profit-oriented. Malicious software (malware) is the traditional way in which cybercriminals infect user and enterprise hosts to gain access to their private, financial, and intellectual property data. Once stolen, such information can enable more sophisticated attacks, generate illegal revenue, and allow for cyber-espionage.

By mixing a practical, hands-on approach with the theory and techniques behind the scene, the course will discuss the current academic and underground research in the field, trying to answer the foremost question about malware and underground economy: "Should we care?" Students will learn how traditional and mobile malware works, how it is analyzed and detected, peering through the underground ecosystem that drives this profitable, but illegal, business.

Understanding how malware operates is of paramount importance to inform knowledgeable experts, teachers, researchers and practitioners how to fight back. Besides, it allows us to gather intimate knowledge of the systems and the threats, which is a necessary step in the successful devising of novel, effective and practical mitigation techniques. To this end, as a concrete ongoing research effort to fight malicious software, the ISG has been exploring several research directions focused on characterizing the behaviour of Android malware (http://copperdroid.isg.rhul.ac.uk --- joint work with University of Milan, Italy) and botnets (initial collaborative research effort with TU Milan, Italy), for which I have recently been awarded a three-year EPSRC -funded grant.

Malicious Software and its Underground Economy: Two Sides to Every Story is going to be a short six-week long introductory course on Coursera, and currently claims more than 20,000 registered students. Although statistics suggest that only 10% of registered students will actually take the course, it's undoubtedly the biggest audience that anyone in the ISG has ever presented a course to! The mixed nature of the audience (background, skills and expertise) will make pleasing everyone quite challenging. Nonetheless, I have been designing the course to try to keep it as interesting as possible for everyone...

So, if you are interested in malicious software and want to know a bit more about this fascinating topic, please do sign up to *Malicious Software and its Underground Economy: Two Sides to Every Story* as soon as possible. I'm looking forward to seeing you guys on June 1, 2013 on Coursera.

http://www.coursera.org/about
http://www.coursera.org/course/malsoftware

OUTSOURCING PERSONAL DATA PROCESSING TO THE CLOUD

By Chris Mitchell

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

01 Introduction

Use of the cloud for a wide variety of data processing purposes is undoubtedly a major growth area, with many potential advantages for users in terms of reduced costs, and simple and quick access to processing resources. However, problems potentially arise when cloud services are used to process personal data or, more precisely, Personally Identifiable Information (PII). In particular, whilst the data processing is outsourced, the legal obligations with respect to PII protection remain with the client of the cloud service. That is, the user of cloud services will have to ensure that the cloud service respects the legal obligations associated with the storage, management and processing of the PII which it submits for processing.

Since it is hard to imagine an organisation that does not hold a certain amount of PII, e.g. relating to its employees, this is likely to be a potential obstacle to almost any organisation wishing to outsource its data processing to the cloud. To ensure that it is not in breach of its legal obligations, an organisation will need to determine which cloud service providers will process PII appropriately.

One possible solution to this problem would be an auditable standard for cloud service providers which process PII. An auditor could verify whether a cloud provider meets the requirements of the standard and, if satisfied, it could issue a compliance certificate. This certificate could then be used both as a marketing tool for the cloud provider and as a simple way for a client to verify that a provider will meet their legal and regulatory obligations with respect to PII processing. Indeed, audited compliance to such a standard could be written into the contract for cloud service provision agreed between the cloud client and service provider.

The main focus of this article is an emerging international standard, ISO/IEC 27018[7], which is intended to become just such a standard. As such, it is hoped that ISO/IEC 27018 will solve a key problem for the cloud industry.

02 Meeting A Business Need

We next explore in a little more detail the need for such a standard. We first introduce some terminology. PII can be formally defined as any information that (a) can be used to identify the *PII principal to whom such information relates,* or (b) *is or might be directly or indirectly linked to a PII principal. As implied above, a PII principal (or data subject in some jurisdictions) is simply the person to whom the PII relates.*

We are concerned here with the needs of organisations acting as *PII controllers*. A *PII controller* (or *data controller* in some jurisdictions) is a person who, either alone or jointly or in common with other persons, determines the purposes for which and the manner in which any personal data are, or are to be, processed. We suppose that a PII controller wishes to use a public cloud service provider, acting as a *PII processor*, to process its PII (note that, in line with the scope of ISO/IEC 27018, we do not address issues relating to private cloud services). A PII processor is any entity that processes PII on behalf of and in accordance with the instructions of a PII controller. We refer also to a *cloud PII processor,* meaning a public cloud service provider acting as a PII processor.

The relationships between the key roles involved in PII management and use are shown in Figure 1.

As briefly discussed, developing the industry opportunity provided by the cloud needs both customer and regulatory authority confidence that PII will be processed in the cloud in ways that do not breach laws or regulations applying to the PII controller. To maximise the market opportunities, such confidence needs be developed as speedily as possible.

The goal of the work described here is to create a system for cloud PII processor governance, and for demonstrating conformance using certification. Moreover, this system should ideally integrate with processes already used by today's cloud infrastructure, based on existing PII processing obligations, to encourage rapid and wide adoption. The system should be capable of being developed in future releases to move towards improved cloud privacy as cloud infrastructure and privacy requirements develop.

03 PII Processing In The Cloud

If the PII controller uses a cloud service to process PII, then the PII controller retains its legal and regulatory obligations relating to the gathering and processing of PII. The precise nature of these obligations will, of course, depend on the jurisdiction within which the PII controller operates. The relationship of the PII processor to a public cloud service provider acting as a PII processor is shown in Figure 2.

The PII controller therefore needs to ensure that the public cloud service provider will meet the PII controller's obligations when processing PII. This can be achieved in two main ways.

1. The PII controller can ensure that the contract it establishes with the PII processor enshrines all the principles necessary to ensure that the PII processor's obligations are met.
2. The PII controller can verify that the PII processor behaves in appropriate ways through compliance auditing.

It is intended that ISO/IEC 27018 can assist with both of these steps. The PII controller can cite ISO/IEC 27018 in its contract, and can verify that the PII processor has been audited against the principles specified in the standard, thereby allowing the PII controller to select a well-governed PII processor.

04 THE ISO/IEC 27018 APPROACH

The cloud provider market already understands, invests in, and extensively implements, audited certification to ISO/IEC 27001 (information security management system requirements)[2], using the information security controls catalogue in ISO/IEC 27002 [3]. Moreover, the notion of ISO/IEC 27001 certification, with its origins in BSI 7799 parts 1 and 2, is now very well-established internationally, and is therefore something that will be familiar to many potential users of cloud services.

