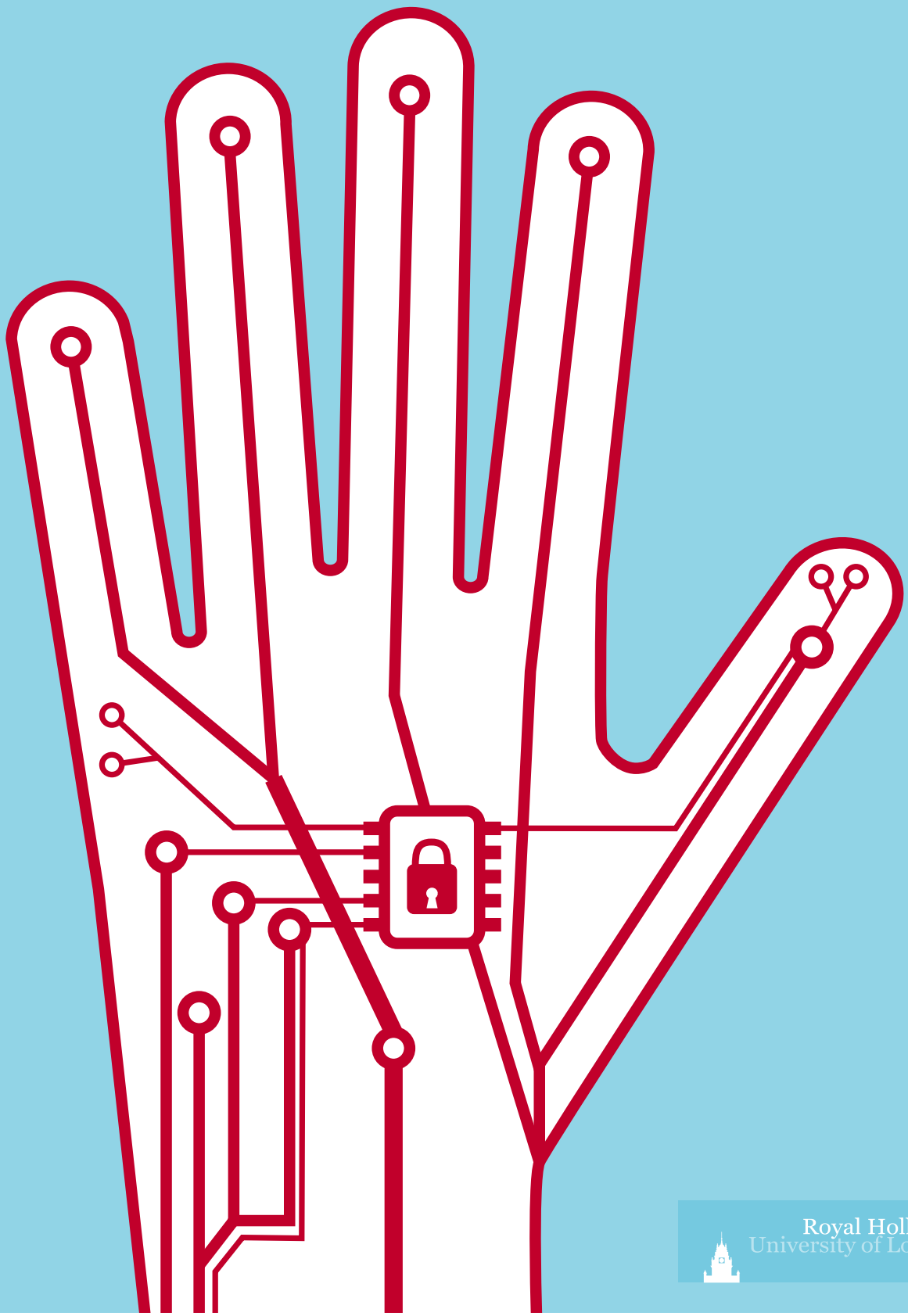
Information Security Group

Review 09/10



Royal Holloway
University of London

LETTER FROM THE ISG DIRECTOR

I am delighted to introduce the latest review newsletter of the Information Security Group at Royal Holloway, University of London. I hope that you will enjoy reading about the diversity of our activities.

Amongst the most exciting developments of the last 12 months has been the launch of a new MSc module on Digital Forensics. This is an increasingly important topic and one that we were keen to incorporate in our MSc Information Security programme. We hope that this will prove of interest not just to new students of the MSc programme, but potentially to some of our alumni, since all our modules are now available as stand-alone CPD courses.

