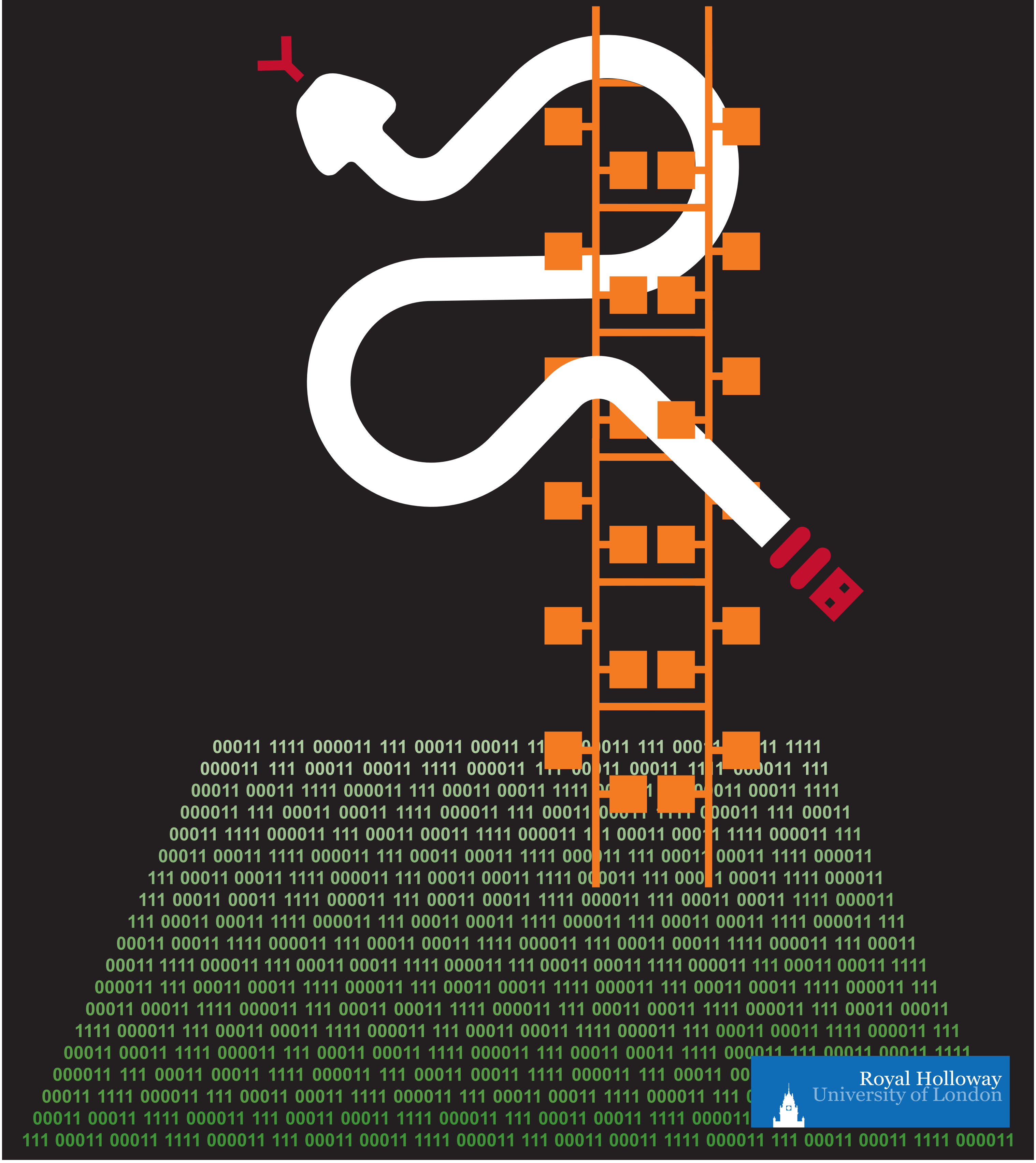
Information Security Group

Review 11/12



Royal Holloway
University of London

LETTER FROM THE ISG DIRECTOR

It is a pleasure to introduce you to our latest annual review. If you are an existing 'friend' of the ISG then I hope you will enjoy finding out about some of our latest activities and adventures. If you are a prospective 'new friend' then I hope that you will get a good overall impression of what the ISG is all about from the various articles in this edition.

We are an 'Information Security' Group and the world seems to have gone 'Cyber Security' mad in the last few years. I am delighted that Geraint Price has stepped up to the mark in this newsletter and addressed the important question as to whether these terms mean exactly the same thing! We have no plans to become a 'Cyber Security Group', but it is fairly safe to say that 'Cyber Security' is very much what we do. We are making several important changes to our MSc Information Security programme this year and one of these, which you can read about in the newsletter, is the launching of a new module dedicated to what we believe 'Cyber Security' to be about.

Elsewhere in the newsletter you will find information about many of the current research projects that are running in the ISG, ranging from securing future energy networks, location-based services, contactless smart cards, through to the latest news from Kenny Paterson's exciting project bridging the theory and practice of cryptographic protocols. I am also delighted to highlight Ian McKinnon's review of the various information security professional bodies that are out there vying for your membership. Personally, I have always found the array of options particularly confusing, so Ian's overview is most welcome.

This year we welcome ISG alumni and current students to our June celebration of twenty years of running an MSc in Information Security. It promises to be a special event. We also launched a new partnership with GCSEC in Rome, where the MSc ran in block mode in Italy for the first time this year. There is never a dull moment when it comes to our teaching activities.

So please enjoy the newsletter and do not hesitate to get in touch with us if you wish to get involved with the ISG through any of our range of activities and interests. We would be delighted to hear from you.

Professor Keith Martin

SHORT NEWS BITES:

Goodbye to Alex: At the end of June, the ISG said goodbye to Dr Alex Dent, who will be well-known to many past students of the Standards and Evaluation Criteria module. Alex conducted highly-respected research into public-key algorithms and protocols, and has moved on to a position as a Security Engineer for Qualcomm in San Diego.

Alex has made substantial contributions to the ISG during his many years here. He has been very actively engaged in the cryptographic research community and has helped to fly the Royal Holloway 'flag' through his research papers and books. He has also consistently been one of our most popular lecturers.

Alex paid tribute to his time with the ISG: *'I don't think it's possible to overestimate the effect of my time at Royal Holloway. I came here as a young mathematician and Royal Holloway taught me the technical skills needed to become an information security professional. I firmly believe that this is the best academic information security group in the world, both professionally and personally, and I'll miss everyone here more than I can say'.*

ISG researchers Nadhem AlFardan and Kenny Paterson have jointly won the best paper award at the 2012 Network and Distributed System Security Symposium (NDSS 2012), held in San Diego, California. The award, sponsored by Google, was given for *'outstanding contributions in the field'* and relates to Nadhem and Kenny's paper 'Plaintext-Recovery Attacks Against Datagram TLS'. Their work has already lead to new versions of the code being released by OpenSSL and GnuTLS.

The ISG have been awarded a grant by Intel to deliver a new module as part of the MSc in Information Security. The proposed course will inform future security professionals, on one hand, about the economic tools that address some of the needs for quantitative methodologies; and on the other hand about methods to include security into economic and business analyses.

Prof. Keith Mayes was invited to visit Peking University (PKU) in September 2011 and gave a guest lecture as part of an autumn school run by the College of Engineering.

Academics from the ISG presented two papers at the special invitation-only New Security Paradigms Workshop in Marin County in September 2011. Dr Lizzie Coles-Kemp co-authored a paper that *'describes a security policy design approach that is sensitive to subcultures within an organisation and uses both policy design and policy implementation approaches to integrate security policy at a sub-cultural level'*. Prof. Dusko Pavlovic *'sketched a framework to measure the value of security by obscurity in games of incomplete information'*.

Prof. Chris Mitchell was a keynote speaker at EuroPKI 2011 (8th European Workshop on Public Key Infrastructures, Services and Applications) in September 2011 in Leuven, Belgium, giving a talk entitled 'New architectures for identity management – unifying security infrastructures'.

Royal Holloway celebrated the 125th Anniversary of the founding of Royal Holloway College with a dinner at the Royal Society in London. The theme of the evening was on Royal Holloway's many links with business, politics, media and the public and voluntary sector.

The Information Security Group was proud to host a table of representatives from our own extensive network of external connections, which included James Quinault (Director of the Office of Cyber Security and Information Assurance), the Rt Hon David Blunkett MP, Dr Richard Pinch (GCHQ), and Sir Edmund Burton (Chairman of the Information Assurance Advisory Council).

Prof. Fred Piper has been awarded an Honorary Fellowship by Royal Holloway, University of London. Honorary Fellowships are awarded to those people who have made an outstanding contribution to Royal Holloway and to society at large.

The ISG is a sponsor of the Cyber Security Challenge, which is a series of national competitions that test cyber security abilities. The ISG contributes expertise in the development of the competitions, as well as providing prizes. Allan Tomlinson attended the Award Ceremony on 11th March 2012 and was delighted to award a place on our MSc Information Security as well as some places on block mode modules to some of the winners.

ISG AND IISP – NATURAL PARTNERS
Prof. Keith Martin

> Prof. Keith Martin is Director of the ISG.

The Information Security Group is delighted to announce that Royal Holloway has been confirmed as one of the first four academic partners of the Institute of Information Security Professionals (IISP). This award recognises the significant base of security-related expertise and activity that exists within the ISG and aims to nurture a culture of collaboration and information security professionalism between the IISP and Royal Holloway staff and students.

There are two reasons why this is very good news.

The first is that we are in the same game. Information security is not a subject that students tend to study solely for entertainment or intellectual stimulation. While there are corners of the subject space where this might be true to an extent (cryptography springs immediately to my mind), the vast majority of information security students come to academic institutions in order to get a broad education in the fundamental issues that matter concerning the practice of information security. And the reason they want that knowledge is to obtain a decent job at the end of their course of study. In other words, if they are not already, they aspire to become information security professionals. The IISP aims to professionalise the industry and we train upcoming information security professionals. It is obvious that we should work on this project together.

The second is, simply, that this type of partnership works. Royal Holloway has trained information security professionals for over thirty years and has run our leading masters programme in this area for twenty. During this time over 2000 students have passed through the institution, the vast majority of who are now information security professionals. We certainly did not do this on our own. From the outset, Royal Holloway's academic offerings in information security have been designed with the input of, taught with the assistance of, and reviewed using the expertise of the Information Security Profession. In order to keep our programmes relevant and informed, we have worked with a large community of information security professionals, of which the IISP is a welcome embodiment. Some of the benefits of the Academic Partnership programme are ones that we have been dining on for years, and we highly recommend them.

The ISG looks forward to a close ongoing relationship with the IISP in the years to come.

INFORMATION SECURITY CAREERS SEMINAR

In spring 2012 the ISG launched a new seminar series devoted to careers in information security. The programme was put together by Visiting Professors Paul Dorey and Richard Walton, who between them have extensive experience of careers in both the private and public sectors.

Each week of this series was devoted to a particular career theme and featured presentations from practitioners who are currently working in that sector. Themes included financial services, roles in government, security consultancy, research and development, service providers, the role of the CISO and professional bodies.

Each speaker was asked to talk about not just security roles, but also the speaker's own career path and their personal perspectives. The speakers came from a wide variety of organisations and ranged from senior professionals reviewing different security roles through to recent recruits discussing their experience of recruitment and establishing themselves in their new jobs. Overall it presented a fascinating glimpse of the information security career landscape and what working in information security is really like.

The main impressions that emerged from the seminar series were just how diverse a range of security roles exist in the job marketplace and, equally importantly, how varied the range of tasks is within these roles . Almost all of the speakers, when asked what they liked most about working in information security, commented on the fact that no two days were the same. They enjoyed waking up each morning knowing that they could not predict which challenges they would be faced with when they connected with work that day.

Richard Gorman, a current MSc Information Security student, found the careers seminar series extremely useful: *'These seminars put us in touch with practitioners who are very knowledgeable about the latest activities within Information Security. The breadth of expertise was great – a mix of commercial, industrial and government representatives. This seminar series was a real highlight for me'.*

The ISG is extremely grateful for all the security professionals who gave up their time to come to Royal Holloway and talk about their working lives and the opportunities that exist for new entrants.

DISTANCE LEARNING CATCH UP
By Colin Walter

> Dr Colin Walter is Programme Director for the Distance Learning MSc Information Security.

Despite increasing competition over the last few years from similar degrees at other universities, the Royal Holloway distance learning MSc Information Security continues to attract large numbers of students. I believe that this is due to its prestige and the fact that it is built on a sound understanding of commercial needs. It is also hugely beneficial that there is a vast network of alumni which provides graduates with opportunities for keeping up to date with developments in the industry and for career advancement in a challenged global economy.

The distance learning version of the degree has a regular intake of around 50 new students per year, 40% of whom are based in the United Kingdom and the remainder scattered fairly uniformly around the world. The majority of students combine their studies with a full time job and take between three and four years to complete the MSc.

The widening need to obtain appropriate qualifications in the subject before being hired has meant that the average age of new students has been decreasing every year. On average, the intake has been a year younger on each successive session over the history of the degree! In recognition of the consequently lower incomes of students, we took the unusual step of reducing the cost of the degree by 10% in 2011.

The demand for qualifications also extends to continued professional development. As alumni have only taken two optional modules as part of their original degree, and due to the recent addition of modules on smart cards and digital forensics, it was decided to offer past students the opportunity to take more of the many options available at a specially reduced rate. We expect that this will continue in the future and hope that it provides a useful service for our graduates.

The past year has seen several personnel changes on the distance learning MSc. A highlight has been having our own new dedicated administrator and we welcomed Claire Hudson to this post in July 2011. We wish the previous (shared) administrator Daniel Miller well as he continues to support activities in the School of Management. Other changes have included the stepping down of several module leaders, including Mick Ganley who oversaw two modules and was programme director for a number of years. The new module leaders include both internal and external appointments to continue the mix of academic and industrial backgrounds which is so essential for developing and teaching a degree of relevance to the commercial sector.

The highlight for many of us was the annual weekend conference in September. Although directly targeted at current students and for those about to start their information security studies, past graduates are also very welcome to attend. This year a packed lecture theatre listened to superb talks on a wide range of topics from gifted speakers, mostly based in industry. Fortunately, a number of these were recorded for posterity and are available on YouTube. They can be viewed by visiting http://www.youtube.com/user/UniofLondon and then searching that channel for ‘Information Security’.