As a result, it has been decided to build on the existing ISO/IEC 27001 security management system. That is, cloud provider PII protection certification will be achieved using the existing ISO/IEC 27001 processes. ISO/IEC 27018 will act as a supplement to ISO/IEC 27002, containing (a) additional cloud PII processing-specific implementation guidance for existing ISO/IEC 27002 controls, and (b) additional cloud PII processing-specific controls; using the ISO/IEC terminology, ISO/IEC 27018 will be structured as a sector-specific standard to cover PII protection for a cloud PII processor. The additional controls in ISO/IEC 27018 will be used in conjunction with the ISO/IEC 27002 controls as the basis for certification of a cloud PII processor.

This approach is designed to provide a practical and pragmatic base to start the process of creating confidence that the cloud industry deals appropriately with the PII that it processes. At the same time, the public cloud industry will have clear guidance about what it needs to achieve to meet the legal and regulatory concerns of its clients.

It is hoped that the ISO/IEC 27018 approach will be attractive to existing cloud providers and will scale well. It also seems reasonable to believe that it will provide an economically viable means of developing an incremental accreditation and certification process, which can be continuously improved once it is in place.

05 SCOPE OF ISO/IEC 27018

The scope of ISO/IEC 27018, as previously explained, is a relatively narrow one. That is, it is restricted to those controls of relevance to a public cloud service provider acting as a PII processor. This scope is show diagrammatically as 'Scope 1' in Figure 3. In particular it excludes privacy concerns which may arise if a cloud service provider also acts as a PII controller. In fact, 'Scope 2' shown in Figure 3 is a potentially considerably larger scope, which it is intended will be addressed by a different standard that is currently at an earlier stage of development. Indeed, this latter standard is currently being balloted as a possible new work item, and will only proceed if the ballot result is positive.

ISO/IEC 27018 can be seen as implementing the privacy principles of ISO/IEC 29100 (the privacy framework)[4] as applied to a PII processor (but not as applying only to a PII controller). In the second Working Draft of ISO/IEC 27018, all additional controls have been classified according to these privacy principles. The scope of ISO/IEC 27018 is summarised in Figure 3. Scope of ISO/IEC 27018 Within SC27/WG5 we believe that ISO/IEC 27018 is a key element to start the cloud

Figure 1: PII – context of management and use

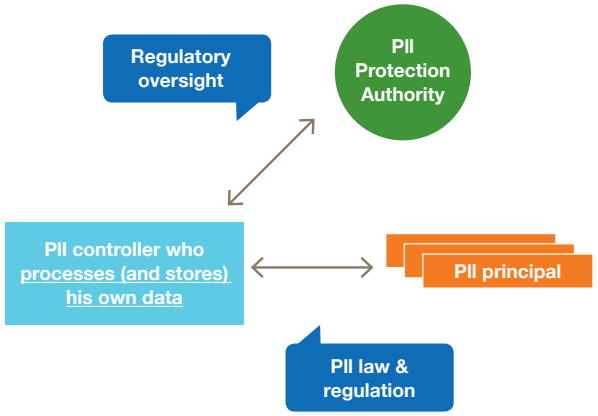


Figure 2: Relationship of PII controller to cloud PII processor

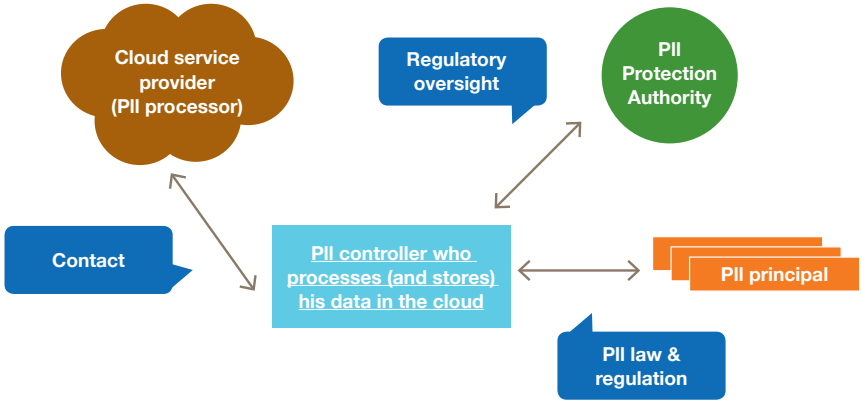
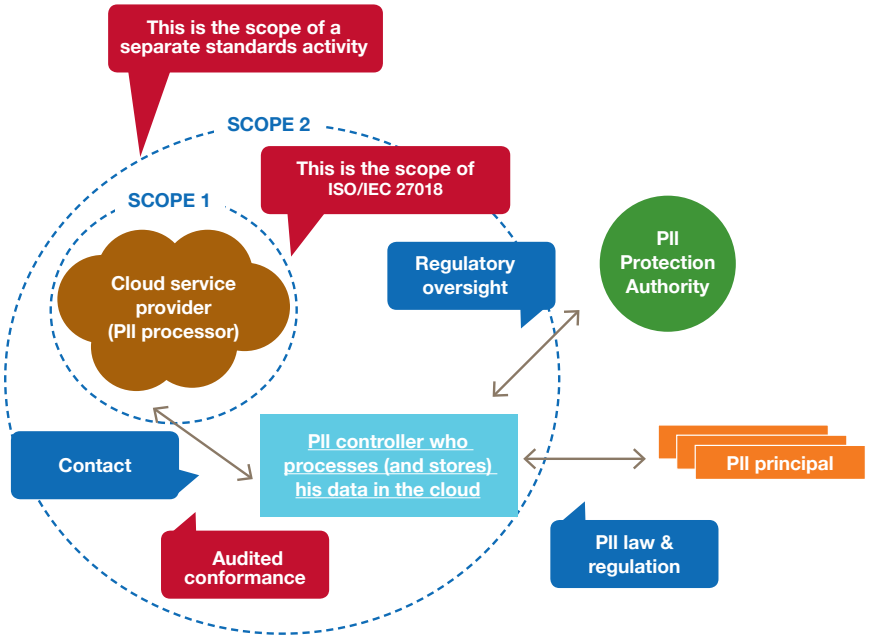


Figure 3: Scope of ISO/IEC 27018



industry moving down the path of privacy conformance.

06 ORIGINS OF ISO/IEC 27018 PROTECTION CONTROLS

Prior to producing the first draft of ISO/IEC 27018, an extensive analysis was performed of existing law relevant to third party processing of PII. The main result of this analysis was a set of 70 controls, which were documented in the original proposal for a new work item[5]. Only those not already covered by the existing set of controls in ISO/IEC 27002 were included in the first Working Draft of ISO/IEC 27018[6].