Research lies at the heart of the ISG's activities, and I am particularly pleased to see a new branch of information security research establishing itself within the ISG. Dr Lizzie Coles-Kemp is leading the ISG's research effort in socio-technical aspects of information security, particularly concerning privacy and consent. This review newsletter features three articles relating to Lizzie's projects, including a fascinating discussion between a computer scientist, Dr Geraint Price, and a social scientist, Dr Iain Crimson, who is collaborating with Lizzie's research group.

Much of the research in the ISG is focussed around projects conducted by our PhD researchers. I hope that you enjoy the insights provided in this newsletter regarding some of their motivations, activities and aspirations.

I am also extremely excited by the prospect of our second alumni reunion conference in July 2010. The first event in 2008 was so successful that we now intend to hold these every second year. Our alumni represent an expanding global network of information security professionals and we are very proud of their achievements. I look forward to renewing old acquaintances in 2010.

Please do not hesitate to get in touch with us if you want more information about any of our activities, or feel that there are issues that we could explore together. We welcome engagement with all interested communities and look forward to hearing from you.

Professor Peter Wild

INDEX

SHORT NEWS BITES:

Dr Stephen Wolthusen was nominated as an adjunct professor in the Executive Master of Information Assurance Program at Virginia Tech University, Alexandria, VA, USA, and continues to serve on programme and steering committees including the established CRITIS conference series, where he will also serve as programme committee chair in 2010.

Professors Fred Piper and Peter Wild jointly presented a series of talks on the development of cryptography "From Black Art to Popular Science" in the St Andrews University School of Computer Science Distinguished Lecture Series 2009.

Dr Alex Dent was invited to speak at several international conferences and meetings in 2009, including the ECRYPT Summer School on Provable Security in Spain, the Provable Security conference in China, and the European PKI conferences in Italy. However, his personal highlight was a presentation on information security management given to the Aerospace and Defence Librarian's Group in London, which examined the way in which individuals perceive security within an organisation, and the different ways in which this can change over time.

The ISG has been collaborating with CREST (The Council of Registered Ethical Security Testers) in the professionalisation of the burgeoning security testing industry, and as part of these activities a joint conference was held at Royal Holloway on the 15th of December. The conference also had extensive backing and support from CESG, the UK's National Technical Authority for Information Assurance. A very encouraging aspect of the conference was the significant number of international participants, particularly from Germany, South Africa, and USA.

Dr Stephen Wolthusen gave an invited talk ``The Cyber Threat: Evolution and Outlook" at the January 2009 NATO Oberammergau Symposium in Oberammergau, Germany. He also gave a keynote talk on ``Mobility, Routing, and Computation in Ad-Hoc and Disruption-Tolerant Networks" at the 5th IEEE LCN Workshop on Security in Communications Networks held in Zurich, Switzerland in October 2009.

Prof. Chris Mitchell demonstrated his diverse interests in 2009 with three invited talks to very different audiences. In May he addressed The Claude Shannon Institute Workshop on Coding and Cryptography, University College Cork, Ireland on "A simple construction for perfect factors in the de Bruijn graph". In September he raised an important question during a keynote talk at the 5th International Conference on Global Security, Safety and Sustainability, University of East London: "Does provably secure cryptography guarantee practical security?" In October Chris presented "New technologies and future security challenges" at the event Cyber Security: A Public-Private Partnership: Government and Industry Working Together to Improve UK Cyber Security, Royal United Services Institute, London.

Prof. Paul Dorey has been appointed as a Visiting Professor to the ISG. Paul has a wealth of experience in many aspects of information security management, which he gained as a senior security and risk executive at Morgan Grenfell/Deutsche Bank, Barclays Bank and BP. The ISG is proud of its links with industry and government institutions and is very pleased to welcome Paul and looks forward to a fruitful association with him.

Prof. Chris Mitchell co-chaired three international conferences in 2009: Trust 2009; Workshop in Information Security Theory and Practice (WISTP 2009); International Conference on Information and Communications Security (ICICS 2009).

Prof. Michael Walker of the Information Security Group was honoured with an OBE in the Queen's Birthday Honours list. Prof. Walker, a part-time professor at Royal Holloway and the Vodafone Chair in Telecommunications, was awarded an OBE for services to the telecommunications industry. He commented: "I was delighted to receive the honour as it recognises not just my work but that of all the very talented colleagues I have worked with over the years".