NEW TRACKS AND MODULES FOR THE MSC INFORMATION SECURITY

We are making some changes to the content of the MSc in Information Security which will apply from the beginning of the 2012/13 academic year. These changes are part of the continuous process of reviewing and updating the MSc programme.

Currently, MSc students take either a Technical Pathway or a Secure Digital Business Pathway through the MSc programme. We will be replacing this concept with a new notion of 'tracks'. Whether or not a student chooses to register for a track is entirely optional. If a student does register for a track, then (a) the name of the track will be recorded on the student's degree transcript, and (b) the choices of core and optional modules and the project topic will be restricted to ensure that the set of courses taken matches the name of the track.

The purpose of tracks is to enable students to obtain a more specialised version of our MSc if desired and, optionally, to have this explicitly stated on their transcript. We are currently planning to have six tracks, with the following titles:

- Secure Digital Business
- Cybercrime
- Cyber Security
- Digital Forensics
- Smartcards and RFID/NFC
- Security Testing

For example, to obtain recognition under the Cybercrime Track, students will be required to take the specific optional modules on Cybercrime and Digital forensics, as well as conduct their MSc project in the area of cybercrime.

We are also making changes to the extensive portfolio of MSc modules. The current core module on the existing Business Pathway on Legal and Regulatory aspects of Electronic Commerce, taught by Robert Carolina, will become an optional module available to all students. This will, we hope, enable more students to access this excellent course. A new core module will replace it, focussing on organisational security architectures.

In addition, we will be introducing two new optional modules on Economics and Security, and Cyber Security. These will replace the modules Application and Business Security Developments and Standards and Evaluation Criteria, with some of the content of the retired modules making its way elsewhere.

The essential elements of the MSc Information Security remain unchanged, but we feel that these refinements will help to maintain the standing of this flagship MSc programme for the years to come.

A NEW CYBER SECURITY MODULE
By Stephen Wolthusen

> Dr Stephen Wolthusen is a Reader in the ISG.

High-value systems and networks may face threats at a number of different levels, including ones where an adversary may seek to target indirect effects resulting from the degradation or compromise of a target. Understanding the nature of such threats and their targets both at the macroscopic, and for selective threats also at more detailed levels, is one of the objectives of a brand new module on Cyber Security, due to be launched later this year.

In approaching this problem space, identifying dependencies and resulting attacks and failures is an important tool in prioritising the limited resources available for defence, whilst also helping to understand the robustness of critical systems and networks up to and including critical national infrastructures and their interconnection. This new module will provide an overview of different approaches to the study of such dependencies.

As many critical infrastructure sectors such as energy rely on linking information and physical systems together into cyber-physical systems, and these interconnections are increasingly commonplace in many areas, particular attention is paid to such cyber-physical systems and the types of attacks that are becoming possible. To this end, key concepts from control systems theory on the one hand and the problems encountered in supervisory control and data acquisition (SCADA) systems are highlighted.

The module will also focus on the abilities of more advanced adversaries, including attacks that combine multiple stages and techniques ranging from social engineering to host- and network-based approaches, sometimes also referred to as Advanced Persistent Threats. As it is difficult to assess the actual threat resulting from such adversaries, this requires the study of risk and attack models.

High-value systems require a formal assessment of their assurance and ultimately their suitability to address the risks and threats. The module will also assess frameworks for information assurance certification and accreditation.

If you are interested in the security of high-value systems and the security of national infrastructures then this is a module that you cannot afford to miss!

CYBER SECURITY: PLUS ÇA CHANGE
By Geraint Price

> Dr Geraint Price is Lecturer in the ISG.

What is Cyber Security? Is it the same as Information Security? Is this what we used to call Information Assurance? These questions have increasingly surfaced over the past few years as the concept of Cyber Security has found more frequent usage. Royal Holloway has an Information Security Group – is that the same as a Cyber Security Group?

At its heart, we believe that Cyber Security is no different to much of what has gone before. With each new iteration and wave of reinvention in this, and other disciplines, there is much that is the same as before. However, the subtleties and complexities also force us to think of the things we already know in a new light.

As a term, Cyber Security clearly has two component parts: ‘Cyber’, implying something to do with the ethereal term ‘Cyberspace’; and ‘Security’, which is something we are all more familiar with in its various guises. The key issue we believe is that the ‘Security’ element has not really changed from previous incarnations.

The desire to provide security services (be it a blend of confidentiality, integrity, availability, and many other exotic variants) is still the same. So is there any novelty in the ‘Cyber’ element? When discussing Cyber-anything, it is tempting to imagine a somewhat utopic hyper-connected future world where every online wish can be met by a simple command. To an extent we already live in such a world, as the last twenty years (depending on which variant of the Internet you take as your starting point) has seen a transformation of the landscape of services and applications that we might realistically label as ‘Cyber’. However, the reality is that much of what is now delivered in a Cyber-environment has been around in some form throughout most of these last twenty years, in some cases much longer. Yes, the connectivity has increased. Yes, the number of services, devices and users present on the Internet has increased. Yes, the range and sophistication has increased. But the basic service framework within which all of this Cyber-activity operates has been around for most of these twenty years.

However, there is something significant that has changed: the rate at which all of the developments previously mentioned have come together to bring change to the average organisation or citizen. While web-based services might have been around for twenty years, the Internet has fast become irreplaceable for a large percentage of the world’s citizens, rather than simply being a plaything of the early adopters. This on its own has not changed the importance of Information Security / Cyber Security / Information Assurance. It has, however, changed its profile.

The key thing we believe is that these changes have brought to the foreground the need for more resilient and more context-aware security services. The sheer volume of interactions which we might now like to protect is astonishing. In addition, the speed at which the attacker can adapt to a new defensive mechanism, or deploy a multi-phased attack, is something which was previously unexpected. There has always been an arms-race between defender and attacker. The key difference now is that the pace of development can be measured in days or hours, rather than months or years.

Another key change is the more open role which governments are playing in this area. Note the ‘Cyber Security Strategy’ of the UK Government for one, and the term ‘Cyber War’ being touted amongst defence strategists as another. The fact that most nation states are now clearly aware that their National Infrastructure could be attacked with a non-ballistic weapon is certainly something new.

So, is there anything new in the term Cyber Security? At its core, probably not. However, as with all of these things, the devil is in the detail, and the detail in this case relates to a Cyberspace that is growing and evolving at unprecedented speed.

While there may be some technical differences between definitions of Information Security, Information Assurance and Cyber Security, we believe that there are very few substantive differences. Those that do exist apply to how we use our tools in any particular context. The key points we raise above (the pace of change, the breadth of impact, etc.) highlight the difficulty in applying these tools intelligently in a broader set of contexts. What this suggests is that refining the use of our tools, and recognising how difficult that can be, is what we should currently be concentrating on.

THE ISG’S NEW SECURITY MANAGER
By Lizzie Coles-Kemp

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

The security management module has been quietly evolving for quite some time and changes this year are part of that process. Five years ago I was invited to work with Peter Wild (who was then leading the security management module) to develop both the support model and the curriculum content of this module. I had already helped develop these areas on the distance learning MSc programme but had no experience of campus-mode delivery. It was a great learning experience working with someone as experienced as Peter. He had the foresight to recognise that what was needed was not the teaching of a particular view of security management, but a set of thinking tools that students could develop during the module which would help them to resolve the multi-faceted socio-technical security management problems out in industry. As a result, we designed a framework of assignments through which students could build these skills and we started to link those assignments to the material taught in each of the lectures. The framework was then subsequently refined with several cohorts of students. This framework now sits at the centre of the security management module in all its modes of delivery.

Peter has now retired and, after an interim year, I now lead the module myself. The module remains committed to the vision of academia and industry in partnership and its focus is still the real-world security problems faced by security managers. We still work with external speakers, although I do give a few more module lectures than my predecessors have done. As a subject, the teaching of security management better lends itself to co-creating knowledge with students than it does to knowledge transmission. The external speakers deliver lectures on this module that are as much about challenging students’ perceptions of security management as they are about informing students of security management functions and practices. My primary role as module leader is to help students make sense of these lectures and develop the thinking tools and skills to create their own view of security management. I recognise that we ask the students to work in a very different way than they are often used to on this module and I am very proud of this year’s cohort of security management students. They have admirably risen to the challenge!

SMART CARD CENTRE UPDATE
By Keith Mayes

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

We have had another interesting year in the ISG Smart Card Centre (SCC) and whilst something in my head still says that the SCC is a young part of the ISG, we are in fact in our tenth year of existence! By a rough calculation, since launch we must have produced around 80-100 publications, supervised around 200-250 MSc projects, and introduced 400-500 students to the interesting world of smart cards, RFIDs and implementation security.

The general philosophy throughout the lifetime of the SCC has been of working close to industry and guiding our research projects and lectures in a direction that produces relevant outputs and useful potential employees; this has stayed the same. However, over time the companies that we have the closest interaction with, and the underlying technologies, have changed. We have been delighted to welcome two new sponsors of the SCC in the last twelve months.

The first is Orange Labs (UK), with whom we have started a very positive collaboration. This has included proactive engagement in our project and general research work, which has already led to one joint publication and another in submission. A number of internships with Orange Labs were offered to MSc project students and one PhD student was recruited for a particular Orange project. Orange Labs are now also providing the mobile and over-the-air programming lectures on the smart card MSc module.

We recently also welcomed the newest SCC funding member in the form of the UK Cards Association. Amongst other extremely positive benefits, this also demonstrates that the SCC is now supported across a broad range of important research areas including mobile communications, banking and transport ticketing.

Work in the transport area has also continued with the support of Transport for London and ITSO. We are currently in the process of recruiting a PhD student for a project that is proposed and part-supported by ITSO.

Meanwhile, technology and the business world have been changing. While there are many successful system solutions that use contact smart cards, new systems are tending to be contactless, with a contactless smart card being a particular example of an RFID. There is no rule that says contactless smart cards have to have weak security, but they are often used in fast one-factor authentication systems such as Oyster cards or touch&pay bank cards. RFIDs do not need to keep to the card format and in fact come in all shapes, sizes and capabilities. I was fortunate to be invited to Peking University last year to give a guest lecture and was interested to note that there was very strong interest in the Internet-of-Things, where everything is potentially RFID tagged in some way; although there was less emphasis on security and privacy issues.

In the SCC we are usually interested in smart card and RFID systems that have more advanced functional and security capabilities than simple tags and so we are closely investigating the evolution of smartphones, SIMS/USIMs and the Security Elements used in Near Field Communications (NFC). NFC gives the phone the ability to emulate an RFID, to act as an RFID reader, or to provide a very close range peer-to-peer connection with another phone and some believe that it will eventually replace all the cards in our wallets. There are suggestions that secure processing areas within the phone CPUs could eventually replace the SIM/USIM and/or physical Security Elements. We are also seeing major changes in the mobile business world with the rapid demise of Nokia and the power struggle of Google and Apple along with the mobile phone operators, banks and smartphone manufacturers. The rush for new services, technology, innovation and market domination is not driven by security and so mistakes will be made, but all this makes for a very interesting research outlook for the SCC.

In 2012 we will also be hosting our second international academic conference, the Sixth Workshop in Information Security Theory and Practice (WISTP 2012 http://www.wistp.org/) from 19-22 June 2012.

Please also reserve 11th September 2012 for visiting the 8th SCC Open Day Exhibition. We look forward to seeing you there.

orange™

THE UKCARDS ASSOCIATION

THE CYBER CRIME THREAT ON MOBILE DEVICES
By Chris Mitchell

Prof. Chris Mitchell is Director of Teaching for the ISG.

This article is concerned with highlighting recent and emerging cyber crime threats to mobile devices. The main classes of threat are briefly reviewed, and the history of attacks against mobile systems is summarised. Two case studies of attacks against general-purpose systems not normally thought of as security-sensitive are given, and conclusions are drawn.

01 Introduction – mobile devices

A wide range of mobile devices are in use today, including (smart) phones, media players, tablets, and notebook PCs. These devices are typically network-connected for most of the time they are switched on. This poses a well-known, albeit not well-understood, threat from cyber criminals.

Apart from the 'obvious' mobile devices, a growing number of everyday objects are also 'always/often connected', including road vehicles of all kinds (cars, lorries, etc.), RFID tags embedded in all sorts of devices, chip-based payment cards, including proximity-based cards, electronic key fobs, and public transport vehicles. Of course, these are just the mobile devices – many everyday fixed objects are also rapidly becoming Internet connected, including 'smart' buildings, e.g. shops, restaurants, homes, and workplaces, and installations within buildings, such as domestic appliances and factory machinery.

Of course, traditional mobile devices (such as phones, PCs, etc.) have been the main focus of security and privacy concerns. Whilst there are very major issues for such systems, perhaps other devices pose an even greater threat. It may well be that the possibilities for crime (and countermeasures) involving such everyday devices have not been properly thought through, and this issue forms the main focus of this paper.

The remainder of this paper is structured as follows. The main cyber (and hence cyber crime) threats to mobile devices are reviewed. We then look at how these threats apply to some of the less well-studied classes of mobile device, and the news is not always good. One reason for problems in all categories of mobile devices and systems is that systems have evolved piecemeal, and there is no overall security architecture. As with all IT products, the pressure to release the latest innovation always takes precedence over the need for security. Moreover threats arise from 'accidental' functionality; systems are interconnected because we 'might as well', without thought about the possible consequences.

02 The cyber security landscape

2.1 Threats:

Cyber threats to mobile devices can be divided into two main classes. Communications-based threats include access network impersonation, mobile device impersonation, and man-in-the-middle attacks (both active and passive). System-based threats include software vulnerabilities, side channel attacks, and social engineering attacks (including malicious applications).

The cyber criminal may have many different motives for performing an attack on a mobile device, including hardware theft, information theft, or simply denial of service or sabotage. It is difficult to enumerate all the ways a criminal might seek to gain from an attack; indeed, it is hard to determine where criminality ends and terrorism begins. As a result, it would seem prudent to consider all possible security issues when trying to address cyber crime.