Subsequently, the European Union published an important review of cloud computing privacy issues [1]. These were carefully analysed, along with other published opinions, and used to derive a number of additional controls which were included in the current (second) Working Draft of ISO/IEC 27018[7].

The origins of the controls in the current Working Draft of ISO/IEC 27018 is summarised in Figure 4.

07 The Development Of ISO/IEC 27018

ISO/IEC 27018 is being developed within SC 27 *(Security techniques)* of ISO/IEC JTC1/SC 27, concerned with Information technology. Within SC 27, the development of the standard is being performed within Working Group 5 (WG 5), concerned with Privacy and identity management.

Work officially started on ISO/IEC 27018 with the successful conclusion of a new work item ballot in February 2012. A preliminary Working Draft was circulated in March 2012, and this was discussed at the Stockholm meeting of SC 27 in May 2012. A first official Working Draft[6] was circulated in June 2013, and discussed at the Rome meeting of SC 27 in October 2013. Following lively discussions in Rome, a second Working Draft[7] was circulated in December 2012, which is due to be discussed at the Sophia Antipolis meeting of SC 27 in April 2013.

To participate in the development of ISO/IEC 27018 please consider joining the work on SC 27/WG 5, via your national standards body. As the editor of ISO/IEC 27018 I am always happy to provide information and answer questions – contact me at: me@chrismitchell.net.

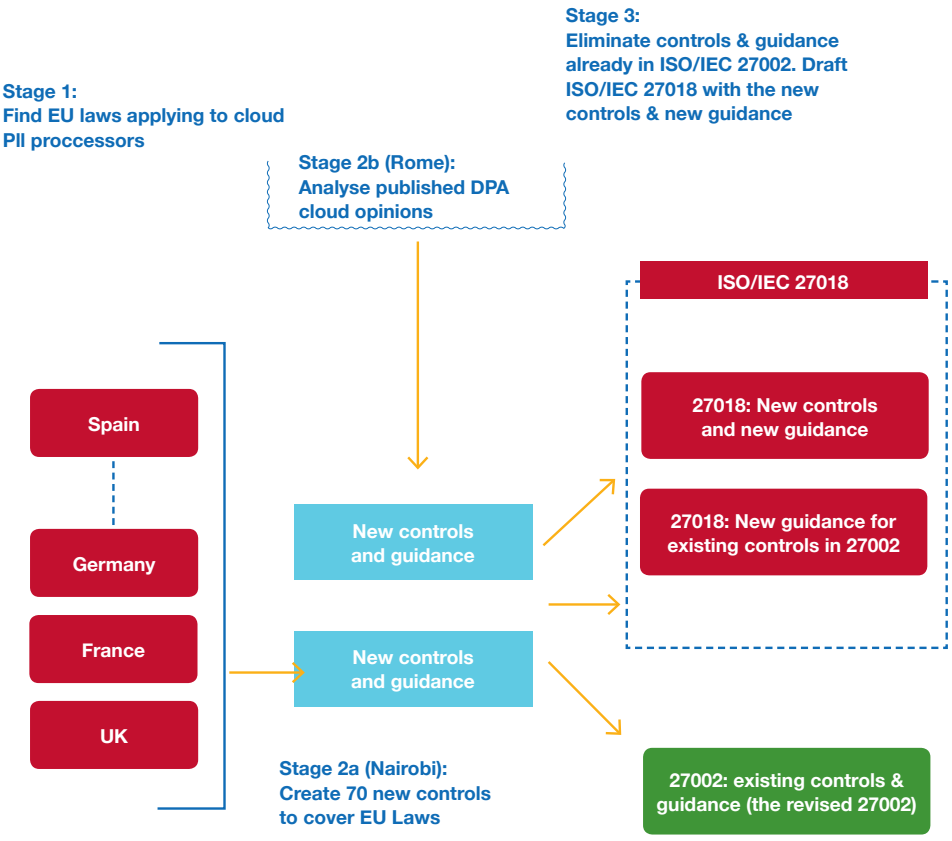
08 Acknowledgements

I would like to thank John Phillips for not only providing all the figures in this article, but also helping greatly with the structure and text. I am further indebted to Microsoft for their generous support during the development of ISO/IEC 27018. Finally, I must thank all the experts in SC 27/WG 5, whose valuable comments and suggestions have helped shape the current draft of ISO/IEC 27018.

09 Bibliography

1. European Union, Article 29 Working Party, Opinion 05/2012 on Cloud Computing, adopted July 2012.
2. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements, 2nd edition (to be published).
3. ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls, 2nd edition (to be published).
4. ISO/IEC 29100, Information technology — Security techniques — Privacy Framework, 2011.
5. ISO/IEC JTC1/SC27 N10550, Proposal for a new work item on Code of practice for data protection controls for public cloud computing services, November 2011.
6. ISO/IEC JTC1/SC27 N11253, 1st WD 27018, Information technology – Security techniques - Code of practice for data protection controls for public cloud computing services, June 2012.
7. ISO/IEC JTC1/SC27 N11742, 2nd WD 27018, Information technology — Security techniques — Code of practice for data protection controls for public cloud computing services, December 2012.

Figure 4: Origin of ISO/IEC 27018 controls and guidance



CYBER SECURITY CLUB UPDATE
By Geraint Price

> Dr Geraint Price is a Lecturer in the ISG

Over the past fifteen years, the ISG has run a number of industrial research "clubs" which bring together various interested parties from industry, government and academia to discuss central issues of relevance to the club theme. We have previously hosted clubs on elliptic curve cryptography, quantum cryptography, PKIs, and identity management; we are currently looking at cyber security.

This most recent club came about through discussion with one of the member organisations who felt that, as the phrase "cyber security" was a burgeoning theme in the press, it would be good to discuss this further. The club itself started in September 2011 and has held eleven meetings to date.

Each meeting involves an invited speaker coming to lead a discussion relevant to their particular area of expertise. As befits discussion surrounding cyber security, we started with a mix of speakers from government and industry. This gave us a basis from which to target more specific topics, such as malware, the policy challenges and mobile security.

What have we learnt? While the discussion is ongoing, there are some consistent and interesting themes that have emerged from our deliberations.

Firstly, the pace of change in this arena is relentless, and it is only getting faster. As a result, our ability to respond and develop coherent strategies for mitigating the threats we face are being severely tested.