The ISG and the Computer Science Department are collaborating to introduce a series of lectures given by distinguished scientists who have played a key role in the introduction of life-changing technology. The first one, which was sponsored by PGP Corporation, was delivered by Prof. Whitfield Diffie, a Visiting Professor at the ISG, who spoke on "The Emergence of Public Key Cryptography". The lecture was attended by over 350 people who had a thoroughly enjoyable, informative evening. It can be downloaded from http://www.isg.rhul.ac.uk/node/329

DIGITAL FORENSICS

Digital and Computational Forensics is a topic of increasing interest in both the end-user and academic communities. While postgraduate students in the ISG have pursued research in this area for a number of years, there has been no structured and formalised pathway into this field as part of the MSc Information Security. This has now been addressed by several co-ordinated developments.

Beginning in the 2009/10 academic year, students can choose an optional module *Digital Forensics*, which provides a structured overview of the key areas that forensic investigators and researchers must be familiar with. While the well-established and highly popular module *Computer Crime* focuses on organisational and procedural aspects, the *Digital Forensics* module aims to provide the technical underpinnings for host and network forensics, as well as an overview of related topics, including the infiltration and exfiltration techniques used by malicious code, steganographic and steganalytic methods, and nonstandard device forensics for mobile and database systems.

For students who wish to augment the theoretical foundations provided by the MSc module with practical experience and professional certification, an agreement with the SANS Institute has been reached to offer a customised version of the SANS course on Computer Forensics, Investigation, and Response in March 2010. The intensive three-day course, which is not part of the formal MSc program and is being offered at a discounted rate, will cover some of the more hands-on and practical aspects of computer forensics.

Anyone, including alumni, who wish to study this new module as a standalone CPD module should contact the ISG (or check the website) for details.

This effort to systematically strengthen teaching in digital forensics is complementary to current research work being conducted in the ISG under the supervision of Dr Stephen Wolthusen. Saif Al-Kuwari is conducting research on computational and digital forensics for mobile and vehicular systems, with an emphasis on tracking mechanisms. Forensic investigation of distributed, particularly cloud systems, is the subject of several new PhD research projects. Michael Gilhespy is studying forensics of distributed storage architectures, while Paul Wright is focusing on forensics and auditing mechanisms in distributed database systems. In both cases the federated and dynamic nature of these networks and services poses a number of interesting research problems. More cross-cutting concerns will be addressed in the research by Suaad Al-Alarifi, who is continuing research conducted during her MSc project by investigating the derivation, transmission, and validation of appropriate metrics for security properties in distributed systems.

This activity on digital forensics was recognised, when Dr Stephen Wolthusen was invited to give the keynote talk "Overcast: Forensic Discovery in Cloud Environments" at the 5th International Conference on IT Security Incident Management and IT Forensics, held in September 2009 in Stuttgart, Germany.

FUTURE CSOs ADVISING CURRENT CSOs?

By Alex Dent

The ISG's MSc programme in Information Security is aimed at producing high quality information security professionals and we like to celebrate success when we see it. One of the ways in which we enjoy rewarding excellence is through awards for outstanding theses. In order to produce a high quality thesis, a student has to combine a keen understanding of information security principles with sound research skills and an independent work ethic. This makes it one of the hardest parts of the degree programme.

The ISG offers two different types of thesis prize. The David Lindsay prize is awarded by the British Computer Society's Computer Security Specialist Group to the project that best addresses innovative applications of information security within the field of computer science. The Search Security prizes are awarded to theses which effectively communicate research topics of relevance to information security managers and professionals. The winners of these prizes are invited to submit articles for publication on SearchSecurity.co.uk.

The goal of the Search Security award scheme is to produce thoughtful, well-written and accessible explanations of topical subjects. I think it is a testament to the skills of the Search Security prize winners that they are able to produce not only excellent technical theses, but also interesting short articles. And it is pleasing to hear that the articles are valued by information security professionals. Paul Dorey, president of the IISP, said of the articles that it was "encouraging to see students developing security knowledge that they can take forward into their careers" and that he was going to be "busy for weeks giving justice to all the good work" (IISP newsletter, June 2009).

The production of these articles provides the ISG with the opportunity to showcase its most talented students, while the students get recognition for their hard work. Christian Bonnici, a previous recipient of the Search Security award and now a PhD researcher in the ISG, commented that "writing about past academic research has encouraged me to further develop my ability to present work in different, and perhaps more attractive, formats; to a novel researcher this is an encouraging process since it incubates a knowledge sharing attitude". Ron Condon, UK Bureau Chief for SearchSecurity.co.uk, is delighted with the results of this partnership:

"The partnership between Search Security and RHUL, which began two years ago, has been extremely valuable for us and, I believe, for the authors whose papers we have featured. The information security professionals who visit our site are hungry for knowledge that will help them in the unending battle to defend their systems. We know that they have found the RHUL papers very valuable and I know authors have received a great deal of positive feedback. In the last two years, the papers have covered a vast range of subjects, and each has thrown fresh light on their particular areas of interest. I have been delighted to make them available to our professional audience, and I look forward to seeing what next year's batch will bring."