The security measures we can deploy to address possible threats can be divided into two broad sets. In a network we can deploy authentication (of network to device, and device to network), and secure channel establishment. Within a system we can employ a range of techniques, including: secure software design (to reduce the need to patch vulnerabilities), attack surface reduction (to reduce the impact of vulnerabilities), secure hardware/firmware design (to make finding side channel attacks difficult), careful user interface design (to reduce the risk of user error), and user education regarding threats.

Unfortunately, systems designers and manufacturers do not always do a good job of deploying the necessary security measures. With respect to mobile network security, security measures have been applied only very patchily. The industry has often worked in the 'deploy first and then make secure later' mode. Additionally, 'quick and dirty' solutions have been deployed which have often proved inadequate. Certainly there are many well-known vulnerabilities in our mobile networking infrastructure which have yet to be fixed, often because of the huge cost of retrofitting security. In terms of system security, the picture is no better. The first mobile virus was reported back in 2004[5], and more recently huge numbers of vulnerabilities have been reported in smart phone systems (see below).

2.2 Network security

Some currently deployed network access protocols offer very limited security. For example, authentication of the 'access network' to the device is sometimes non-existent, e.g. as in GSM and IEEE 802.11 Wi-Fi. Existing security measures aim at controlling access to the network to protect the investment of the network owners, rather than the serious threat to end nodes posed by unauthenticated access points.

The effects of such a lack of network authentication have been widely documented in print and on the Internet. This situation has given rise to a series of public domain implementations of 'fake network' attacks on GSM and IEEE 802.11, as well as attacks arising from compromised access points, where the compromise might arise from software or hardware attack. There are a host of examples of fake network software, including AirJack and airsnarf. For example, Airsnarf is a rogue wireless access point utility designed to demonstrate how a rogue access point can steal usernames and passwords from public wireless hotspots. A graphic description of how airsnarf could be used to compromise user security is provided on Kewney's blog. Pair-wise device authentication can also be vulnerable; for example the original Bluetooth pairing scheme was rather weak. In general, as a result of the lack of comprehensive and integrated security solutions for mobile connected devices, there is an ever-growing risk of widespread malware attacks, as devices become more 'smart' and flexible. This is all happening in an environment in which malware attacks on mobile devices continue to become more numerous and serious (see below).

Apart from poor security fundamentals, privacy is also a major issue. Device tracking is a particular problem. In any network protocol, addresses of some sort are exchanged between devices, and, at least at some level of the protocol hierarchy, these addresses need to be exchanged in cleartext. If the address of the mobile device is fixed, then this offers a simple way of tracking the location of that device, and by implication, its owner. Of course, work is ongoing to address this problem for a wide variety of protocols, including for mobile networks.

It is not only the protocols used in networks that have proved vulnerable. A range of attacks have been devised against the cryptographic algorithms that underpin these security protocols. For example, WEP (the first suite of algorithms for Wi-Fi) was quickly broken[4], and the replacement suite (WPA) has also been attacked[12] (although WPA2 appears to be robust). A wide range of attacks have been demonstrated against GSM cryptography[1]; this is not so surprising – after all, GSM is 25 years old. However, this is not all ancient history – a very recent announcement from Ruhr University Bochum shows that satellite phones are not immune from simple crypto attacks[3]. These attacks do not arise because of the lack of robust cryptographic technology – it is often about cost pressures trumping security requirements.

2.3 System security

System security problems with mobile devices have been known for some time. For example, the Register reported back in February 2007 that, according to McAfee, 3G malware attacks in mobile networks had reached a new high. Informa had reported that 83% of mobile operators were hit by mobile device infections in 2006, and the number of reported security incidents in 2006 was more than five times as high as in 2005. Even five years ago, 200 strains of mobile malware had been discovered. Since then the situation has got much worse, as more recent reports show. For example:

- Bloomberg reported in April 2011 that, according to Kaspersky, the 'Android mobile-phone platform faces soaring software attacks and has little control over... applications. Applications loaded with malicious software are infiltrating the Google operating system at a faster rate than with personal computers at the same stage in development. [Kaspersky] identified 70 different types of malware in March, [an increase] from just two categories in September'.
- Wyatt, in *'The Lookout Blog'*, reported in May 2011 that *'multiple applications available in the official Android Market were found to contain malware that can compromise a significant amount of personal data. Likely created by the same developers who brought DroidDream to market back in March, 26 applications were found to be infected with a stripped down version of DroidDream [called] 'DroidDreamLight'.* At this point we believe between 30,000 and 120,000 users have been affected by DroidDreamLight'.
- A Sophos report from November 2009 reports on a range of iPhone malware.

2.4 Is this as bad as it gets?

So far we have looked at the traditional notion of mobile systems. These are relatively closed systems, sometimes carefully designed from a security perspective. What's the worst that can happen in such a case? We would expect to see loss of hardware (possibly with a relatively small impact), and loss of user data; clearly such attacks are not good, but the overall impact on society is probably limited. Indeed, organisations can limit the damage by protecting their back-end servers.

However, there is a far more serious emerging threat scenario involving the much larger world of everyday devices with embedded IT functionality and connectivity. We now have always -connected mobile systems which are often thought of as not having major security requirements; they are typically designed without concern about, or knowledge of, security threats. However potentially very serious threats apply: valuable hardware is at risk, and there are even major safety implications.

3 The problem

It is reasonable to ask why we have these serious security problems. Of course the picture is complicated, but the following factors appear to play a major role.

- Perhaps most significantly, there is huge business pressure to market products first and worry about security and the risks of cyber crime second.
- Technology gets used in ways unanticipated by designers (as exemplified by the growth in SMS, and the use of the Internet Protocol in almost every kind of network), which means that initial threat analyses no longer hold.
- Retrofitting security is typically very difficult; indeed, it is sometimes impossible in practice.
- Available 'retrofit' security technology is not used (examples of such 'failed' technology abound).
- Improving security and privacy rarely has a big pay-off to the user (individual or corporate) – except perhaps after the event, i.e. after a major cyber crime event.

There are also conflicting pressures on suppliers of products. Two major security and privacy requirements are the need for high robustness, because of the criticality of IT, and the need for privacy protection, not least because of emerging legal frameworks and user demands.

These requirements often conflict directly with business, technological and social forces, which are inevitably a lot more powerful than security and privacy requirements. Major economic, technological and social factors include increasing complexity, arising from inevitable technological drift and which directly threatens robustness, the increased use of third parties (outsourcing) which makes privacy and security assurance very hard to achieve, and the use of intelligence (sophisticated IT) everywhere, not least to improve flexibility which also directly threatens robustness.

4 Case studies

We briefly examine two case studies of major security issues which have been found in classes of system which are not normally thought of as security products.

4.1 Case study I – remote keyless entry (RKE) systems

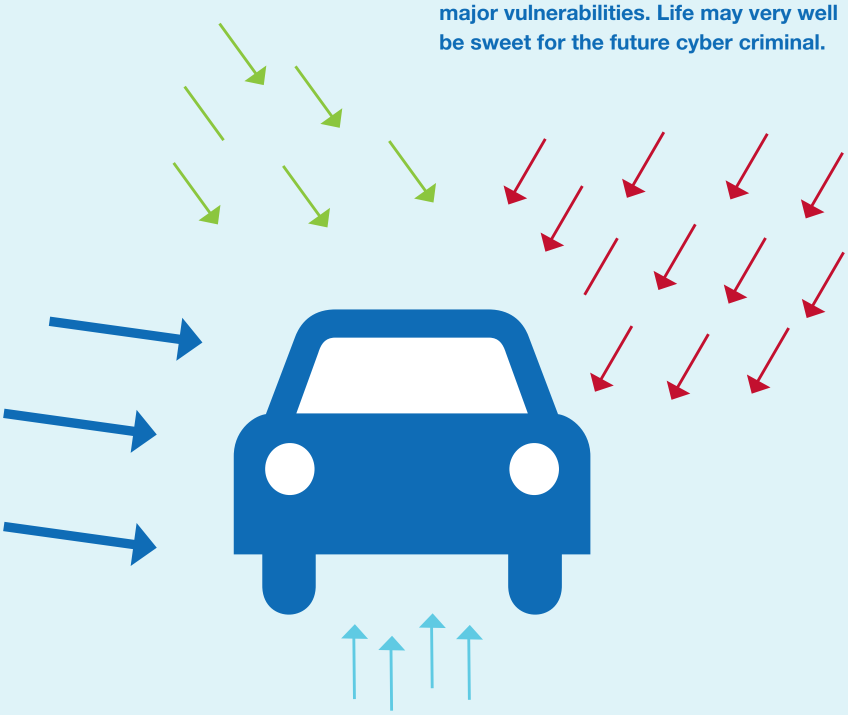
Over the last half dozen years, Paar and his collaborators at the Ruhr University of Bochum have looked at attacks on a variety of real world hardware systems. One system they studied extensively is based on a cipher called KeeLoq. KeeLoq is widely used in remote keyless entry (RKE) systems, as employed for garage door openers and car door systems.

Their work[6,11] reveals a variety of worrying facts. The KeeLoq cipher itself is not terribly strong. However, much more serious is the fact that the design of the key management system is such that all devices for a single system share the same key. Compromising this key (which can be achieved through the analysis of a single consumer device) breaks the entire system. This means that cloned keys could be simply and cheaply manufactured – the possibilities for large scale criminality are clear.

The RKE/KeeLoq attacks were completed a couple of years ago. More recently the Bochum team have successfully attacked a range of other real-world systems, including:

- FPGA security systems, designed to protect the confidentiality and integrity of software[10]; and
- personal wireless systems (including electronic passports, contactless payment cards and RFID systems)[7,8].

The sad lesson from their work would appear to be that almost every real world system they have looked at contains very major vulnerabilities. Life may very well be sweet for the future cyber criminal.



4.2 Case study II – cars

In the second case study we consider recent work of a group of researchers at the University of California at San Diego and the University of Washington (two major papers on this work were published in 2010 and 2011[2,9]). They have performed a detailed study of cyber attacks on cars.

Their attacks have been made possible by the recent evolution of IT in cars. A modern car contains networks of communicating devices (computers/ECUs). These networks control most aspects of a car's operation, including its brakes (and anti-lock mechanisms), gears, throttle, and engine management. Functionality often also includes external connectivity, e.g. including mobile telephony. This gives rise to a large and varied attack surface, including the following elements. In the US, the mandatory Onboard Diagnostics Unit (OBD-II) port provides direct access to the vehicle's internal network. User-upgradeable systems (e.g. audio players) are routinely connected to internal networks. Wireless devices (e.g. Bluetooth) are also connected to internal networks. Finally, and most seriously, remote telematics systems (for safety, diagnostics, and anti-theft) provide continuous connectivity via mobile phone networks.

The team performed experiments using two cars purchased specifically for purpose. They observed that the car's internal CAN bus has little security – any compromised component can impersonate any other component. There are many other security issues.

They demonstrated remote attacks on a car via a broad range of attack vectors, including: mechanic's tools, CD players, Bluetooth and mobile telephony. To perform a mobile phone based remote attack, they reverse-engineered the telematics protocol and used a buffer overflow vulnerability in the car gateway to take over the car telematics unit. This attack works completely 'blind', i.e. without listening to responses from vehicles. Building on this attack they demonstrated the ability to compromise internal vehicle systems, and thereby systematically control the car's engine, brakes, lights, instruments, radio, and locks. The attack could be exploited for theft and surveillance.

Why are such serious attacks feasible (and arguably even easy)? Part of the problem is simply the way the supply chain works. Manufacturers integrate components provided by third party suppliers, and do not even have access to details of how the security functions in the components. That is, they cannot assess the level of security provided, even if they wanted to. This is compounded by the fact that users may add third party systems (e.g. audio players) with serious security ramifications, yet systems are low cost consumer items. Finally, suppliers are subject to serious cost pressures and do not even understand the nature of the cyber threats, since security is not their field of expertise.

5 The way forward

How can we start to address these issues? Perhaps the most serious problem is that we are adding communications functionality, and so serious cyber crime vulnerabilities, and internal inter-connectivity to systems without thinking through the security issues. Manufacturers and users are encountering major security (and cyber crime) problems they have no previous exposure to. There is a serious danger that the sorry cycle of security problems with PCs will endlessly repeat itself with new classes of product.

It seems likely that the situation will get worse before it gets better. This is the usual pattern with new technology that allows ubiquitous connectivity. For example, first generation mobile phone networks had no security functionality, and so a major crime problem arose. Similarly, once the Internet became widely used, PCs and servers were (and still are) subject to many attacks. This pattern is now repeating itself with smart phones, and, more worryingly, looks set to arise with many other consumer products.

Possibly even more worryingly, no-one in academia (as far as I know) has worked on understanding the security properties of public transport systems such as planes and trains (which are increasingly network connected). However, exactly the same issues as arise for cars may well apply in this domain. That is, it is far from clear whether these systems have been designed to counter the kind of adversarial threat mode encountered on the Internet.

How can we start to address these problems? Well, this paper is intended to try to raise awareness of the threat. Producers of systems need to be aware of two main things: security is a problem that cannot be ignored, and getting security right is non-trivial. Perhaps most importantly, security is not just a question of randomly adding some cryptographic functionality.

The good news is that getting security right does not need to be expensive. For example:

- eliminating unnecessary functionality (reducing the attack surface) can solve many problems;
- following good software engineering practices can minimise the risk of buffer overflow vulnerabilities;
- robust crypto and sound security protocols are widely available and standardised.

What can consumers/end users do? Sadly, we must be prepared to pay just a little more for devices which make life harder for cyber criminals. We must put pressure on manufacturers to make more secure products, and on governments to legislate and regulate, where appropriate. At this point it is also tempting to demand that users be less easily duped. However, ultimately, users need to be protected; it seems unreasonable to expect users to become security experts.

Perhaps our best hope in the long run is that governments and regulatory bodies will act. We rely on regulation to ensure that cars, airliners and trains are safe. These regulators need to take on board the new mobile threat – this is a very serious issue! However, a closed *'conformance mentality'* by manufacturers is not always a good thing, and standards alone will not solve all the problems. Anecdotal evidence suggests that FIPS 140 (a US standard for Hardware Security Modules (HSMs) has had a limited effect on overall HSM security. The focus has been on compliance (and addressing issues covered by the standard) possibly at the expense of worrying about security in general. Perhaps FIPS 140 does not focus on the most important issues, but instead on those easiest to standardise.