The second recurring theme is that we need to move away from a silo mentality. The very nature of "cyber" is that of an interconnected world. No one individual or organisation can provide the answer. Indeed, the highly interconnected nature of the services we produce and consume on the Internet means that action and reaction are becoming increasingly difficult to map out.

Another theme consists of an existing truth that only gets more and more relevant as time goes on. After a decade of attending industry-focused security events, I have lost count of the number of times that I have heard that there needs to be a greater understanding and symbiotic relationship between the core business function and the security function within an organisation. This is not something new but, taking into account the two previous findings, it is only going to get more imperative that we get to grips with this issue.

Another theme that has emerged is that efficiency will be the key to good cyber security. With an increased range of services to protect, and an ever expanding range of threat actors, we are likely to be asked to provide more varied security services in a wider range of environments, without a suitably commensurate increase in the level of funding. And this was going to be the case even before the cascading effect of the economic downturn of the past few years.

Finally, what has become all too apparent is that the burden of responsibility needs to be shared between the public and private sectors when we come to look for solutions to the problems faced. Ultimately, this highlights that the focus in the club has come full circle. In starting off with a wide range of speakers from government and industry, our initial goal was to ensure that we had sufficient breadth to set the scene for our discussions. However, we now believe that this far-reaching shared view of responsibility is itself integral to our findings.

While the club meetings have been interesting and informative, there is also a desire to move the discussion beyond the confines of the club itself. We have already presented a précis of some of our findings at the 2012 ISF Congress. Once we have concluded our discussions, we intend to publish the findings in a white paper which we hope will help to inform some aspects of the contemporary debate about the nature of cyber security.

NEW CYBER SECURITY RESEARCH LAB AT THE ISG

By Dusko Pavlovic

> Prof. Dusko Pavlovic is a Professor in Information Security with the ISG

1 What is ASECOLab?

ASECOLab is the Adaptive Security and Economics Laboratory at the Information Security Group of Royal Holloway, University of London. It was started in September 2012, with funding from the US and the UK Governments, including EPSRC and AFOSR, and with a gift from Intel Corp. At the moment, ASECOLab consists of 14 aseconauts, including 5 PhD students, and 4 external members. It is located on the first level of McCrea Building, and on the web at asecolab.org.

2 What do we do at ASECOLab?

We try to solve some problems of security and economics in cyber space. Security and economics are, of course, two sides of the same coin: wealth comes with security, security with wealth. In the early days of computing, the problems of security and economics were tackled separately; but it is becoming increasingly clear again that many security vulnerabilities cannot be solved without an economic analysis, and that many economic problems require security solutions.

2.1 Exploring New Directions

There are already many different approaches and directions in security. Why seek new ones?

Security is one of the driving forces of history: both war and diplomacy are efforts towards attaining security goals. With the advent of computers and their spreading through our work and life, computer security came into focus, as a new family of engineering problems. A new family of security solutions emerged from modern cryptography, based on the capabilities and the limitations of computers.

Diffie and Hellman's paper *New directions in cryptography* is often mentioned as the inception point of the revolution that produced the cryptographic tools of computer security. But as computers joined into networks, cyber security emerged as a new problem area, where the old solutions didn't seem to apply. Resolving the problems of cyber security seems to require a paradigm shift, akin to the one brought forth in cryptography by Diffie and Hellman's *'New directions'*. We are thus looking for *new directions in cyber security.* Tables 1 and 2 (Below) provide a crude overview of the paradig-matic shifts in computation and in security.

2.2 Cyber Security Problems

Cyber space is the distance-free space of costless communication, where modern networking technologies assure that every two nodes appear to each other as neighbors. But since this *'end-to-end'* network service hides the communication routes, a pair of nodes with whom I am communicating cannot be distinguished by their positions in cyber space, like they are distinguished in the physical space. And since I cannot tell these two nodes apart, the problem of authentication arises. In this way, cyber space challenges some of our basic communication assumptions. Similar authentication problems have, of course, already been treated in computer security. But cyber space also changes our notion of computation. In a computer, computation is the process of executing programs. In a networked computer, as a gateway into cyber space, computation ceases to be programmable in the old sense, as the processes invoke each other across the network, and run out of sight, beyond the horizon. Computation is therefore not fully and directly controlled by programs any more, but it can only be steered indirectly, through security protocols. Network computation is not a pure artifact of programming, but it involves natural information processing, like life, or society. Although it still involves a lot of programming and engineering, network computation as a natural process is thus not only a subject of engineering, which synthesizes artifacts, but also a subject of *science,* which analyzes natural processes. Cyber security requires that we take the *'science'* in 'computer science' seriously.

2.3 Cyber Security Solutions, and the Gap

As a new problem area of great economic, political and technical interest, cyber security has attracted a lot of attention, and focused efforts from government, from security industry, and from academia. Extensive and focused legislative and policy efforts have been undertaken in many countries, attempting to tackle the problems cutting across all areas of social life, from national security and governance, through industry, economy, to culture and social networking. The looming dangers of cyberwar and the intricacies of protecting the critical infrastructure from cyber attacks have been quickly recognized by governments and their agencies. The grave economic losses from the cyber attacks have been extensively analyzed, publicized, and transformed into signicant business opportunities for the security industry. The complex and quickly evolving problems of social networking in cyber space, such as cyber bullying and loss of privacy, have attracted a lot of public attention and interdisciplinary research. The gentle reader

Table 1: Paradigms of computation

AGE	ANCIENT TIMES	MIDDLE AGES	MODERN TIMES
Platform	computers	operating system	network
Applications	Quicksort compilers	enterprise systems	World Wide Web botnets
Requirements	correctness temination	liveness safety	trust privacy
Tools	programming languages	specification languages	scripting languages

Table 2: Paradigms of security

AGE	MIDDLE AGES	MODERN TIMES	POSTMODERN
Space	computer center	cyber space	cyber-social- physical space
Assets	computing resources	information	public & private resources
Requirements	availability authorization	confidentiality integrity	trust privacy
Tools	locks | tokens | passwords	cryptography protocols	mining & classification

of the ISG's newsletter has probably already encountered much more information about all these problem areas than could fit into this issue. Figure 1 illustrates the main cyber security problem areas, ranging from cyber war, through cyber crime, to cyber bullying. Figure 2 illustrates the main types of cyber security solutions. The two distinct families of approaches, at the two ends of the spectrum, tackle the cyber security problems through:

- Policy, i.e. the legislative and regulatory efforts of governments and industry consortia; and through
- Technology, i.e. by adapting and extending the existing cryptographic techniques for cyber security applications.