We also look forward to seeing the best of the future Master's student theses and rewarding their authors for their efforts.

The 2008 Search Security award winners were:

- **Interdomain Routing Security (BGP-4): A Comparison between S-BGP and soBGP by Rostom Zouaghi, supervised by Steven Wolthusen.**
- **Maximising the Effectiveness of Information Security Awareness Using Marketing and Psychology Principles by Geordie Stewart, supervised by John Austen.**
- **Information Security Awareness: An Innovation Approach by Carlos Orozco Corona, supervised by John Austen.**
- **Fuzzing for Software Vulnerability Discovery by Toby Clarke, supervised by Jason Crampton.**
- **Applying Misuse Cases to Improve the Security of Information Systems by John Neil Ruck, supervised by Geraint Price.**
- **Buffer Overflows in the Microsoft Windows Environment by Parvez Anwar, supervised by Andreas Fuchsberger.**
- **Management of Risks associated with De-perimeterisation by Kwok Keong Lee, supervised by Peter Wild.**
- **Digital Rights Management: Towards a Balance between Copyright Rights and Fair Use exceptions by Christian Bonnici, supervised by Keith Martin.**
- **Extending Secure Execution Environments Beyond the TPM by Talha Tariq, supervised by Chris Mitchell.**

SearchSecurity.com

SECURING THE SWARM
By Fiona Higgins

Swarm robotics is a relatively new technology that shows great potential for a variety of different applications and environments. As with many technologies, there is no definition of swarm robotics which engenders universal agreement. However, one that is widely accepted was suggested by Erol Sahin who is a prominent researcher in the field. He stated that “Swarm Robotics is the study of how large numbers of relatively simple physically embodied agents can be designed such that a desired collective behaviour emerges from the local interactions among agents and between the agents and the environment”. One key assumption is that the robots are strongly autonomous – meaning that not only do they act without exterior intervention, but that they also have the power of self-government.

Robots are capable of not only sensing information, but having the potential to be able to act, if necessary. The large number of robots in a swarm enables it to act quickly and reliably, the latter largely due to the fact that the loss of one unit has little effect on the overall performance. Swarms of robots are already under development, and are being tested in diverse applications, such as military intelligence gathering in dangerous areas, space missions, environmental monitoring, toxic agent clearance, performing routine tasks in a hospital, and disaster relief.

Previous emerging technologies have often overlooked security until later developmental stages, when it has had to be undesirably (and sometimes expensively) retrofitted. Before the ISG started investigating, there had been little research into security for swarm robotics. Fiona Higgins, Allan Tomlinson and Keith Martin wrote a first position paper in the area, “Survey on Security Challenges for Swarm Robotics”, which won a best paper award at the Fifth International Conference on Autonomic and Autonomous Systems, held in April 2009. Fiona is now following on from this paper by investigating the concept of identity within the swarm.

THE VALUE OF AN INTERNSHIP
By Carlo Gebhardt

I am a third-year PhD student with interests in virtualisation, trusted computing and operating system security. Last year, when I was offered the opportunity to conduct an internship at the Hewlett-Packard Research Labs in Bristol, I did not hesitate for a second. Not only because working in a corporate research facility was something I was already familiar with, but also because I saw how this could benefit me personally, as well as benefit my research. Technology excites me, and at HP labs I had the opportunity to work with cutting-edge equipment and prototypes before they were even announced to the public.

So why do I think internships are worth doing? Apart from access to specialist equipment, the staff in the research labs are leaders in their fields. Working together with experts, and being part of a successful team, is more than simply a lesson learned and a skill put on a CV – it is a unique experience. The outcome of my research internship has also been very beneficial for my academic career in the form of several publications. The ability to combine academic research and practical skills can stand out in a competitive job market. It also renders candidates more marketable to future employers. Also, the business contacts gained during an internship can enhance personal networks and can help jumpstart a career. And of course towards the end of your studies it can be very beneficial to have had an internship position; around 80% of available jobs are not advertised externally. Therefore there is always the possibility of turning a successful internship into a job.