6 Concluding remarks

There are ways in which disasters can be avoided. However, there do not seem to be any urgent general efforts to fix the problems, although individual manufacturers may be taking significant steps. Certainly, in the past, manufacturers and network operators have been left to clear up the mess they have created. This may be fair, but what happens in the mean time to the victims of cyber crime? Perhaps more general action is required, e.g. from government and regulators?

It is clear that making connected systems secure is non-trivial. It requires specialist expertise and a long-term commitment to adopting state of the art product development practices. However, the technology already exists. What is required is a willingness to address the problem, and also to invest in the expertise required to fix problems before they arise.

This paper is based on a presentation given at the Inaugural Cyber Crime Symposium, held on 1st/2nd March 2012 in Sydney, at which Chris Mitchell was a 'keynote international speaker'.

References

1. E. Barkan, E. Biham, and N. Keller, *'Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication'*. Journal of Cryptology 21(3) (2008) 392-429.
2. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, *'Comprehensive Experimental Analyses of Automotive Attack Surfaces'.* In: D. Wagner (ed.), Proceedings of USENIX Security 2011, USENIX (2011).
3. B. Driessen, *'Eavesdropping on satellite telecommunication systems'*. Draft of February 8th 2012.
4. S. R. Fluhrer, I. Mantin, and A. Shamir, 'Weaknesses in the Key Scheduling Algorithm of RC4'. In: Proc. Selected Areas in Cryptography 2001, Springer (2001) pp.1-24.
5. M. Hypponen, *'Malware goes mobile'*. Scientific American (November 2006) 70-77.
6. M. Kasper, T. Kasper, A. Moradi, and C. Paar, *'Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed'*. In: Proc. AFRICACRYPT 2009, Springer (2009) pp.403-420.

7 T. Kasper, D. Oswald, and C. Paar, *'Wireless security threats: Eavesdropping and detecting of active RFIDs and remote controls in the wild'*. In: Proc. 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2011).

8. T. Kasper, D. Oswald, and C. Paar, *'Security of wireless embedded devices in the real world'*. In: N. Pohlmann, H. Reimer and W. Schneider (eds.), Securing electronic busibness processes, Vieweg (2011), pp.1-16.
9. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, *'Experimental Security Analysis of a Modern Automobile'*. In: Proc. IEEE Symposium on Security and Privacy 2010, IEEE (2010) pp.447-462.

10 A. Moradi, A. Barenghi, T. Kasper, and C. Paar, *'On the vulnerability of FPGA bitstream encryption against power analysis attacks: extracting keys from xilinx Virtex-II FPGAs'*. In: ACM Conference on Computer and Communications Security 2011, ACM (2011) pp.111-124.

11. C. Paar, T. Eisenbarth, M. Kasper, T. Kasper, A. Moradi, *'KeeLoq and Side-Channel Analysis – Evolution of an Attack'*. In Proc. FDTC 2009, IEEE (2009) pp.65-69.
12. E. Tews and M. Beck, *'Practical attacks against WEP and WPA'*. In: Proc. ACM WISEC 2009, ACM (2009) pp.79-86.

Web Links 2.2
http://en.wikipedia.org/wiki/Snarfing
http://sourceforge.net/projects/airjack/http://airsnarf.shmoo.com/
http://www.newswireless.net
http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/

Web Links 2.4
http://www.theregister.co.uk/2007/02/12/mobile_malware/
http://www.techshout.com/mobile-phones/2007/15/83-per-cent-of-global-mobile-operators-have-been-hit-by-mobile-device-viruses-reveals-mcafee-report/
http://www.bloomberg.com/news/2011-04-21/google-s-android-system-faces-more-app-attacks-in-new-security-frontier-.html
http://blog.mylookout.com/blog/2011/05/30/security-alert-droiddreamlight-new-malware-from-the-developers-of-droiddream/
http://nakedsecurity.sophos.com/2009/11/23/lightning-strikes-iphone-malware-malicious/

THE EVOLUTION OF THE INFORMATION SECURITY PROFESSION
By Richard Walton

> Prof. Richard Walton is a Visiting Professor with the ISG.

This year Paul Dorey and I arranged some seminars for the MSc students at which information security professionals from a range of organisations have talked about their careers and experiences working in a variety of infosec-related disciplines and given pointers to the future employment opportunities. This article is based on the introductory presentation that I made outlining the evolution of information security as a profession in its own right.

Before about 1970, information security was not really recognised as a category. Mainstream security was concerned with physical security and personnel security. Within government this was seen very much as the province of the Security Service (MI5), the police or the armed forces. Good practice and policy were developed in those institutions and in the private sector most security practitioners were recruited from those with a military or police background. Information Security (the term had not yet been coined) occurred as document security and communications security. Document security was part of mainstream physical security and was basically the set of policies and procedures for identifying, labelling and controlling physical documents containing sensitive information.

In these days communications security (Comsec) was a highly specialised subject – and at that time was mainly concerned with cryptography. Comsec was a government monopoly in most countries including the UK. Ever since the founding of the Government Code and Cypher School (GC&CS - later GCHQ) after the First World War, the logical design and evaluation of cryptography for UK Government (i.e. military and diplomatic) applications was vested in that organisation. The associated engineering design was undertaken by the post office or military laboratories with volume production under classified contracts in appropriately cleared industrial organisations. Until 1972 British companies were not allowed to produce crypto other than under the auspices of the Government.

At first Comsec in GC&CS was a bit of a 'Friday afternoon' activity and was not taken very seriously. There was very little private sector interest in using cryptography and the governments of most of the leading industrial nations maintained a similar monopoly to the UK. Enigma had started life as a commercial development but failed in the marketplace and owed its later success to the takeover by the German Government. One private company (Crypto AG) was founded by a Swede (Boris Hagelin) and established in Switzerland. Crypto AG traded on its status as being from a neutral country and sold its products to governments – especially (but not exclusively) to those without their own crypto capabilities. In the 1930s this included almost everyone and a major lifesaver for the company was winning a massive order from the US military for their M209 cipher machine which provided tactical security throughout the US army in World War 2.

After 1945 the UK and GCHQ took Comsec much more seriously. Formal standards were established, together with methodologies for designing and evaluating cryptographic equipment. These standards, the evaluation and cryptological design remained in GCHQ while the engineering design was done partly by the Post Office research laboratory at Dollis Hill and partly by the MoD. In the mid-1960s the various engineering facilities were brought together as CESD (Communications-Electronic Security Department) and in 1969 CESD joined GCHQ and was merged with the existing Comsec organisation there as CESG.

In the 1970s it became increasingly clear that the existing government monopoly of Comsec was no longer sustainable. Three driving forces were:

1: A compelling requirement for use of cryptography in the banking and finance sector;
2: Pressure from industry to be allowed to compete (with Crypto AG and other 'neutral' companies) in the global market for cryptographic equipment;
3: Evolving requirements for computer security (initially for the encryption of sensitive data).

As well as to the removal of the ban on private sector provision of crypto mentioned earlier, this led to the development by IBM of a data encryption algorithm that was to be adopted by the US standards body NIST as the data encryption standard (DES). It also marked the beginning of interest in cryptography as an academic subject. This was given a significant boost by the publication in 1976 by Martin Hellman and Whitfield Diffie of their paper 'New Directions in Cryptography', which introduced the concept of public key cryptography to the world at large.

These changes brought about a substantial broadening of career opportunities in the disciplines that would later evolve into Infosec. There were now opportunities for developing technical security careers in finance and banking, the crypto and computer industries, and academia. However, in these early stages before the mid 1980s there was still an almost complete separation between mainstream security careers and the technical security disciplines. Although the latter had expanded to include other technical aspects of security such as TEMPEST (a formerly-classified term covering compromising electronic emissions), tamper protection and traffic flow security, the discipline was still dominated by cryptography and Comsec.

The next major changes came about from developments in computing. Although in general the concern was with standalone computers (i.e. not networked), the developments involving sharing the computer for multiple tasks and many disparate users gave rise to a number of concerns about access to sensitive data or to potential damage to the integrity or availability of the computing facility. These concerns led to the development of Computer Security as a discipline and the evolution of standards and practices to promote secure operations. Again this led to an expansion of career opportunities covering such topics as secure operating systems, computer security evaluation and certification, accreditation, access control, password management etc. By the late 1980s it was realised that Computer Security was a mere staging point and that a more integrated approach was required. The term Information Security was finally coined.

By the 1990s the major security issues arising from networking were emerging as the potential for the spread of malware was realised. Throughout the 1990s the various technical and non-technical processes were matured individually and it became increasingly clear that each individual discipline was merely a component in a complex set of security measures. It followed that security issues would only be addressed successfully by a whole range of measures from a number of widely disparate disciplines. Management was therefore key to the whole process and people factors were central.

This is broadly where we are now. Although technology is at the heart of the features that give rise to the security risks, technical fixes and gizmos alone cannot provide the whole answer. Thus there is now a need for the convergence of security disciplines with the consequent requirement for a broadly-based security profession encompassing all those technical and non-technical aspects that have traditionally been seen as separate.

This is proving to be a major challenge since it is unusual for anyone to develop the level of deep expertise required in many of the technical disciplines while remaining in tune with the broader issues. As a result, it hasn't proved possible to establish a common core of professional expertise that covers the whole field. However the challenges have brought major career opportunities available at all levels, ranging from deep expertise in a highly technical area through to leadership across a whole range of expertise and the management challenge of melding a successful team. It's almost enough to make me wish I were 24 again!

HAS NEAR FIELD COMMUNICATIONS COME OF AGE IN THE UK?

By Keith Mayes & Kostas Markantonakis

> Prof. Keith Mayes is Director of the ISG Smart Card Centre.
> Dr Kostas Markantonakis is a Reader in the ISG.

Near Field Communications (NFC) is a very interesting technology development, particularly for mobile phones. In fact NFC may have a major impact on how we make use of smart cards, RFIDs, Security Elements and mobile phones within transactional systems. In simple terms, NFC permits the phone to emulate a smart card/RFID (we will use the collective term 'card' in the text) or alternatively behave as the card reader. There is also a peer-to-peer (P2P) mode for communications between two phones, although here we will focus on the more popular card/reader modes, which can interact with legacy systems. From an application point of view the NFC phone has much to offer as it can potentially host multiple card emulations, doing away with the physical cards in our wallets. Alternatively an NFC phone could interact with our physical smart cards or perhaps even passports and product tags to establish identity and authority. There is also a lot of interest in using the phone to read 'smart' posters that incorporate an RFID tag. Here the idea is often to direct the user to a website that has some relation to the poster e.g. to buy a ticket for an event.

You may wonder why we are not all using NFC technology at the moment, especially when you appreciate that the NFC Forum[1] standardisation body started life in 2004. The obvious barrier is that you need an NFC enabled phone and manufacturers have been a little slow to support this due to uncertainty over the demand and the range of security options (that we will discuss later). The good news is that popular phones[2] are now NFC enabled. Android phones include the Samsung Galaxy Nexus and Galaxy S II, and the Google Nexus S. For Blackberry devotees there are the BlackBerry Bold 9900 and 9930 as well as BlackBerry Curve 9350/9360/9370. Apple has been rather quiet with its iPhone range, however there are rumours that Apple has been busy filing a range of related patents and are about to enter the NFC arena. Before you rush out to buy a new mobile, you should appreciate that just because a phone has NFC capability does not mean it supports all the modes, so you may have a phone that could act as a P2P device, or perhaps as a reader, yet be unable to emulate a card. To be more precise, the phone hardware might have the ability to support all the modes, although the phone firmware and APIs may not make them available to applications and so it is not only the phone model that is relevant, but also the version of the firmware.

Nevertheless, the prospect of fully capable NFC mobiles from multiple vendors seems almost upon us, so it is a good time to consider some of the security issues. The need for security in NFC phones was not overlooked by the NFC forum, which incorporated a Security Element (SE) within the standards. Actually there are three main options for the hardware implementation of the SE within the mobile device as shown in Figure 1.

The earliest NFC phones included the SE as a specialist chip that was soldered in to the phone circuitry. As the chip was meant to host smart card applications, such as those found on a bank card, it needed to be strongly attack/tamper-resistant and so a smart card chip was used (e.g. NXP SmartMX[3]). Mobile network operators are none too keen on this option and the prospect of having 'new' smart card chips in their phones, especially when the UICC used to host SIM/USIM[4] (we will use 'SIM' as the common term) applications can also provide the SE functionality. The SIM-SE is therefore a standards option that has a lot of support from mobile operators. Because of the interface limitations of the SIM it is connected to the NFC radio circuitry of the phone via just one contact and the Single Wire Protocol[5] (SWP) was standardised for this purpose.

For parties that do not want to be dictated to by handset manufacturers or mobile phone operators, there is the option of having an SE on a memory card as a plug-in solution. Although you could use the same chip in each of the SE variants the ownership, control, configuration and key management could vary enormously. Having many options driven by conflicting parties is usually a warning bell for security systems. Worse would be if frustrated service and application providers move to software SEs using the main phone processor. A hybrid solution for the future could be the use of a secured execution area within the main phone processor such as the ARM TrustZone[6] although it may be difficult to prove that an adequate level and range of attack protection is provided. Table 1 (see right) includes some subjective comparison of the various SE options.

Opinions may vary on the security merits of the various SE options, but all of them should have the functionality for hosting multiple card emulations. At this point it is hard to keep a little pessimism from this note. It arises because multi-application smart cards have been around for years, but examples of card sharing in the UK are not common. There have been some public examples such as the Barclays/Oyster OnePulse[7] card, but this was a special arrangement between two collaborating parties rather than some generic sharing solution. Will history repeat itself via NFC? Returning to optimism, perhaps things will be different this time. There is a feeling that the drive to use NFC phones for payments and service access is remorseless and so the established players in these areas might just have to jump on board or risk being displaced by new entrants.