To connect and coordinate the two types of solutions, the stakeholders from governments, industry and academia initiated broad collaborative networks, casting aside many old boundaries. In cyber space, nobody can win without their friends, not the attackers, and not the defenders. The main challenges, however, remain on the middle ground, between the technical solutions and the policy solutions. The strategic gear box in the middle of Figure 2 is needed to synchronize the engine of cryptography with the wheels of policy. Although the interdisciplinary combinations of the methods from social and computational sciences provide some solutions, it seems unlikely that a toolkit for management of computational and economic resources will be obtained by mixing the existing toolkits. The genuinely new adversarial situations that arise in cyber space require genuinely new adaptive strategies, leading to security as equilibrium, through economics. This strategic middle ground, the gear box on Figure 2, is the area that we are studying in ASECOLab.

2.4 Adaptive strategies

In the 1950s, the new strategic challenges engendered by the Cold War grew to be more complex than anything that generals and diplomats had seen before. They asked mathematicians for help, and game theory was developed to facilitate strategic decisions in adversarial situations. The Cold War is now over, but game theory is still used to model the adversarial situations in various sciences, and in daily trading on the markets. The problems of cyber security are also complex and adversarial. Why is game theory not a standard tool of cyber security, like it is a standard tool of economics?

The reason (or at least one of the reasons) is, roughly speaking, that game theory assumes that the players follow the rules, whereas the cyber attackers often break the rules, and sometimes prefer to win that way. This type of adversarial situations brings with it new challenges. As an illustration, consider the toy model of a game of attack vectors, displayed in Figure 3. The first picture illustrates the slogan that the defenders have to defend all attack vectors, whereas the attackers only need to choose one. The remaining illustrations show how System turns this strategic disadvantage into an advantage by assigning increasingly greater weights to the information about the opponent. The final graphic depicts the strategic situation where the attackers have to conceal all identity markers, whereas the defenders only need to defend one marker. Our adaptive immune system is a realization of this strategy. The illustrations thus show how the strategy of a 'fortress under siege' on the left evolves into the strategy of a 'macrophage devouring a bacterium' on the right. The illustrations correspond to the states arising in the mathematical model of this game. For more details and references, please visit asecolab.org.

3 What else do we want to do at ASECOLab?

While the game of attack vectors illustrates our overarching goal, to provide mathematical tools for strategic reasoning in cyber security, it is just an example from one of the projects. Like computations in a network, the projects invoke each other, pass tasks to each other, and depend on each other's results. There is not enough space here to try to introduce all of them, but the web site at asecolab.org provides an overview. Covering the important questions, but not spreading the efforts too thinly, and determining the right priorities – is a matter of subtle balance. At the moment we have enough funding for 3 years of research, and probably enough questions for 30. We'll do our best.

Please don't hesitate to contact us for more information: dusko.pavlovic@rhul.ac.uk

Figure 1:
Flavours of cyber security problems

Figure 2:
Flavours of cyber security solutions

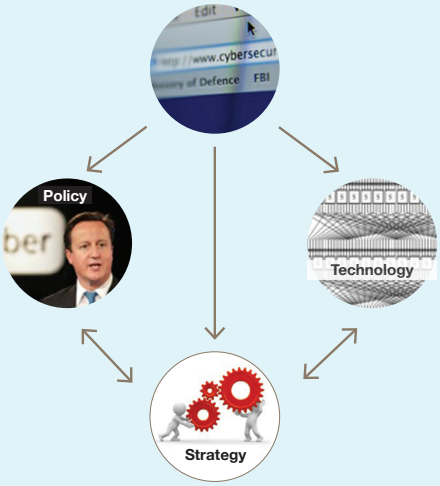
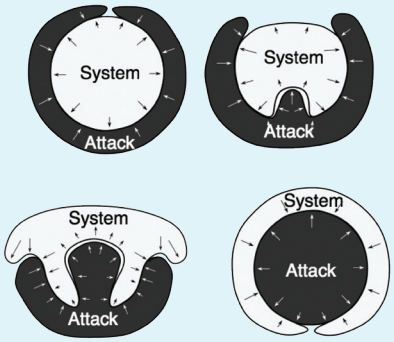


Figure 3:
Game of attack vectors



VISITING PROFESSOR: ANDY CLARK

The ISG is delighted that Andy Clark's long association with the ISG was recently formalised through the establishment of a Visiting Professorship.

Andy, you've had a diverse and interesting career – can you provide an overview?

My career in the information security industry started in earnest in 1984 when I joined Open Computer Security as Research & Development Manager responsible for managing the development of the company's range of commercial encryption products aimed at the banking and finance sector. I remained with the company during its acquisition by new owners and renaming as Computer Security Limited in 1985. In late 1990 I left to join Logica plc.

I was both a Programme and Divisional Manager with Logica's Secure Systems Division where my work was focused towards specification, design and management of the development of systems with very stringent security requirements developed for a specialist government client base.

I left Logica in 1996 to found a consulting practice, Primary Key Limited, specialising in the analysis of the security of cryptographic systems. At the same time I accepted a part-time position on the Board of Sapher Servers Limited where I joined my good friend Vince Gallo (ex OCS and Sapher's founder) and was responsible for technical and corporate development of a range of secure messaging products.

Sapher Servers Limited was acquired in 1998 by Entegrity Solutions Corp. I joined the Board of the U.K. operating company as its Operations Director from 1998, then in 2001 joined the Corporate ISS team where I specialised in the design of large scale business-to-business information security architectures.

I left Entegrity in late 2001 and founded Inforenz Limited, a U.K. company specialising in information system and cryptographic forensics. We designed and implemented a range of specialist forensic tools and software applications. I was a member of the Board responsible for product development and also undertook detailed forensic casework for both criminal and civil matters.

Inforenz Limited was acquired by Detica Limited in July 2006 at which point I was appointed Head of Forensics at Detica. I remained in that role until December 2010 when I left to form a new company, Primary Key Associates Limited, a company that provides a range of consulting services including digital forensic investigation of information systems and analysis of the security of information systems designed to protect digital assets.

How did you first get into the area of information security?

Well, ironically, it was in my first real job out of school. Some ten years before joining Open Computer Security I was working for a flight simulator manufacturer. Because of my natural interest in radio communications systems (I was an active radio amateur at the time) I managed to get assigned to the department responsible for the design of (simulated) navigation and communication systems. The first project I worked on was Concorde (still my favourite) but the second was the Jaguar strike aircraft. As part of that project I had to understand the mechanisms of the IFF (Identify Friend Foe) protocol. It was my first introduction to cryptography (Challenge/Response) and I was naturally curious to find out why it was considered 'secure'. As part of my research I discovered David Kahn's book, The Codebreakers, which opened my eyes to a new and exciting world, albeit one that I would not join as my profession for another decade.