Internships are more common in the rest of Europe than they are here in the United Kingdom. I, for example, did not start my PhD straight after graduating from university. I looked around before, and while studying at, undergraduate level. My past internships have also washed me up at interesting places all over the world, for instance New Zealand. To all the work side, there is also a fun side!

HP encourages students who are enthusiastic about Information Security to explore the possibility of an internship by sending a CV to Richard Brown (richard.brown@hp.com), detailing any previous work experience and particular areas of research interest.

Myself? I am currently planning my next internship with another global player in the IT industry, shortly after graduating.

THE 20TH HEWLETT-PACKARD COLLOQUIUM ON INFORMATION SECURITY
By Kenny Paterson

Thanks to the continued generous sponsorship of Hewlett-Packard Laboratories, the ISG hosted the 20th annual Colloquium on Information Security on 14th December 2009. This event brings together the ISG community in its widest sense - our staff, PhD students, postdocs, and partners from industry, academia and government. We were fortunate to have three exceptionally strong speakers this year - Gregoire Ribordy, CEO of id Quantique, Alan Paller, Director of Research at the SANS Institute, and Colin Whittaker, Head of Security at UK Payments Administration.

In his talk, Gregoire Ribordy gave a lucid and accessible account of quantum key distribution, explaining the fundamental physical phenomena that give rise to this approach to key management, discussing the technology being used by id Quantique to build commercial quantum key distribution systems, and providing a refreshingly frank assessment of the challenges facing the technology as it becomes a commercial proposition.

In his talk entitled “Surprisingly effective leverage points for broad and rapid improvement of computer security”, Alan Paller focussed on practical methods that can be used to bring about significant and lasting changes in security practices within organisations. His talk was both highly entertaining and informative, and drew upon his substantial experience in working in the US government and defence sectors. He emphasised the need for “doing it for real”, with themes of his talk being that offence can be used to inform defence, and the use of effective and meaningful security metrics to bring about change.

Our final speaker, Colin Whittaker, reflected on the journey that has been taken by the UK Financial Sector in improving customer authentication methods since 2001. His talk, “Customer Authentication: The journey from Legoland to Nirvana, are we there yet?”, touched on many facets of the problem, including the challenges of building consensus within a membership-based organisation, and the balance to be struck between cooperation and competition when promoting new technology adoption in the banking industry. He spoke about the EMV CAP standard and its successful application in reducing online banking fraud, as well as the challenges of designing and deploying a usable security technology.

As usual, the talks were accompanied by plenty of tea, coffee, sandwiches and discussion in the foyer of the Windsor building. Around 15 posters produced by ISG PhD students were on display, and these attracted a steady stream of visitors. Topics were as diverse as “Time Specific Encryption” and “Differential Power Analysis of AES Implementations on PIC chips”. Our colleagues from HP also provided a new edition of the Stefek Zaba memorial crypto challenge. This year, the solution required a combination of visual cryptanalysis and breaking a playfair cipher. It was solved in record time by a team of eagle-eyed cryptanalysts - Matthew Dodd and Steve Babbage. It was great to see Steve putting his Royal Holloway training to good use!

TAKING SECURITY SERIOUSLY IN NIGERIA
By Keith Martin

The 2009/10 academic year saw a surprising increase in the number of Nigerian students joining the MSc Information Security Programme. More intriguing still was that almost none of the new students were aware of each other's existence before commencing the programme. Nigeria has a slightly tarnished name in information security circles, largely because of the prolific email fraud schemes that almost every Inbox on the planet must have encountered at some stage. So has Nigeria started to take information security seriously? And, if so, why now?

Probably the most experienced of the new MSc students is Olutoyin Oloniteru, who is Group Head of Information Technology and Strategic Marketing at 3Line Card Management Limited, Lagos. His company engages in transaction processing, switching, card personalization and point of sales terminal deployment. Olutoyin was formerly with ATM Consortium Limited, Nigeria's main deployer of ATMs. Olutoyin recognises the need for building up information security expertise in Nigeria. "Nigeria's information security infrastructure is still in its infancy. It is mainly private sector driven at present and there are many interoperability and integration issues. For example, right now there is migration from magnetic stripe to EMV card solutions and we have observed some problems already, since some of the current solutions are vendor based. We've also had some high-profile incidents of fraud. Some fraudsters even cloned the website of one of the major e-payment switches in Nigeria, requesting cardholders to send their card details due to a certain upgrade that was allegedly to be done on the network. And there will be many more incidents to come! You can imagine, for a country with over 150 million people".