Who will end up in the driving seat is not clear cut. We have the conventional players such as phone manufacturers, mobile network operators and banks, but now also search engine companies, on-line/mobile payments companies, Operating System (OS) and trust service providers. We know that mobile operators are not waiting around as you can already buy an NFC enabled QuickTap wallet[8] from Orange in the UK. The situation is not unlike a 'gold-rush' although in the first instance it is keys that are precious. If you have the main/root management keys for the SE then you are in control of NFC card emulation applications. The sensible thing is perhaps to give the keys to a trust manager that provides an independent service for the loading/management of the card applications, and there are some industry moves in this direction. However, whilst most parties would agree that a trust manager is a good idea,

Figure 1

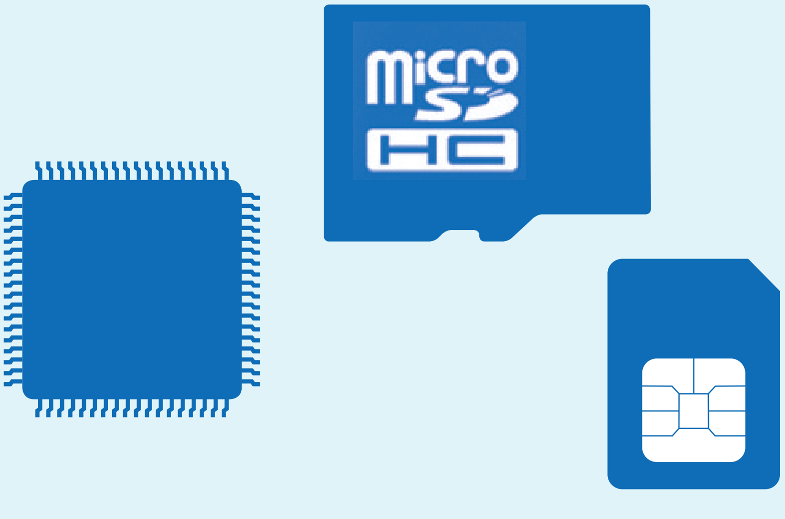


Table 1: Comparison of Security Element Options.

	Phone-SE	SD-CARD-SE	SIM-SE	Software-SE	<Future?> CPU-SE
Compatibility	Only phone modules with embedded SE.	Any phone with an SD-CARD + APIs.	SIMs with SE and NFC/SWP phone.	Any phone supporting NFC via APIs.	Phones using secured execution area in CPU.
Personalisation	In the field OTA or app (post-issue).	Conventional (pre-issue).	Conventional (pre-issue).	Via wireless app/IT protocol (post-issue).	Via wireless app/IT protocol (post-issue).
Key loading	Replace transport keys In the field OTA or app.	Conventional (pre-issue).	Conventional (pre-issue).	Replace transport keys In the field via wireless app.	Replace transport keys In the field via wireless app.
In normal use	Strongly attack resistant.	Strongly attack resistant.	Strongly attack resistant.	Weak attack resistance.	Weaker attack resistance than chip SE (suspected).
Management	OTA	OTA	OTA	Via wireless app/IT.	Via wireless app/IT.
Best features	Not operator dependent.	Independent of operator and phone manufacturer.	Securely managed via well proven methods.	Least barriers to use.	Cheaper than chip SE. CPU intensive crypto.
Worst features	Either weak ownership, allowing mis-management, or dominant party makes SE restrictive.	Needs to be deployed which is difficult/costly. Potentially one SD card per service.	Application provider needs to engage with all operators. Barrier to new services.	No tamper resistance. Risks rapidly escalating attack. Threats from malware.	Unproven attack resistance. Dominant party could make SE too restrictive.

there is a lot of argument about who should fill this role. Of course another way to solve the SE sharing problem is for an industry giant to crush all its competitors and take control of everything! A less extreme, but still worrying prospect is that the powerful industry players will rush out NFC enabled services that pay inadequate attention to security and attack-resistance, or that have secretive proprietary solutions that will attract researchers and hackers like bees to honey.

In fact NFC is already becoming very popular with attackers. This is not just because it provides some interesting targets, but also because NFC phones may be used as powerful attack tools. Previously, to attack a contactless card required a sniffer, a computer and perhaps a clone emulator. This usually meant building and then carrying around some custom equipment, which acted as a brake on the number of potential attackers or ‘enthusiasts’. An unsecured NFC mobile phone replaces all of this, and to run an exploit may just require an app download. In fact, we have taken this approach in some ISG-Smart Card Centre research work, cloning a static data payment card[9] and carrying out a range of relay attacks, including one on the P2P mode[10]. Another attraction is that in a future world where we might all use phones instead of cards, an attack application on an NFC phone is far less likely to be noticed than someone with a bag of custom electronics.

Conclusion

NFC technology has certainly come of age in the UK as evident from the fact that there are detailed standards and that you can buy a phone off-the-shelf for touch&pay style transactions. However, there is not really a clamour for this at the moment, as UK citizens have not yet got used to contactless payments with their conventional bank cards. In fact some users might just skip the card stage altogether and go straight to the phone. This is more likely now that popular and desirable phones have NFC capability, however the functional support and SE approach is varied. With the many competing parties and business interests at stake it is hard to predict the winner, so a handset vendor might be tempted to include an embedded SE as well as support for SIM and memory card SEs. The question then is if, and when, you use any, or all, of them?

NFC infrastructure, processes and business models have not yet reached maturity.
It is hoped that this is not too far off, although a successful conclusion is not guaranteed.
It is also hoped that the result would be an open, generic solution with demonstrable security protection, but the potential for vulnerable, restrictive and proprietary methods still remains.

References

1. The NFC Forum, http://www.nfc-forum.org/home/
2. NFC compatible phone list http://www.nfcworld.com/nfc-phones-list/
3. NXP, SmartMX platform features. Rev 1.0 March 2004
4. K. Mayes, K. Markantonakis, *‘Smart Cards, Tokens, Security and Applications’*, Springer Verlag, 2007, p85-112
5. ETSI, TS 102 613 V7.7.0 Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 7), 2009-10.
6. ARM, *‘TrustZone’*, http://www.arm.com/products/processors/technologies/trustzone.php
7. Barclays, *‘OnePulse’*, http://ask.barclays.co.uk/help/loans_credit/onepulse
8. Orange, *‘QuickTap’*, http://shop.orange.co.uk/mobile-phones/contactless/overview
9. L. Francis, G. Hancke, K. Mayes, K. Markantonakis, *‘Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms,’* ICITST 2009, p1-8
10. L. Francis, G.Hancke, K. Mayes, K. Markantonakis. 2010. Practical NFC peer-to-peer relay attack using mobile phones. In Proceedings of the 6th international conference on Radio frequency identification: security and privacy issues (RFIDSec’10), Siddika Berna Ors Yalcin (Ed.). Springer-Verlag, Berlin, Heidelberg, p35-49.

Definition of SCHMOOZE:
VERB: to converse informally: chat:
to chat in a friendly and persuasive manner
especially so as to gain favour, business,
or connections.

SCHMOOZING FOR FUN AND PROFIT – A BEGINNER'S GUIDE

By Ian D. McKinnon

> Ian McKinnon is a member of the Security Practice within Logica and a Consultant to the ISG

There are many things that go into making an information security professional. Fundamentally I believe that ours is a knowledge-based industry and as a consequence it helps to know stuff. Taking the MSc in Information Security at Royal Holloway is certainly an excellent way to accrue significant amounts of that knowledge, and for many, gaining an MSc in Information Security is the first step on the career ladder. The route to full-blown professional from this milestone is not always obvious, but there are some key ingredients. Practical experience and the skillful application of knowledge to solve real world problems are critical. Also of importance is engagement in the wider community and seeking professional recognition, which can be assisted by the host of professional bodies in the information security space. This article will attempt to point you in the direction of a number of these bodies in the UK and try to explain how they may help you develop into a fully-rounded information security professional.

A professional requires knowledge, skills and experience. Academic qualifications can be used to demonstrate knowledge. They are usually indicators of a minimum baseline knowledge which the holder has achieved, but very possibly exceeds.

In contrast, professional qualifications are meant to attest to more than just knowledge. They also cover experience, skills and behaviour. They can be used to indicate that you not only have enough knowledge to do a specific job but that you also have the necessary skills and experience to be competent, and trustworthy, to do it.

Professional bodies support their membership in a variety of ways. They can provide professional qualifications, a peer community, opportunities for continuing professional development and volunteering or mentoring. In addition these bodies provide a channel through which public opinion and legislation can be influenced.

Information Security is a relatively immature discipline so the knowledge and competencies that reflect professionalism are not yet very well defined. Over the last decade there has been significant competition in this space to determine who will represent the emerging profession.

As a consequence there are many professional bodies operating in the UK vying for members. These include the British Computer Society (BCS), Institute of Engineering and Technology (IET), Institute of Information Security Professionals (IISP), Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA), International Information Systems Security Certification Consortium (ISC2) and the CESG Listed Advisor Scheme (CLAS).

Each of these organisations provides a range of opportunities and support to aspiring professionals. Some focus exclusively on providing a focal point for the profession in terms of information and events.

One example is the ISSA, which runs a full events schedule on a variety of topics. These events are open, friendly and informative and are excellent opportunities to meet fellow security specialists.

Other organisations are predominantly focused on providing certifications, for example ISC2 and CLAS. Membership of these organisations enables individuals to maintain their qualifications without providing significant additional benefits. However those organisations who do put on events in the UK often invite non-members to a limited number of events as 'taster sessions'.

Some organisations offer both information, events and certifications, for example ISACA and IISP. ISACA are active as a membership organisation in the UK and also administer the Certified Information Security Auditor (CISA) and the Certified Information Security Manager (CISM) qualifications. The IISP now offer the new CESG Certified Professional qualifications discussed elsewhere in the review.

Finally there are organisations that offer a broader range of services, such as the BCS and IET. These organisations have been in existence for far longer than those previously mentioned. Benefits are similar to those for membership organisations, but also include things like chartered status and facilities in London which members can use. The BCS is also one of the three organisations offering the new CESG Certified Professional qualifications. In general terms these organisations have a far broader remit than those exclusively focused on IT security and use special interest groups to cater for sub-groupings.

This list of professional bodies above is not exhaustive as this space is crammed. There are others which you might like to investigate if those discussed are not to your taste including: SANS, Security Institute (SyI), Information Assurance Advisory Council (IAAC), Jericho Forum, Worshipful Company of Information Technologists (WCIT), Information Security Forum (ISF) and OWASP. And of course your local Royal Holloway MSc Information Security Alumni Chapter (the London Chapter is particularly active).

Whilst the primary goal of any professional should be to actively practice their art, it should not be at the exclusion of career development. Managing one's career should ideally be a constant background task to keep you moving forward. However you should be mindful to ensure that the effort you apply to your career advancement doesn't exceed the effort you apply in delivering. Whatever stage of IT security career you are currently at, do give the professional bodies discussed in this article some consideration as they can provide a range of support, qualifications and recognition that you can benefit from. Some of them, on occasion, are also a great source of beer and nibbles.

Professional Body	General Activities (meant to be factual)	Suitability (pure opinion)
BCS	Organisation: UK-based Broad Professional Membership History: 50+ years Membership: Student through Chartered Fellow Annual Costs: £25 through £137 annually One-off Costs (example): £142 for CITP assessment Certifications: ECDL, CITP, ISEB and CESG Certified Professional	The BCS is a professional body which offers value for those involved in IT throughout their career. It is possible that offering the CESG Certified Professional qualifications will provide a focus on security that has weakened somewhat in the last few years.
IET	Organisation: UK-based Broad Professional Membership History: 100+ years Membership: Student through Honorary Fellow Annual Costs: £20 through £150 annually One-off Costs (example): None Certifications: None	The IET is a professional body with significant history and an impressive headquarters on the Embankment. Probably best considered by those later in their career for the facilities and kudos.
ISSA	Organisation: US-based Membership History: 30+ years Membership: Student through Full Annual Costs: $30 through $95 annually + chapter fees (UK Chapter levy no fees) One-off Costs (example): None Certifications: None	The UK chapter are a friendly organisation and provide excellent opportunities to network with fellow and aspiring professionals. This is a good starting point in the UK for early schmoozing activities.
IISP	Organisation: UK-based Focused Professional Membership History: 6+ years Membership: Student through Full Member Annual Costs: £20 through £200 annually One-off Costs (example): £50 for Full membership Certifications: CESG Certified Professional scheme	The IISP is a more recent entrant into the arena and represents a UK-centric focus for IT Security Professionals. Having finally gained traction the IISP is an increasingly strong candidate to support UK based professionals.
ISACA	Organisation: US-based Membership & Certification History: 40+ years Membership: Student through Full Annual Costs: $25 through $135 annually + chapter dues One-off Costs (example): $140 for CISA exam Certifications: CISA & CISM	ISACA provides a good range of professional services in the UK and beyond. It is undoubtedly skewed towards audit and governance, which needs to be considered when comparing it with the competition.
ISC2	Organisation: US-based Certification History: 20+ years Membership: SSCP, CAP, CSSLP & CISSP Annual Costs: $35 through $85 annually One-off Costs (example): SCCP £190 & CISSP £370 Certifications: SSCP, CAP, CSSLP & CISSP	ISC2 has a strong brand focused primarily around CISSP, which is a globally recognised certification. That said ISC2 have struggled to demonstrate significant value beyond their certifications.
CLAS	Organisation: UK-based Membership History: 14+ years Membership: CLAS Annual Costs: £1250 One-off Costs (example): Transfer £400 Certifications: CLAS	CLAS is very expensive and specifically aimed at UK IA professionals operating in the HMG sector. As such it is historically a mid-career aspiration for those with significant experience.

BOOK REVIEWS:

'EVERYDAY CRYPTOGRAPHY' BY PROFESSOR KEITH M. MARTIN

(Oxford University Press, 2012,
ISBN 978-0-19-969559-1)

Reviewed by Kenny Paterson

Albert Einstein is reputed to have once said *'Everything should be as simple as possible, but no simpler'.* This is an excellent maxim for any prospective author of a textbook and could accurately be used to describe Keith's new book.

First, a little ISG history. For many years, the core course on the ISG's masters programme 'Introduction to Cryptography and Security Mechanisms' was taught by Fred Piper, in his own inimitable and unique style. When Fred allegedly retired (though as we all know, he didn't really), Keith was assigned to take the course over. How to follow Fred? Keith in fact had already attended Fred's course in its entirety to help him develop the distance learning version of the course. He was thus well placed to take Fred's course forward. This involved some reorganisation and extension of the syllabus, while still maintaining the core philosophy of Fred's approach:

- Since the ISG's student intake is so diverse, the lecturer cannot assume any mathematical or computer science background on the part of the audience.
- Yet the discussion of complex cryptographic concepts needs to be as rigorous as possible.
- Moreover, cryptography is not just about algorithms and protocols, but also about key management, system design and human factors.