Tell us about your association with the ISG.

In the mid 1980's the UK crypto manufacturing community was pretty small. Each company had access to mathematicians and cryptologists, either as fulltime staff members or as external consultants. At OCS we retained the services of Donald Davies with whom I consider myself privileged to have worked. I think it was Donald that introduced me to Fred (Piper) and I started then to understand the importance of the crypto group at RHUL. My relationship with the ISG started in 1991 when I was General Chair of the IACR's Eurocrypt conference held in Brighton. I needed help with the operational aspects of running the conference and Fred suggested some of his students might be able to help. I seem to recall a young Keith Martin being one of them…

Remind us now - exactly how many IP-enabled devices did you say you had in your home?

I checked my router this morning and there were 48 active leases – my latest favourite device is a Raspberry Pi – it's running my home VoIP phone system, brilliant!

What do you hope to contribute to the ISG as a Visiting Professor?

I hope that sharing my experience of designing, implementing and forensically analysing secure systems over many years will help the ISG understand the commercial structures and objectives that drive the 'security industry'; one that has been through a substantial level of change during the time in which I have been engaged within it, and one that continues to change.

If you had one piece of advice for aspiring cyber security professionals, what would it be?

Try and think from a systems viewpoint – it can be too easy to be submerged in security technologies without considering the bigger picture. I recall several projects where the proposed security solution was nothing more than window dressing to comply with an internal standard, missing the threats completely. Security needs to be "business driven" and thinking from a systems viewpoint is critical to understanding where best it should be applied and the benefits it should deliver.

As someone who has been an information security practitioner, whilst maintaining close relationships with academia, how do you see the relationship between academic research activities and information security practice?

I am really encouraged by how this has changed over the years. When I attended my first Eurocrypt in 1987 there was limited understanding of the role of cryptology outside government, academia and the banking sector. Since then, organisations like IACR have provided, through workshops and conferences, a showcase for the best academic research in the field, and that has been picked up by the information security industry and beyond. Institutions like RHUL now have a much higher profile outside the

InfoSec community as being at the leading edge of security research and a source of innovation.

What do you see as the biggest cyber security challenges facing society?

I am reminded of the rather pointed help desk acronym PICNIC – Problem In Chair Not In Computer; security usability remains one of the most challenging areas for society. The vast majority of us have no interest in interacting with any security system, we just want it to work and do its job. Our increasingly technology-led society develops more and more sophisticated devices, some of which can be life-enhancing or life-threatening, such as intelligent vehicles and remotely accessible medical equipment and implants. The users of such devices are probably the least well-qualified to make any decisions about their security features and functions and we should not consider them to be the problem if it fails. That means we need to consider system failure as an integral part of our security design and decide how best we can recover safely, without having to involve a user; that is not going to be easy.

As an information forensics professional I think there is a big risk that system designers will frequently continue to ignore the importance of designing and implementing proper audit facilities in a system to establish what happened when things went wrong. Planning to understand security failures in systems is critical to improving them over time.

What's your prediction for the future of the Internet and its security?

As Niels Bohr said "Prediction is very difficult, especially about the future" and I feel less qualified than him to make accurate predictions. I think one thing is clear: our (Western European) society is already almost completely dependent on IP-based communications systems. More than three quarters of the UK's critical national infrastructure (CNI) is controlled by commercial companies whose primary interest is their duty to their shareholders. We are going to need to recognise this dependency and make sure that the CNI is not just technically, but also commercially resilient.

You're a technology fan, what future gadget would you love to see developed?

The babelfish.

NEW MSC MODULE ON SECURE BUSINESS ARCHITECTURES
By Geraint Price

> Dr Geraint Price is a Lecturer in the ISG

This academic year has seen the addition of several new modules on the ISG's MSc Information Security programme, one of which is Secure Business Architectures. This is a new core module for students following the pathway through our MSc which is directed towards students with more of a "business bent".

Why this new module? For some time I have felt that organisational requirements were not sufficiently represented when discussing the security infrastructures and technologies which are implemented in those organisations. While the core module Security Management covers many aspects of the business-to-security relationship, I felt that the "why?" of the design choices made in relation to the technology was not sufficiently covered. This led me to propose a new module to fill this void, which ran for the first time this year.

The overall syllabus is broken down into three parts. The first part effectively sets the scene and outlines the tools through which we will analyse the technological choices which the organisation is faced with. It covers GRC (Governance, Risk and Compliance), Risk Assessment (as its own component) and the Secure Development Lifecycle. These are then used as lenses through which we analyse some candidate infrastructures and technologies which many modern organisations implement. Those are: Identity Management, Cloud Computing, PCI-DSS, BYOD, Supply Chain Security, and Big Data. To close, we had a guest lecture from one of our alumni, Holger Mack, which brought those themes together from the viewpoint of a practitioner in the field.

A number of topics were delivered by subject-specific experts, including Paul Dorey (Visiting Professor, and former CISO) who commented: "This new module gives life to how security management processes and standards are used in practice. I have been delighted to share real experiences with the students."

MSc student Alan Watkins enjoyed the experience: "Secure Business Architectures was an interesting and stimulating course. After covering the mechanics and the processes involved, week by week we went on to see how they have been applied in different industries. We saw how it has shaped and refined the security of everyday systems, such as credit cards and mobile phones, and the challenges emerging technologies like BYOD and Cloud still have to address. We were encouraged to participate in lectures, with lively debates where students could draw upon their work experience and how these things work in practice."

ALUMNI REUNION CONFERENCE 2012
By Chez Ciechanowicz

> Dr Chez Ciechanowicz is MSc Information Security Programme Director

Our third Alumni Reunion Conference, held at Royal Holloway from 25th – 27th June 2012, was attended by well over one hundred of our alumni. It was also the twentieth anniversary of the launch of the MSc in Information Security. Many of these alumni are now in very senior, in many cases top, positions within the information security sphere. The format was similar to previous events in that, with the exception of two keynote speakers, all the talks were given by alumni of the Royal Holloway Information Security MSc programme. What was particularly pleasing was to see two of the original alumni from the 92-93 cohort (in which there were only seven full-time students!) delivering two of the presentations.

The first of the keynotes, "The Future of Security - responding to what is ahead", was delivered by Dr Alistair MacWillson from Accenture Technology Consulting. Alistair frightened the life out of us with his predictions, but at the end of his session he redressed the balance by reassuring us that all of our jobs were safe for many (many) years to come! The second keynote was by our own Visiting Professor, Whit Diffie, who gave a fascinating historical talk about the fundamental turning points in the development of cryptography.