Olutoyin believes that this is a very exciting time for Nigerian students to establish a career in information security because there are so many new projects starting up. "Right now in Nigeria, on behalf of my current company, I am working on a transport ticketing solution for the Lekki-Epe Expressway in Nigeria. Three toll plazas will be built, where drivers or vehicles passing through the plazas will be expected to pay toll charges either using their ATM/Debit cards or using RFID tags on their vehicle's windscreen. The ATM/Debit cards are expected to be used to make payments on point-of-sale terminals using contactless smartcards. Also, we have the "Freedom Card", which is a prepaid platform that we are deploying for the purpose of banking on the street in Nigeria. The card will be used for light banking services such as cash withdrawals and money transfers at merchant point-of-sale terminals. And we have over 60 million mobile phone users, so mobile payments are in the offing. At the centre of all these is information security".

Adeniran Seriki is a Nigerian currently working in the U.K. for the London Borough of Hounslow as the IT Carezone Officer, providing a link between IT and social services. Adeniran believes that the profile of information security is on the rise in Nigeria. "Information security incidents are now widely reported in Nigeria, which perhaps adds to the nation's relatively poor international reputation in this field. Nigeria is just developing an information security structure, especially with the recent introduction of the card payment systems in the banks. I think that the increase in Nigerian students coming on the Royal Holloway MSc could well be through a desire to seize the new career opportunities arising through the emerging national information security infrastructure". This is confirmed by Andrew Lori-Skinn who was attracted to the MSc because he identified a dearth of personnel skilled in this area at his workplace. "I think people perceive that there are opportunities for good career prospects because of the specialized skills, which are currently not available in Nigeria".

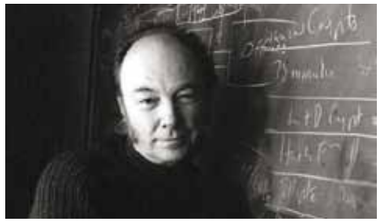
One of the areas of concern in Nigeria is the lack of a regulatory environment within which to apply information security practices. Fola Ogunsola is an experienced Nigerian IT professional who is hoping to specialise in this aspect of information security. "Nigeria does not have sufficient enabling laws in place for businesses to comply with. Those that do exist are neither well publicised nor being enforced. Some businesses do comply with some international regulations, more as a requirement from, or in order to be comparable to, their international business partners or competitors".

Olatunde Idowu is one of the Nigerian students who does not have a background in information security and came to Royal Holloway to establish a new career, but not before doing some homework. "I talked to a Nigerian lawyer before I came on the course who told me that electronic evidence is not accepted in Nigerian courts because the Evidence Act does not support it". Lawrence Soremi, who is currently based in the U.K. agrees. "There is an urgent need to put in place necessary legislation so that the perpetrators of computer-related fraud can be tried in the court of law".

Like several of the other students, Olutoyin Oloniteru has ambitions to change this situation. "I am motivated to study the MSc Information Security not just for career enhancement, but also because of its national and public service utility. I hope to be able to assist my home government in the areas of law making, regulation and policy design in the areas of e-commerce, digital signatures, review of the Evidence Act, and policies on forensic technology and its applications".

Olutoyin is convinced that the ISG has a genuine role to play in helping Nigeria develop its security infrastructure. "Nigeria has a large population that needs to be educated. British universities such as Royal Holloway are of great influence in this regard. For me, the ISG offers a unique course with a distinct pedigree. As a bonus, Royal Holloway is located close to London. As a working professional, I am taking full benefit of the block mode delivery of the MSc. I can fly from Lagos directly to Heathrow and then it is just a very short hop to the campus. For me, it's perfect".

Lawrence Soremi thinks that this is just the start of a stronger relationship. "With even more Nigerian students on the course this year, I am convinced that the reputation of the MSc will spread quickly. I believe that there are going to be even more Nigerian students next academic year". Whether Lawrence is right or not, it is fascinating to learn about a nation building its information security infrastructure based on the experience of some of those who have gone before. Even more exciting is to meet the future professionals who will help to make it happen. Nigeria does seem to be taking information security seriously, and we wish these students well in their studies and future careers.



ALUMNI CHAPTERS AND IISP HELP TO UPDATE 'THE KNOWLEDGE'
By Fred Piper

It has always been recognised that most university degrees are "snapshot" assessments of a person's knowledge and understanding at a specific time. There are no follow up processes for ensuring that the recipient of a degree keeps their knowledge up to date or that they have any experience of implementing what they have learnt. This can cause problems for potential employers, particularly in a dynamically changing topic like Information Security.