Naturally, this approach creates some acute pedagogical challenges. In particular, with one notable exception ('A Very Short Introduction to Cryptography' by Fred and Sean Murphy), there are no books on cryptography that really match this approach. But the subject is sufficiently complex that a textbook is extremely beneficial in order to support the students in their learning, no matter how well-organised and informative the lecturer. Thus was this book conceived.

After a protracted gestation period, Keith's book has finally arrived. So how does it match up to expectations?

As Sam Goldwyn once said, *'I read part of it all the way through'* and can safely declare that this book delivers in full. By which I mean, this textbook is the perfect accompaniment to Keith's course and is the monographic embodiment of the 'simple as possible but no simpler' philosophy. At more than 500 pages, it is long (much longer than 'A Very Short Introduction'), but no longer than it needs to be. It presents difficult concepts in a simple way, but no simpler than is absolutely necessary. It will be accessible to everyone with an interest in the subject of cryptography (or who needs to pass an exam!), but that accessibility will require a genuine effort on the part of the reader. And the book is very readable - the prose flows, concepts are introduced in a logical order, and there is little 'fat'. Above all, this is a book that knows what it is trying to achieve, and sticks to that mission. It is obviously written by someone who loves the subject and knows how to teach it effectively.

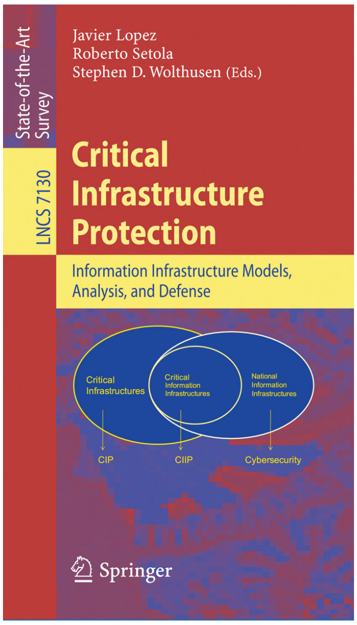
Of course, this book will not satisfy everyone. Some will want to read something shorter - and they have a perfect alternative in Fred and Sean's earlier book (but then will want to read this book!). Some will want a more mathematical treatment - and they can read Doug Stinson's excellent text. Some will want an introduction to theoretical cryptography - they can go and read Katz and Lindell (and then Goldreich if they still have an appetite!). Some will want a historical overview involving spies and Mary Queen of Scots - for which Simon Singh's book is perfect. But if a reader wants an honest-to-goodness overview of what cryptography is about, what problems it can solve, and how it is used in the real world, then this should be their text of choice.

CRITICAL INFRASTRUCTURE PROTECTION

This book is the latest part of the 'State of the Art Surveys' sub-series of Springer's Lecture Notes in Computer Science series. This volume, which is edited by J. Lopez (University of Malaga, Spain), R. Setola (University of Rome, Italy), and S. Wolthusen (Royal Holloway) and is entitled 'Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defence', provides a timely overview of current core research areas in critical infrastructure modelling by a group of international researchers.

The book is divided into four parts, beginning with a high-level overview of infrastructure sectors and threats, followed by an in-depth review of modelling techniques for interdependencies and attack detection. A third part covers selected aspects of control systems security and protocols. There are several sector studies including electric power grids, oil and gas, and financial services highlight sector-specific aspects and challenges.

The book is primarily intended for researchers, but is also anticipated to be used in postgraduate lectures in several universities worldwide.


State-of-the-Art Survey
LNCS 7130

Javier Lopez
Roberto Setola
Stephen D. Wolthusen (Eds.)

Critical Infrastructure Protection

Information Infrastructure Models, Analysis, and Defense

Critical Infrastructures
Critical Information Infrastructures
National Information Infrastructures
CIP
CIIP
Cybersecurity

Springer

CESG CERTIFIED PROFESSIONAL SCHEME

By Ian D. McKinnon

> Ian McKinnon is a member of the Security Practice within Logica and a Consultant to the ISG

In keeping with a tradition that the Information Security Group at Royal Holloway has developed over more than twenty years for effective links with industry, the ISG is part of a consortium which is now able to certify information assurance professionals. The ISG is partnering with the Institute of Information Security Professionals (IISP) and CREST (Council of Registered Ethical Security Testers) to provide certification services under the recently launched CESG Certified Professional (CCP) scheme. This clearly demonstrates the commitment of the ISG to continue to be at the forefront of the development of Information Security as a profession within the UK.

These certifications are a key part of the Information Assurance Professionalization Programme being driven by CESG, which is part of GCHQ and acts as the National Technical Authority for Information Assurance. Prior to this initiative the primary endorsements in the government IA space have been InfoSec Training Pathways and Competencies (ITPC), originally run by the Cabinet Office, and the CESG Listed Advisor Scheme (CLAS).

The new certification scheme supports a variety of IA roles each at three different levels – practitioner, senior practitioner and lead practitioner. The new scheme addresses concerns associated with the old CLAS scheme. These concerns were predominantly associated with the fact that CLAS membership did not give an indication of areas of expertise within the HMG IA spectrum or the extent of their experience.There are three certification bodies operating under the scheme who can attest to a candidate's competencies against the roles supported. These are the BCS, the consortium led by the IISP, and the APM Group. The IA roles defined by the scheme are Security & Information Risk Advisor, Security Architect, IA Auditor, Accreditor, IT Security Officer (ITSO) and Communications Security Officer (ComSO).

The role most broadly aligned with the existing CLAS scheme is the Security & Information Risk Advisor. This role, Security Architect and IA auditor role are most closely associated with the supply side, whereas the roles of Accreditor, ITSO and ComSO are more usually undertaken by civil servants. However the demarcations between supply organisations and civil service are being broken down as consultants are more frequently asked to take crucial roles such as Accreditor or ITSO. The scheme is also open to civil servants to allow them to certify against their competencies, which they could previously demonstrate via ITPC, but not via the CLAS scheme.

The CESG Certified Professional scheme is aimed firmly at those operating in HMG environments, but there is a continued convergence between commercial IT security and government IA activity. This certification scheme may become common across both public and private sector within the UK over time. It builds on sound foundations in terms of the required skills in the form of the BCS-owned Skills for the Information Age (SFIA) framework and the more IA-specific skills framework developed by the IISP to measure competencies.

Whilst this scheme is in its pilot phase and is firmly focused on HMG security within the UK, it would be foolhardy of any aspiring IA professional not to keep at least one eye on its progress. It is difficult to know which qualifications in the IA sector will emerge as critical in the future. However it is the responsibility of the professionals to ensure they don't miss out if CCP becomes the de facto qualification. What is certain is that the ISG will be in the leading pack defining the IA profession in the 21st century, and beyond.

PROJECT UPDATE – AN INTERVIEW WITH KENNY PATERSON

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

Q: You're now an EPSRC Leadership Fellow. How did that come about?

A: Back in 2005, I started working with some of my research students on finding cryptographic flaws in network security protocols like IPsec and SSH. At the same time, I was increasingly involved in consulting work where I had to analyse systems using cryptography. What eventually became apparent is that theory and practice in cryptography were heading for a divorce. Well, they'd got to the stage of sleeping in separate rooms, but divorce seemed to be on the cards! The different communities of academic researchers, standards bodies and implementers had increasingly strained lines of communication - while theoreticians might have something useful to say to practitioners, their results are written in a language that is almost impenetrable; at the same time, practitioners would blithely ignore even the most basic lessons from theory, for example the desirability of using authenticated encryption. After a few years of writing research papers and articles about this gap, I eventually realised that the problem was significant, and that I should try to get research funding to look into it more closely.

Q: So you applied to EPSRC for funding?

A: Right. They had a very attractive funding mechanism at that time called the Leadership Fellowship programme. Basically, they wanted people to write ambitious 5-year research plans saying how their research would influence the field. I thought that I had a good story to tell around the topic of 'Cryptography: Bridging Theory and Practice', and a good research track record to back it up. We had just published a paper breaking SSH that had got a lot of attention and that had reinforced the key messages to me - the SSH protocol had been subjected to a detailed security analysis by some very respected scientists back in 2004, and yet we found an attack that lay just outside their security model. This highlighted to me some of the shortcomings of the approaches then being used to formalise the analysis of secure protocols. This gave me added confidence that I could say something novel in my research proposal.

Q: What was the funding process like?

A: It was very tough! There was an outline proposal stage. 600 people applied. Then about 100 were invited to submit full proposals, and the ones who came through this went on to an interview at the EPSRC HQ in Swindon. I survived that, but coming home on the train from Swindon, I was a bit disappointed by my performance at the interview. Fortunately, I had had some very nice reviews on my proposal. And the panel seemed to like the idea that I was going to try to unite two diverging communities. I explained that the work I would do would have a practical as well as a theoretical impact, and I had some great letters of support from industrial partners. If I'd only said 'I'm going to do more of the same', then I don't think I would have sealed the deal. The bit about building a community of researchers was very important.

Q: So what does the funding enable you to do that you couldn't do before?

A: Several things. First off, from starting the project in March 2010, I have been officially free from all teaching and administration duties. In other words, the fellowship 'buys me out' of this kind of work. In reality that stuff can be a huge time drain since university departments are managed by the academics, and there are innumerable committees and requirements to produce meaningless bits of paper. So this part is incredibly important, as it means I can concentrate fully on research. In practice, things are not quite that simple - it took about 18 months to fully divest myself of other responsibilities and projects, and I already had a full crew of talented PhD students knocking on my door at regular intervals. I also get asked to do various things from time to time by my colleagues, like reading their grant proposals or sitting on interview panels. But I am largely left alone!

Q: Do you miss teaching on the MSc?

A: I really do - I really liked being in the classroom and got a huge buzz out of putting on a good show in the lectures. But I don't miss marking the exam! So Jason Crampton has taken over the Network Security course, and has given it a good kicking to get it into better shape. But he's still kind enough to invite me to pop up and give a couple of guest lectures on things like IPsec and SSL/TLS. So I still get my fix.

Q: You were talking about what the funding lets you do that you couldn't before...

A: Right. So the grant also gave me funding for two PhD students and two postdocs, to build up a team to help execute on the planned research. The PhD. students - Susan Thomson and Dale Sibborn - are now both on board. Hiring postdocs took a bit longer - the first appointee, Martijn Stam, stayed long enough to help us produce a couple of really strong papers, but then got an offer of a permanent lectureship at Bristol - very hard to turn down! His replacement, Bertram Poettering, comes on-board in April, and then the second postdoc will join us in September. So the team will be up to full strength by then. I am hoping we can get a real buzz going around the team, with lots of ideas being thrown around and interesting sub-projects coming up. I have lots of ideas for what we should do, but the students and especially the postdocs will bring their own insights too.

The other thing that the fellowship brings me is a bit less tangible. I think it's about confidence: to some extent, I see getting such competitive funding as being an external vote of confidence in my abilities as a researcher. That spurs me on to try to be more ambitious and do bigger things.

Q: You are now two years in. So what are the main outcomes of the project so far?

A: Well there's a nice list of research papers building up. We had some pretty interesting results on IPsec published at ACM-CCS in 2010, and a paper giving a detailed security analysis of SSH at Eurocrypt 2010. Then, late last year, I published a paper with some US-based collaborators, Tom Ristenpart and Tom Shrimpton, at Asiacrypt 2011, giving a formal security analysis of the TLS Record Layer protocol - that's the symmetric crypto part of TLS. The title was 'Tag Size Does Matter: Attacks and Proofs for the TLS Record Layer', which is meant to be funny... Anyway, the interesting thing here was that, even after 15 years of analysis, we still didn't have a proper security analysis for this thing. Imagine: the de facto secure protocol of choice for the Internet, and the crypto community had not yet got around to doing a full analysis! So we managed to provide one, but along the way found some new attacks against the protocol that no-one had anticipated. That was an exciting moment that came out of staring at a whiteboard for several days with very smart people.

The next cool thing was a paper with my student Nadhem AlFardan in which we analysed implementations of the DTLS protocol. This is kind of a morph of the TLS protocol, defined for use over UDP instead of TCP. It's being more and more widely used. Cisco use it extensively in their VPN products. That choice of transport protocol turns out to have a big impact for security... We managed to find some very cute attacks against both the OpenSSL and GnuTLS implementations of DTLS. The two projects - OpenSSL and GnuTLS - did new code releases on account of our work. So we had an immediate impact with the research: these systems are now more secure. And we won a Distinguished Paper Award at the NDSS 2012 conference for our efforts - that was a nice surprise!

But the most important thing so far, I think, was a workshop that I co-organised with

Nigel Smart from Bristol. The workshop was provocatively titled ‘Is Cryptographic Theory Practically Relevant?’, which fits with the theme of my whole project. The event attracted more than 100 participants, especially lots of younger researchers who seemed genuinely eager to understand more about the real-world problems being faced in industry and how (or even if!) theory can help to address these. So we had three days of lively discussion and debate, concluding with a panel session. We held the event at the Isaac Newton Institute in Cambridge, and they kindly videoed the whole thing, so anyone can go and listen to the lectures online at http://www.newton.ac.uk/programmes/SAS/sasw07.html

We’re now planning a follow-up event for 2013, and are talking to Dan Boneh at Stanford about hosting it there. There was a fantastic atmosphere at the workshop. I really think it’s going to help in establishing that community of researchers I was talking about before.

Q: And what about the next three years?

A: I expect things to change a bit now. So far, the emphasis has been largely on looking at specific protocols. There’s still work to do there - we’ve just published a fun paper on the EMV protocols at the CT-RSA conference, and there is more to come on TLS for example. But now I want to start looking at more general questions. For example, what is the role of randomness in cryptography, and how can we deal with imperfect randomness sources? This is not a completely new question, of course, but I don’t think it’s been systematically explored yet. And it’s crucial to real-world security. Once the project postdocs are up and running, these bigger questions will be right at the top of the agenda.

Q: And beyond that?