As always the atmosphere was convivial, the quality of the talks was excellent, and a thoroughly enjoyable time was had by all, including some mutually beneficial recruitment sessions (or should I say "poaching sessions"?). Reactions from the attendees were very positive and more than one alumni commented that the event was easily as good, if not better than, equivalent commercial conferences, while attendance involved a minute fraction of the costs.

I would like to thank Kostas Markantonakis, Emma Mosley, Fred Piper and Geraint Price for their considerable help with organising and running the 2012 conference.

2500
ALUMNI CAN'T BE WRONG!

The MSc in Information Security is now twenty years old, being one of the first such programmes worldwide. Embarrassingly, however, we have never established exactly how many students have successfully graduated from the programme. Nor have we ever determined precisely how many different countries they have come from. Is it 1500 graduates from over 50 countries? Is it maybe even 2000 graduates from 60 countries?

We were thus very pleased to discover that when this surprisingly difficult information was finally computed, thanks in no small part to the efforts of Lynne White, the latest tally is over 2500 alumni from more than 100 countries. This is a statistic which the whole of the Information Security Group is incredibly proud of and is a testament to the ongoing efforts to maintain this as the number one masters programme in its field. Adding to the list of countries is getting harder, but 3000 alumni is firmly in our sights...

Q. CAN YOU CRACK THE ENIGMA CODE?

A. YES, BUT IT'S GOING TO TAKE SIX YEARS

It started back in 2006 when the ISG was contacted by Richard Belfield with an intriguing project: to set a series of puzzles to be interleaved with the chapters of Richard's book "Can You Crack the Enigma Code?" (Orion, ISBN-10:0752875264). An ISG team was formed, a series of six puzzles of increasing difficulty were set, a website and online discussion forum was built, and the book was published.

The original prize from the publisher Orion was a Genuine WWII Enigma machine. Unfortunately nobody managed to crack the puzzles before Orion's deadline expired, and the prize was withdrawn. Eventually, the machine was sold off in order to market the latest instalment of some footballer's autobiography.

However, an international team of four determined code breakers, three from England and one from the USA, never gave up. Six years later, they have finally broken all six puzzles; an extraordinary feat of collective intellectual firepower, creative thought and dogged perseverance.

Dan Fretwell, one of the successful code-breaking team, takes up the story:

"As a 17-year-old teenager I was interested in many things that were quite distant from the interests of a standard teenager. I loved puzzles, mathematics and cryptography (although I was only an amateur at breaking ciphers). I first learned about the book `Can you crack the enigma code' from the BBC puzzle magazine `Mind games'. In fact I won a competition in that magazine and my prize was a signed copy of the book."

"When I received the book around the date of publication, it didn't take me long to read it. I already had a bit of knowledge about most of the unsolved ciphers mentioned in the book but what intrigued me the most was the competition. The idea was simple: break the ciphers, solve the riddle and win an Enigma machine! At the time, I was a high-ranking player of the hit ARG Perplex City and so it was natural for me to want to invest some amount of time on these six seemingly harmless ciphers. However, these ciphers were not harmless; they were skillfully crafted by a team of experts from the ISG (Carlos Cid, Jason Crampton, Laurence O'Toole and Kenny Paterson). Their difficulty became more and more apparent the longer I spent on them."

"Six long years later and the trail has finally been slain through the use of lots of persistence and patience. I did not go it alone though, I was part of a team (consisting of me, David Dack, Mark Armitage, Robert Matson and Robert Dickson... four people who I had never met!). We each decided to collaborate through the online forum provided by the ISG."

"Each of us worked through the first three ciphers independently but joined forces for the final three ciphers. Incredibly, every member of the team has provided a vital contribution at some point in the trail. I myself exploited certain patterns in cipher five that led me to its solution in the realms of music. I was also credited as being the annoying guy that begged for clues from the code-setters (often receiving a polite 'no' in return) and as being the most persistent guy on board. I managed to keep the team together and working on this even through times when we drifted apart."

"Although the prospect of winning an Enigma machine was long gone, we were still happy to continue towards a solution and, as a nice treat for solving their puzzles, both the author and the code-setters invited the team to dinner. It was a great evening, and strong evidence that hard work can induce pleasure..."

"As closing words I can recommend this trail to anyone with a love of challenges. For not wanting to spoil the solution I cannot mention exactly what these ciphers entailed, but I can mention the existence of a 63-letter anagram, many pangrams and a musical theme. Good luck..."

Step forward and take a bow: Dan Fretwell, a PhD student in Mathematics from Sheffield, Mark Armitage, a semi-retired organic chemist, David Dack, a retired research lab manager at Hewlett-Packard, and Robert Matson, a space scientist who lives and works in California.

The solutions to the Enigma puzzles will remain secret for now, so that future generations of puzzlers can also pit their wits against this challenge. However, here are the first couple of puzzles from the series, to whet the appetites of aspirant code-breakers:

Puzzle 1:
WKHFLSKHUWHAWLQWKHQHAW
SXCCOHLVDPBVWHULRXVDQG
ODUJHDQDJUDP(WKHSODLQW
HAWPDBSURYHXVHIXOLQVRO
YLQJVXEVHTXHQWSXCCOHV)

Puzzle 2:
ALAN TURING, ENIGMA, VISIONARY,
EXPOSES THEIR HARD ROTOR CODE,
FOR IT HALTS WAR.

Full details of all the puzzles can be found in Richard's book and at the Enigma puzzles website: enigma.isg.rhul.ac.uk

SHORT NEWS BITES

The ISG was delighted to host the 23rd HP Colloquium on Information Security on the 20th December. Attendees enjoyed three excellent talks as well as great networking opportunities. John Madelin (Verizon) spoke about 'The Business of Security', giving an overview of the role of security within a large business environment. James Lyne (Sophos) provided a highly interactive and entertaining look at recent trends in contemporary cyber crime. David McGrew (Cisco) presented a thoughtful critique of quantum key distribution. We are, as always, very grateful to HP for sponsoring this extremely successful event.

The ISG hosted InTrust 2012, the 4th International Conference on Trusted Systems, on 17th and 18th December 2012. This was the fourth in a series of conferences focusing on the theory, technology and applications of trusted systems. Prof. Chris Mitchell and Dr Allan Tomlinson from the ISG were co-chairs together with Dr Liqun Chen from Hewlett Packard.