The introduction of the block mode (and distance learning) delivery of a number of our MSc modules enables us to offer them as stand-alone CPD or CPE courses for alumni and is a small contribution to addressing the "how do we stay up to date?' issue. Similarly, the introduction of some extra technical modules and a number of industry provided hands-on workshops have allowed us to add more practical experience to the degree programme.

As a result of the July 2008 alumni reunion conference, many countries have formed alumni chapters. Not surprisingly these chapters vary in size and in the level of activity, ranging from (greatly appreciated and enjoyable!) social gatherings when ISG members visit the country to holding regular seminars and networking events. Such seminars provide yet another route by which alumni members can refresh their knowledge.

One example is the London Chapter, which holds seminars at roughly two monthly intervals. It invites speakers and attendees not only from the alumni chapter, but also from the company that hosts the event and also the Institute of Information Security Professionals (IISP). This means that they can have up to 60 or 70 attendees and leads to lively, informative debates.

IISP is a very interesting organisation with the potential to solve both the "is their knowledge up to date?" and "do they have any real experience?" issues. It was formed partly as an attempt to help employers answer the question "how can I recognise an Information Security professional?" and provides a competency/skill based qualification. It has the potential to provide information Security with the professional body that it requires and has received considerable backing from UK Government and a large number of corporates (See www.instisp.com for details).

After a slow start, IISP now has tried and tested processes for handling applications for associate and full membership. The standards are high and the application process can be time consuming. Significantly, jobs are starting to appear that list A.Inst.ISP and M.Inst. ISP as suitable qualifications for specialist Information Security positions. Aiming for M.Inst.ISP might be an excellent way for alumni to establish that they have kept their knowledge up to date and that they have gained sufficient experience. (In fact, apart from personal references from employers, it may be the only way.)

IISP's other activities are also gaining momentum and the website provides details of some recent innovations like its Graduate Development programme, its mentoring scheme and its Top Gun programme. Although it is UK based, IISP has many international members. Furthermore, other countries are showing interest in either joining with IISP or using it as a model for their own professional body.

Although it has existed for a few years now, I have so far avoided recommending that ISG members and/or alumni should consider joining IISP. However it is now mature enough and sufficiently well-established that my position is changing. I think it represents a unique opportunity to unite the Information Security profession.

Will it succeed? Unfortunately this is still not clear. There is an almost classical dilemma. In order to have real credibility, IISP needs to reach a critical mass of full members but the "what's in it for me?" reasoning means that people will not want to join until it has that credibility. My personal perspective is that it is in everyone's interests, (universities, companies, Governments and individuals) for IISP to succeed.

There are now over 1500 ISG alumni with an excellent knowledge-based qualification. For "junior" alumni, the IISP badge will tell employers that they have experience to back up their knowledge. For "senior" alumni, the IISP badge provides a means of identifying potential employees. I believe that anyone who sees these membership benefits should join and contribute effort to make sure that the IISP is successful.

ALUMNI REUNION CONFERENCE 2010

The ISG is holding its second Alumni Reunion Conference on the 5th, 6th and 7th of July 2010. After the huge success of our first ever alumni reunion conference in July 2008, it has been decided that these conferences will be held every other year.

The format of the conference will be very similar to the first one and will consist of two and a half days of presentations given exclusively by our alumni. In addition to this, there will be two keynote sessions delivered by invited external speakers. (In 2008 we had Rob Carolina and Whitfield Diffie.)

The cost for attending the conference will be £50. If you want to find out what happened in 2008, do have a look at http://www.isg.rhul.ac.uk/alumniconference08/information and also look at the conference programme details on this page.

To book a place at the conference please register at the RHUL online store.

We hope that many of our alumni will attend the event, to re-establish old links, make new links, learn something new, and of course have a lot of fun!

ALUMNI CHAPTER NEWS

• Cyprus

Cyprus ISG Alumni was formed back in April 2008, with myself, Margaret Georgiou, as the local contact. I initially formed a Google group where everyone I knew from the RHUL ISGroup was invited to join. The group now has 12 members and is still growing. The members are not only located in Cyprus. We have one member living in California and a member from Taiwan who currently lives in Cyprus.

We had our first physical meeting during Fred Piper's visit to Cyprus for the Information Security Conference that was organized by the Cyprus Computer Society on the 5th of November 2009. We went out for a very enjoyable dinner, which almost every member attended. Our next step is to find more local members. Fred has volunteered to search the ISG's database and send us names of other graduates from Cyprus. We also plan to hold more gatherings in the near future in order to make the group more active. Please get in touch if you wish to join us!