A: Hard to say! I never really used to plan my research, but just did whatever was interesting to me at a given moment in time. It seemed to work reasonably well as a ‘strategy’! But applying for a large and complex grant forced me to be more organised, and at least come up with a framework within which to operate. That seems to be about the right level of planning for me. If I was pushed to give an answer, I’d have to say ‘tools’. Right now, we analyse everything by hand - both for proofs and for finding attacks. But I know that other people have some interesting tools to at least partly automate this work. I need to learn more about that. But then just last week I was talking to some colleagues about private computation on DNA - this is a fascinating question. So in the future, sequencing your entire DNA will be very cheap, and maybe everyone in the developed world will get this done as a matter of course. But what are the privacy implications? And how can cryptography help? Right now, I’ve no idea what the answers are, but it looks pretty interesting. So maybe not tools after all. Who knows? I guess that’s the joy of research!

Q: How can people learn more about your project?

A: The best place to go is my homepage (www.isg.rhul.ac.uk/~kp). One of these days I will get around to making a proper project page. But right now people can at least find all the papers there. And if anyone wants to get involved or has any good ideas for targets for our techniques, just drop me an e-mail.

STAFF PROFILE: LORENZO CAVALLARO

> Lorenzo joined the ISG as a lecturer in January 2012.

Tell us a bit about your background and research interests.

It all started with 'Phrack', but allow me step back for a second. In the mid-90s, I enrolled in a five-year Computer Science degree program, as I've always been fascinated about Math and Computer Science (CS). For some unclear and unknown reason, I quickly became interested in everything that was related to hackers. Unfortunately, there wasn't much information available at that time about this fascinating world. Or, at least, such information was 'hidden'. I thought that CS could be key to helping me explore in that direction.

Anyway, it was shortly after we had Internet for end users in Italy that I started to search for hacking-related topics (remember Altavista?). Sadly, most of the searches led me to questionable web sites and not to the information I was looking for. Occasionally, I could stumble upon reports that explained how to make bombs or how the US phone system worked (phreaking was very popular at that time)!

At that time, I had no idea what an academic paper or conference was. Then, by luck (you need that in your life, sometimes), I came across a fascinating article called 'IP-spoofing Demystified', by daemon9/route published in an e-zine named Phrack. This was what I was looking for! It goes without saying that I did not understand a single word, but that was not the point. I had finally found the kind of information I was looking for. Mike Schiffman (aka route/daemon9 of infonexus.com, who later became well-known for his work on libnet) unwittingly jump started me.

Luckily for me, the paper had references. The most enlightening one was 'TCP/IP Illustrated Volume 1', by Richard W. Stevens. I decided to start reading Stevens' book in my spare time. He could really explain complicated matters in a very easy-to-understand manner. I devoured the book. It was just terrific (my priceless thanks to you Richard, RIP). That book provided me with the basis to understand route's paper in Phrack, and many others, such as 'Smashing the Stack For Fun And Profit' by Aleph One, followed shortly thereafter.

Those years were really a lot about reading underground research papers. They were golden years, when you still had full disclosure and you could hang out with smart hackers on IRC as well. I then moved on, took a (working) break, got back to university, finished up all the classes (while still reading underground research papers and broadening my interests to academic research as well) and graduated. I started my PhD at the University of Milan, Italy and halfway through I decided to go overseas to spend a rather long visit in the Department of Computer Science at Stony Brook University working with Prof. R. Sekar on memory error related topics, taint analysis and intrusion detection. I defended my PhD on Feb 2008 and I was then offered a two-year PostDoc position at University of California, Santa Barbara, working with Profs. Kruegel and Vigna on malware related subjects. Afterwards, I joined Profs. Andrew S. Tanenbaum and Herbert J. Bos as a PostDoc at Vrije Universiteit Amsterdam working on OS dependability and systems security (until Dec 2011). Finally, I landed in the UK as a happy Lecturer of Information Security in the ISG, where my beautiful and exciting journey - always revolving around systems and network security, and malware analysis and detection - will continue.

What attracted you to come to work at Royal Holloway?

Many factors, indeed. First, Royal Holloway is a highly-ranked research institution worldwide and the ISG offers a really broad and diverse expertise in Information Security, which was reflected by the ISG's open-minded short listing of candidates from across the security landscape. This was the environment I was looking for. Having the freedom to engage and pursue your very own research and teaching interests while being supported by a strong, active, and respected research group. Besides, Royal Holloway is really close to London, one of the most-vibrant capitals of the world. A unique personal-professional relationship that I bet is hard to find elsewhere.

Not to mention Founder's Building which, according to Thomas Holloway, was designed 'that it may not by an insignificant style dishonour its name - you are aware that nowadays, it is necessary to fill the eye'.

Is it true that you once took over a botnet?

Legend says that's true and, luckily, facts confirm it as well. It happened during my PostDoc at UCSB in 2009. It was a rather unique and exciting opportunity that gave us a chance to gather important insights into the data that's actually stolen by a botnet. Over a period of 10 days, we observed more than 180,000 infections and recorded more than 70 GB of data that the bots collected. While botnets have been 'hijacked' before, the Torpig botnet exhibited certain properties that make the analysis of the data particularly interesting. First, it was possible (with reasonable accuracy) to identify unique bot infections and relate that number to the more than 1.2 million IP addresses that contacted our command and control server. This shows that botnet estimates that are based on IP addresses are likely to report inflated numbers.

Second, the Torpig botnet is large, targets a variety of applications, and gathers a rich and diverse set of information from the infected victims. This opens the possibility to perform interesting data analysis that goes well beyond simply counting the number of stolen credit cards. For instance, users do still use weak passwords and roughly 1 out of 3 reuse credentials across different web services (enabling for more successful social engineering attacks).

What developments do you foresee in the near future regarding malware?

The malware landscape has changed drastically in the past years. What was once a for-fun activity has now turned into a fully-fledged profit-driven criminal business. In its last quarterly threats report, McAfee identified 150,000 malware samples every day, which is a 60% increase over 2010. In addition, Sophos reports an average of 19,000 new malicious URLs each day in the first half of 2011, and more than 80% of those URLs were legitimate websites hacked by cyber criminals (drive-by download or stealing access via malware infected machines).

Mobile malware is on the rise, counting more than 1,200 samples at the end of 2011. New infection vectors (e.g. social engineering exploiting trust in social networking), Mac malware, advanced malware (e.g. stealthy botnets and sophisticated rootkits), services for hire, etc., don't let me believe that upcoming years will be any better either…

A 2010 report by Cyveillance showed that only about 60% of new malware is detected on average by AV after 30 days, showing that malware is a moving target. Besides, with a total gross count of 70M malware samples around, it seems that traditional signature-based detection approaches will be unlikely to be able to keep up in the long run.

It is clear that more research is needed to fight such ever-evolving threats. We should likewise start accepting the fact that

eventually something will break, and keep focusing on how to make things harder for the attacker and minimizing the risk. Do you think we will ever get 'on top' of the malware problem?

Hard to say - it's a cat and mouse game. We should however keep doing research to raise the bar. For instance, studying real-world malware modus operandi and new offensive technology is not a mere academic exercise. And, contrary to popular belief, it is not even a way to train our next cyber criminals (they will get on fine without our help, honestly). It is rather an effective (and likely the only) way to form knowledgeable experts, teachers, researchers, and practitioners able to fight back. Besides, it allows you to gather an intimate knowledge about the systems and the threats, which is necessary to successfully devise novel, effective, and practical defence techniques.

What are your plans for the coming year?

To keep pursuing my dreams. This includes working on exciting topics such as (but not limited to) malware, mobile security, cloud security, virtualization technology, software protection, program analysis, and systems and network security.

Noting your beautiful hair, some people say that you are the new Fred Piper – is it true?

Although Samson's strength was in his hair, I unfortunately don't believe it only takes long hair to be as successful and inspirational as Fred has been!

THE INTERNET OF ENERGY PROJECT
By Stephen Wolthusen

> Dr Stephen Wolthusen is a Reader in the ISG.

The recently-commenced Internet of Energy project brings together 40 partners from ten EU and EEA member states under the European Commission's 7th Framework Programme's ARTEMIS Joint Undertaking in a major initiative with a total funded volume of €45m.

The objective of this project is to study the infrastructure required for the successful interconnection of electric power networks with a primary focus on the electric grid edge up to the distribution grid with the Internet, and electric account mobility. This will require going significantly beyond the so-called Smart Grid by incorporating mobile generators and storage systems alongside buildings and residential systems.

Each of the sectors of energy, communication, and transportation is individually considered to form part of national and European Critical Infrastructures, but although these have long been understood to be strongly interdependent, the need to integrate these more strongly and intelligently poses a number of new challenges both for robustness and security.

Building on long-standing research on modelling critical infrastructures at different levels, Royal Holloway is responsible for the study of security and privacy-related aspects of the overall project, in co-operation with partners in the UK (QinetiQ, Infineon UK), Finland (Nokia Siemens Networks, VTT), The Netherlands (Technolution), Italy (Universities of Bologna and Siena), and Germany (Siemens and Lantiq). The group is comprised of two post-doctoral researchers, Dr. Y. Feng joining from the Computer Science department at Royal Holloway, and Dr. C. Dowden, from Oxford University.

The project, scheduled to run until May 2014, will encompass an in-depth study of new and emerging security requirements arising from these interconnections. This includes the need for real-time operation and graceful handling of faults and responses to deliberate attacks. The resulting outputs will involve the development of guidance materials and a security infrastructure architecture. We also plan to develop novel adversary models including state estimation mechanisms robust to missing and maliciously manipulated data. This will also include the development of algorithms that can efficiently provide robust state and threat estimation in the type of dynamic network topology that underlies energy networks.

For more information, see http://www.artemis-ioe.eu/

ARTEMIS

SEVENTH FRAMEWORK PROGRAMME

IoE
Internet of Energy

WHERE ARE WE WITH SECURE LOCATION SERVICES?
By Gerhard Hancke

> Dr Gerhard Hancke is a Teaching Fellow in the ISG.

Technology is said to make our lives easier. We are surrounded by a collection of devices with embedded computational intelligence that assists us in our daily tasks. You can choose to have a freshly brewed coffee at the press of a button, or make your car park itself. Much has been written and spoken over the years about the reliability and security of embedded systems, and with good reason. Embedded systems are often used to provide services that are crucial to our safety and security, such as an aircraft's autopilot or programmable logic controllers regulating industrial processes. System developers spend a significant amount of resources testing their software and hardware to ensure that systems such as these work reliably. It is, however, sometimes the case that these systems must interact with, and rely on, systems that are less secure.

There are an increasing number of embedded systems, used in safety and security sensitive applications, which incorporate public location information into their core functionality. Embedded systems that rely on location information are responsible for aviation and maritime navigation, emergency response and rescue operations, high-value asset or vehicle tracking, and even rail signalling and train control. The main source of location information in these embedded systems is global navigation space systems (GNSS), such as GPS (US), GLONASS (Russia) and the forthcoming Galileo (EU) and Compass (China). The large-scale use of GNSS for position, navigation and time (PNT) data is the result of such systems' ubiquitous availability, accuracy and the relatively low cost of use. There are numerous proposals for location-based services incorporating non-GNSS technology, which include the use of mobile network base stations or terrestrial radio (LORAN), but the issue of availability inhibits these systems reaching the scale of GNSS. For example, mobile infrastructure is generally limited to developed areas and continued operation is dependent on private enterprise, while LORAN has been largely decommissioned and it is not yet certain how widely the enhanced version (eLORAN) will be deployed.

The US Global Positioning System (GPS), currently the most widely used GNSS, transmits two basic signals. The precision P(Y) signal used by military receivers does feature an encryption mechanism and therefore only a transmitter with the correct shared key can generate it and only a receiver with the correct key can track it. The crude access (C/A) signal used by civilian receivers provides no security mechanisms. The security of GPS became a very public matter in December 2011 when a US Sentinel UAV was captured by Iranian forces, who claimed that they had done so by manipulating the UAV's GPS navigation system. However, the security vulnerabilities of the GPS system and the increasing reliance of sensitive applications on global positioning were issues already pointed out more than a decade before. In 2001 the US Department of Transportation highlighted vulnerabilities in transport infrastructure relying on GPS in the 'Volpe' report. They identified three main methods of what they termed 'intentional interference'. Wholesale disruption of signals (jamming), the rebroadcasting of legitimate signals that results in an incorrect position being reported (meaconing) and the creation of signals with the purpose of causing an incorrect location to be reported (spoofing). The report also made recommendations to mitigate these security issues, including cryptographic authentication and verifying signals' angle-of-arrival. A decade later security vulnerabilities remain while the use of GPS in critical applications have increased dramatically, a situation affirmed in a 2011 report by the Royal Academy of Engineering emphasising the reliance on, and the vulnerabilities of, GNSS.

At the time of the Volpe report the equipment needed to perform meaconing or spoofing was expensive and bulky. Technology has moved on from then and with the advent of software defined radios the transmission of GPS signals has become significantly easier and cheaper. These days GPS signals could feasibly be received, relayed or created with open source software, such as GNU Radio, and a small, generic software radio platform such as the Ettus USRP. Although it is not as elegant an exploit, jamming is just as big a threat as meaconing and spoofing. The loss of GPS services potentially disrupt a wide range of services usually taken for granted. In October 2011, the Royal Navy jammed GPS signals off the coast of Scotland as part of pre-planned military exercises but had to stop doing so because of safety considerations when the navigation systems of fishermen, who had not received the advanced warning, stopped functioning. Small scale GPS jammers are widely available for online purchase and marketed as personal privacy devices (PPD), which can jam both GPS and mobile communication. These products are intended for people who wish to prevent third parties from tracking them using location-based services but unfortunately such a device can just as easily be used by thieves to disable asset and vehicle tracking systems. PPDs could also unintentionally effect much more critical applications. A good example of this is a Federal Aviation Authority investigation into the reason why a GPS-based landing systems used at New Jersey's Newark Airport suffered from periodic breaks in reception. PPDs used by truckers on the nearby freeway were eventually identified as the cause.