Dr Gerhard Hancke was invited to present on the topic of NFC security at the recent European Electronic Crime Task Force (EECTF) plenary meeting, which focused on the security of innovative payment systems. This event was held at the headquarters of Poste Italiane on the 29th of November in Rome, and was attended by around 120 participants representing 50 organizations from 8 different countries. The EECTF is an initiative founded in 2009 by Poste Italiane, the Italian Postal and Communication Police and the United States Secret Service to share information amongst a wide community of organisations that play a leading role in countering cyber crime.

Dr Carlos Cid was one of the invited speakers at the ECRYPT II AES Day event, held on 18 October 2012, in Bruges, Belgium. The event, to commemorate the 10th anniversary of the AES standard, was organised by ECRYPT II - European Network of Excellence in Cryptology, and featured historical talks on the design and selection process, as well as more recent work on security and implementation. The list of speakers also included Miles Smid, David Naccache and Joan Daemen (co-designer of the AES and of the recently selected SHA-3 hash function algorithm).

Professor Kenny Paterson from the ISG was one of the invited keynote speakers at the 9th edition of EuroPKI which took place in Pisa, Italy on September 13th and 14th 2012. The workshop, which is associated with the premier annual European security conference ESORICS, deals with all aspects of research into Public Key Infrastructures. Kenny's talk, entitled 'Key Reuse in Public Key Cryptography: Theory and Practice' covered a range of issues in key management and cryptographic security arising from the common practice of using public keys in multiple algorithms. In this talk, Kenny reported on his recent research on the security of key reuse in EMV, the global de facto standard for payment cards.

Researchers from the ISG have been selected by intelligence agency GCHQ and EPSRC to use their expertise to form part of the UK's first academic Research Institute to investigate the "Science of Cyber Security." Royal Holloway was selected along with three other universities, University College London, Imperial College and Newcastle University following a tough competitive process. The new institute will bring together a diverse set of interdisciplinary researchers to tackle cyber crime and make the UK more resilient to cyber attack. The collaborative team will focus on driving forward the basic understanding of how to assess the relative security of an enterprise system – including its constituent technology, people and processes – and the effectiveness of different mitigation strategies. There will be a particularly strong emphasis on the human behavioural aspects of security.

Dr Konstantinos Markantonakis was one of the invited keynote speakers at the 8th edition of RFIDSec which took place in Nijmegen, The Netherlands, on July 1st – 3rd 2012. RFIDSec is the earliest workshop devoted to security and privacy in Radio Frequency Identification (RFID). Starting in 2005, RFIDSec is today the reference workshop in the RFID field with participants from all over the world. RFIDsec aims to bridge the gap between cryptographic researchers and RFID developers through invited talks and contributed presentations.

The ISG attended the 2012 Information Security Forum (ISF) Congress held in Chicago in November (the last day coinciding with the re-election of President Obama). Visiting Prof. Whitfield Diffie gave an invited keynote, outlining some of the important challenges from computer science that system designers and builders have had to overcome, and how these have translated into vulnerabilities in real world systems. Dr Geraint Price gave a member presentation which outlined the early findings of the ISG's Cyber Security Club.

SPACE PROJECT: Many organisations are moving their infrastructure to `The Cloud'. This poses some interesting security, and legal, questions depending on the particular cloud configuration adopted. One area of interest to researchers at the ISG is that of cloud storage and data sharing. The ISG, as a member of a consortium led by technology company Thinking Safe Limited and including design company Wax RDC, has recently won funding from the Technology Strategy Board's `Innovating in the Cloud' competition, for a project to make information storage more secure for people using cloud computing.

The Service Protection and Acceleration into the Cloud for Enterprise (SPACE) project has ambitious goals and seeks to design and develop a national infrastructure for enterprise data protection, which will enable the UK to establish a leading role in the international cloud services industry. Co-ordinated by Allan Tomlinson, the ISG's role in this project is to provide a threat analysis of the proposed scheme and subsequently develop protocols to allow secure data sharing between users of the service.

RECENTLY COMPLETED PHD THESES

Qin Li
Design and Analysis of Electronic Feedback Mechanisms

Raja Akram
User Centric Security Model for Tamper-Resistant Devices

Muntaha Alawneh
Mitigating the Risk of Insider Threats When Sharing Credentials

Julia Novak
Generalised Key Distributions Patterns

Haitham Al-Sinani
Managing Identity Management Systems

Elizabeth Quaglia
Anonymity and time in public-key encryption

Penying Rochanakul
Protecting Digital Copyright with Fingerprinting Codes and Separating Hash Families

CONFERENCES HOSTED BY THE ISG

Prof. Chris Mitchell was General Chair of IFIP IDMAN 2013, the 3rd IFIP WG 11.6 Working Conference on Policies & Research in Identity Management, which was hosted by the Information Security Group on the 8th and 9th of April 2013 - see idman2013.com. IFIP IDMAN 2013 was the third in a series of conferences focusing on the theory, technology and applications of identity management. The two previous conferences (IFIP IDMAN 2007 and IFIP IDMAN 2010) were held in Rotterdam, The Netherlands and Oslo, Norway, respectively. IDMAN 2013 was co-located with a workshop organised by the EPSRC-funded Future of Identity Network of Excellence.

ESORICS (European Symposium on Research in Computer Security) is the premier European research conference in computer security. ESORICS started in 1990 and has been held in several European countries, attracting an international audience from both the academic and industrial communities. ESORICS 2013, the 18th symposium in the series, will be held in the UK at Royal Holloway, University of London. ESORICS has not been hosted in the United Kingdom since 1994, when it took place in Brighton, and has never been hosted by Royal Holloway. The conference will take place in early September. Prof. Jason Crampton is co-chair of the Programme Committee alongside Prof. Sushil Jajodia of George Mason University, one of the world's most prolific and experienced researchers in computer security. Prof. Keith Mayes is chair of the Organizing Committee. Further details are available from the conference web site http://esorics2013.isg.rhul.ac.uk/ or contact esorics2013@rhul.ac.uk. The organisers would be very interested to hear from potential sponsors.

Dr Carlos Cid is joint Programme Chair and General Chair of Fast Software Encryption (FSE) 2014, to be held in Central London in March 2014. FSE is one of the International Association of Cryptologic Research flagship events, and over 150 participants are expected to meet to discuss the design and analysis of fast and secure primitives for symmetric cryptography. The ISG has a long history of expertise in this area, and Carlos and his research student Gordon Procter received the best paper award for their paper *On Weak Keys and Forgery Attacks against Polynomial-based MAC Schemes* at FSE 2013 in Singapore.

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
F: +44 (0)1784 430766
E: isg@rhul.ac.uk
W: www.isg.rhul.ac.uk/isg