Redesigning GNSS to allow for secure civil location services will in all likelihood not happen anytime soon and securing civil location services does not appear to be an immediate concern. GPS III, which is scheduled for deployment in 2014, introduces a second civilian channel and a 'Safety of Life' channel, alongside a backward compatible civilian channel, but none of these channels provides for any security mechanisms. GPS III does include improved anti-jamming and security measures on the military channel. Only one of Galileo's five forthcoming services does allow for jamming resistance and encryption. This service, 'Public Regulated Services' (PRS), could potentially alleviate secure location issues for some systems as it is intended not only for defence purposes, but also for law enforcement and emergency services in addition to selected critical telecommunication, energy and transport applications. Access to this channel will, however, be regulated and only authorised parties will be able to use a PRS-capable receiver, so it is likely that this service will not be implemented in most products intended for the civilian market.

Of course, if security mechanisms were ever to be implemented on civilian channels this might adversely affect their ubiquitous usability. For example, a cryptographic solution would need a suitable key management system, which would allow for timely key distribution to both transmitters and receivers. This especially adds to the complexity and cost of the receiver, and some users with limited security needs might not be satisfied with a system where they could lose service out in the wilderness or on the ocean because their device was unable to receive a key update. This means that the responsibility rests on systems designers to find ways to improve existing receiver architectures, hardening these against simple attacks, to take GNSS security risks into account when designing location services, and to incorporate adequate fail-safe measures, such as back-up non-GNSS solutions.

WATCHING OR BEING WATCHED: CO-EXPLORING PRIVACY IN PUBLIC SPACES

By Lizzie Coles-Kemp

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

This year the Visualisation and Other Methods of Expression project (VOME) was lucky enough to take part in the Economic and Social Research Council's Festival of Social Science. This will be the very last time that VOME takes part as the project closes on the 4th July, so we wanted to make it a true celebration of the innovation and public participation that VOME has striven to achieve during its four years.

The event was entitled Privacy.Co.OK? and was led by Freya Stang who has fronted all of our public engagement with performance art. The aim of the event was to co-create with the general public a 10 foot collage in the underpass of Middlesbrough railway station that captured the secret things that people like to do online and the secrets that they want to protect from the ever-more-powerful reach of the Internet.

Setting up an event like this is not trivial. Months of planning go into the logistics, format and outputs of the event. Freya selected Middlesbrough railway station as the location because, in her words:

> ***'It is a space of movement and transfer. People of all ages, different ethnic groups and social backgrounds come and go from this location; connecting, meeting and parting. It's a public space where intimate moments happen. It's also a place where people spend time watching other people, much like the way people often behave on the Internet'.***

Whilst this space worked well for Freya and her team of artists, for me as a project manager it was a little terrifying – not least because the railway station is a listed building and gaffer tape and listed buildings do not always mix well! By the end of the planning, with the support of Freya, the wonderful staff at Middlesbrough Railway Station and Lynne White who co-ordinates VOME, I was extremely familiar with the layout of the underpass, the quality of the grouting on the tiles and the physical security for the project staff and equipment!

Engaging with the public without any prior trust-building is always challenging. It is even more challenging to ask for almost immediate real-time engagement. However, participatory theatre techniques are often effective because the artists build a narrative which uses techniques that promote engagement in such a way that all participants are on an equal footing. Artists and researchers work together to develop an environment in which the public feels able to engage and express themselves about on-line privacy.

Freya put together a team of performance artists who have worked with VOME over the last few years. Freya explains her plan:

> ***'To draw the public in and to help stimulate thought and creativity, a small team of performers used themed character interactions. Reeta, one of the performers, had a suitcase of her own secrets that she shared. Andy Christie and Jose Parra (Bimbilibausa) went out in a duo, acting as live comment boards, changing identity with use of masks and providing light relief by way of celebrity red-carpet interactions which led to portrait taking, skilfully photographed by Luke Avery. We showed a short humorous (5 min) film made specifically for this year's Festival of Social Science event by Rita and myself, starring Rita, called 'Watching or Being Watched'. It could be viewed through a keyhole installation in the station's café. Rita interacted with people as this character and also went out as another masked character. I went out as Margareth the clown, bearing the world's smallest mask, the red nose. The red nose is the mask of the theatrical clown and it reveals aspects of the often hidden self; it displays humanity and therefore often touches people'.***

As scientists, we often miss the importance of the level of detail with which an artistic intervention is designed. Freya comments on the use of masks:

> ***'Mask work is an interesting artistic practice in relation to the process of how people choose to present themselves when they are on the Internet. Mask work involves dealing with issues and questions about how we construct a sense of identity, who we wish to be, and how we want to be seen by others'.***

By the end of the Sunday session, the team of artists and researchers had achieved their goal and had worked with the public to build a 10 foot collage full of drawings and comments, as well as producing an accompanying sound collage. We had showcased the innovative way in which VOME researchers and performance artists work together with the general public to engage in grass roots debate on the nature of privacy in an internet-immersed society. Before the end of the project, we intend to run similar events in Sunderland and possibly one other city that has hosted the VOME over the last four years. We also hope to produce a sound and visual collage to reflect VOME's engagement with the extremely generous and engaging communities of the Northeast.

Some pictures of this event, as well as many of our other activities, can be found on the VOME website http://www.vome.org.uk

ISF UPDATE
By Geraint Price

> Dr Geraint Price is Lecturer in the ISG.

In a little over a year the evolving relationship between the ISG and the ISF (Information Security Forum) has shown real promise, and already delivered in a few areas.

The ISG was well represented at the ISF Congress (their annual global forum) in Berlin back in September 2011. I manned a stand at the event, and there was a steady stream of interest throughout the event in what we did, particularly around the different flexible modes of delivery for the MSc Information Security. What this showed was that, for those currently working in the information security industry, the Distance Learning and Block Mode delivery modes of our degree programme are very appealing since both provide the capability to cement or develop knowledge while still having time to engage with the 'day job'. I was pleasantly surprised by the number of those in managerial positions who discussed the course with me, highlighting that they felt a number of their staff could benefit from attending the MSc. I think this reflects the strength of what we have always intended our MSc to be: a vehicle for the development of industry-relevant graduates.

As well as the ISG stand, Robert Carolina delivered one of the keynote presentations. Those who have seen Robert talk about his belief that Cyberspace does indeed have borders, just like any other space, will appreciate the positive impact that his presentation had on the audience.

One of the key things that the ISF does for its members is to carry out research projects which then deliver a report that is intended to guide the membership in some aspect of information security. One of 2011's priority ISF projects was to investigate the nature and effect of Information Security Governance. Lizzie Coles-Kemp provided some much-appreciated input to the formulation of this project. Lizzie acted as an external advisor, providing input to the questionnaire and the thematic analysis of the results. While the output is not a traditional academic report, Lizzie was happy to provide some relevant know-how. The ISF were very glad of her input, and reciprocated by running a Governance Workshop as part of the Block Mode version of the Security Management MSc module.

I believe that this first year of partnership between the ISG and ISF has demonstrated that the relationship has the potential to grow even deeper, providing ongoing mutual benefits based on the different types of expertise available within each group.

HP DAY 2011

The 22nd Hewlett-Packard Colloquium on Information Security was held at Royal Holloway on 19th December 2011. This annual event brings together the Information Security Group's partners from academia, industry and government in an informal and relaxed environment, to enjoy informative and entertaining talks, to network, and to properly start the wind-down to Christmas. Unlike last year, the weather held good and an audience of around 100 people attended on the day.

The event was formally opened by the Principal of Royal Holloway, Professor Paul Layzell. In his welcoming remarks he discussed the increasing profile and importance of cyber-security, as evidenced by the UK government's recently published strategy documents. This was followed by the award of the David Lindsay prize for the best MSc dissertation of the previous year, as judged by the British Computer Society - Information Security Specialist Group. This year the prize was awarded to Antony Bills for his dissertation on 'Practical Implementation of Grouping Proof for RFID'.

We were blessed with three very different invited talks this year. Michael Colao kicked proceedings off with a provocative talk on cloud computing and security, putting forward the dichotomy that everything and nothing changes with the advent of the cloud. His talk was highly entertaining and engaging, but also carried a serious message. Michael was followed on stage by Professor David Basin from ETH Zurich who gave an overview of his research group's efforts over the last 10 years to develop a method and tool support for enabling the modelling of secure software designs and to automatically transform these models into secure systems in the form of running code. This report from the frontiers of research into secure systems development was warmly welcomed by the audience. Finally, Rick Howard from Verisign/iDefense gave a fascinating insight into his team's work to 'reverse engineer' high profile hacking incidents using only information in the public domain. A particular focus was placed on Stuxnet, where Rick emphasized the degree of sophistication and planning that had gone into designing, launching and finally escalating the attack.

Professor Kenny Paterson, the event organiser said 'Once again, HP's invaluable support has enabled us to put together an exciting day of talks. We're already planning the 2012 event, and we encourage everyone in the ISG's extended network of friends to make sure we have your up-to-date contact details in our database. (Please advise us any change of details by sending them to Emma Mosley at isg@rhul.ac.uk).

RHUL MSC LAUNCHES IN ROME

By Chez Ciechanowicz

> Dr Chez Ciechanowicz is the MSc Information Security Programme Director.

Almost four years ago, a prospective student from Italy applied to Royal Holloway to study our MSc Information Security as a block mode student. After attending his first module, he was so impressed with the course that he wanted to set up something very similar in Italy.

Fast forward to Autumn 2011, and the student (Andrea Rigoni) was now Director General of the 'Global Cyber Security Center' (GCSEC) and Director of eCommerce in Poste Italiane. In the intervening years he had devoted a lot of effort in negotiating with Royal Holloway so that the MSc Information Security could be delivered in block mode in Rome. The contract was finally signed in August 2011 and the first module, which covered the Legal and Regulatory Aspects of Electronic Commerce, was delivered by Robert Carolina in February 2012.

A total of 20 students, from quite diverse backgrounds including MasterCard, Nato, Euroclear, and various Government Departments, are enrolled on the programme. While most of the students are from Italy, there are also students from Estonia, Mauritius, and Belgium.

I was delighted to formally launch the programme in Rome and to ensure that the administrative aspects were dealt with (and am pleased to say that I also managed to take a short break to visit St Peter's, which is absolutely awesome!!). We are looking forward to many years of fruitful engagement with GCSEC and the delivery of our MSc Information Security in Rome.

ISG AWARDED CENTRE OF EXCELLENCE STATUS

Royal Holloway, University of London has been recognised for its world class research in the field of cyber security by UK intelligence agencies GCHQ. The College is one of just eight institutions to receive Academic Centre of Excellence in Cyber Security Research (ACE-CSR) status.

Prof. Keith Martin said: *'The ISG is delighted that its long-standing reputation for research in cyber security has been recognised through this award to Royal Holloway. This sends a very positive signal to the outside world about the quality of our research, since we are one of a select few institutions to receive ACE-CSR status. We found the ACE-CSR application process to be a very positive experience, since it provided an opportunity to formally document the breadth and depth of cyber security research that has been undertaken by the ISG'.* Royal Holloway and the other Centres of Excellence will help make the UK government, business and consumers more resilient to cyber attack by extending knowledge and enhancing skills in cyber security.

RECENTLY COMPLETED PHD/ MPHIL THESES

Liang Chen
Analyzing and Developing role-Based Access Control Models

Carl Gebhardt
Towards Trustworthy Virtualisation: Improving the Trusted Virtual Infrastructure

Simeon Xenitellis (MPhil)
On the identification of security vulnerabilities

Saif Al-Kuwari
Forensic Tracking and Surveillance: Algorithms for Homogeneous and Heterogeneous Settings

Ziyad Al-Salloum
Topology-Aware Vulnerability Mitigation Worms

Arshad Ali
Linearisation Attacks on FCSR-based Stream Ciphers.

Georgios Kalogridis
Preemptive mobile code protection using spy agents

Ciaran Mullan
Some Results in Group-Based Cryptography

Anastasia Panoui
Wide-sense Fingerprinting Codes and Honeycomb Arrays

25th – 27th
June 2012

2012 ALUMNI CONFERENCE

Tickets for the 2012 Alumni Reunion Conference organised by the Information Security Group are now on sale.

The Conference will be held from 25th-27th June 2012 at the Windsor Building, Royal Holloway, University of London.

The conference will mark a significant event - the 20th anniversary of the MSc in Information Security here at RHUL. We do hope that you will be able to join us for what has proved to be a successful, interesting, educating and exciting event. Ticket price is £75 per person. This includes all lectures and presentations, refreshments, dinners and WIFI connectivity. The drinks reception will be covered by sponsorship. If you are interested in sponsoring this conference, please contact Emma on isg@rhul.ac.uk

We are pleased to announce two keynote speakers for the conference, Professor David Naccache (Professor at Université Paris II) and Dr Alastair MacWillson (Global Managing Director at Accenture Technology Consulting).

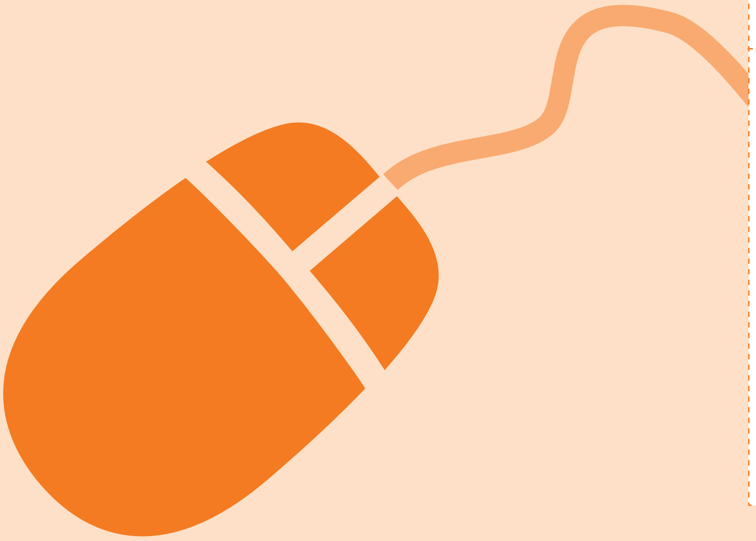
For further details, please visit our alumni page. Tickets can be purchased here. Any questions, please contact Emma on isg@rhul.ac.uk

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

Twitter:
http://twitter.com/isgnews

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

You Tube
http://www.youtube.com/user/UniofLondon



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