Margaret Georgiou

• UAE

Within the UAE, Dr Chan Yeun and I organised the first GCC Region ISG Alumni Conference on 24th March, 2009 at Khalifa University in Sharjah, UAE. It was well attended with alumni and industry representatives from across the UAE, Oman and even Pakistan. It also coincided with Fred Piper's visit to Khalifa University. Overall the feedback was that it was a good opportunity to discuss Infosec initiatives across the region and catch-up with other alumni.

The alumni conference included a keynote presentation by Fred on the application of cryptography, as well as talks by Chan on ubiquitous network security, Fauzan Mirza on digital forensics, Anees Rahiman on digital signatures for long-term archiving and myself on advanced digital signatures for PDF documents. In addition to this, Chan, Dr Arafat Al-Dweik and I presented a workshop at the National Security Middle East 2009 Conference on 21st June. This workshop had over 40 delegates, with representatives from Government and Industry. We hope to organise further meetings in 2010 and anyone interested should get in touch with me.

Liaquat Khan

• Greece

Nikolaos Virvilis and Konstantinos Papapanagiotou are the two contacts for ISG alumni in Greece. The majority of the MSc graduates are located in Athens, so all our meetings take place there. We have created our own Google Group that we use to post anything relevant to the chapter, such as meetings and events. The group has 38 members as of November 2009. Although we don't have fixed dates for meetings, we usually meet once every two months for a drink or dinner.

Apart from the casual meetings, there is the idea of having very short presentations every time we meet (about 30 minutes) in order to give an additional value to our meetings by sharing knowledge and experience. Almost all graduates in Greece are working in information security related positions, in banks, consultancy companies, government and universities, so sharing experiences is very beneficial. We are looking forward to meeting new alumni as there are still many that are not aware of the group and the meetings.

Nikolaos Virvilis

• London

The first gathering of the London chapter of the ISG alumni took place in November 2008 and was an informal evening in a pub near Waterloo Station. Since this beginning, several events have been organised, which have been increasingly well attended.

The first of these was hosted by Barclays Bank and, after it had to be rescheduled due to the severe weather in February, was finally held in April 2009. It was opened by Fred Piper, who introduced Piers Wilson's presentation on 'Information Security issues for 2009'. The second event was held in June 2009 at Deloittes in the City and featured Robert Carolina who gave a talk on the 'De-globalisation of the internet'. The most recent event in September 2009 was again hosted by Barclays and included the speakers Mike Maddison on the topic 'Value for Security Spend', Nick Humphrey on the topic 'Protective Monitoring – Challenges for the 21st Century' and Andrew Yeomans on the topic 'Clouds forecast – doing business beyond the perimeter'. There were over 60 attendees at this event.

At the time of writing the next scheduled event will be held on the 24th November 2009 at Deloittes and will feature talks by Graham Palmer on '2010: More of the Same' and Owen Brady on the 'Anatomy of an insider dealing offence'. A varied programme of events is already being planned for 2010.

Fiona Higgins

• Bedfordshire/ Buckinghamshire/Oxford

The alumni chapter that I attend (Beds/Bucks/Oxford) meets quarterly and involves a social get-together, usually at a good Indian restaurant. This chapter spawned from a support group that David Alexander set up for distance learning students of the MSc. Other than having a chat (and the odd moan!) it acts as a good forum for discussing, implementing and practicing information security domains across a diverse range of organisations. The most recent meeting discussed CLAS membership and the approval process. We'd be delighted to have new members in the region.

Gary Dooley

• Korea

ISG-Korea Alumni's year-end event was held on 9th of December 2009. This was the fourth time ISG-Korea members have met together in 2009. We met in an English-style pub called "JAY PUB", where most people ordered beers that we usually drank in pubs in the UK! The group normally meet a couple of times each year, with additional meetings if an ISG member visits Korea.

Taewan Park

Full list of Alumni chapters from around the world:

Austria / Australia / Belgium / Brazil/ Canada /China / Columbia / Cyprus / Egypt / France / Germany / GCC region / Ghana / Greece / Hong Kong / Iceland / India / Ireland / Israel / Japan / Korea / Lebanon / Malaysia / Malta /Mexico / New Zealand / Nigeria / NORDIC Saudi Arabia / Singapore / Spain / Sri Lanka / Sudan / Switzerland / Taiwan / UAE (United Arab Emirates) **/ UK** (Beds / Bucks / Oxfordshire / London / Manchester / West Midlands / Egham / Hampshire / Reading) **/ Ukraine / USA**

More information about the chapters can be found at:
http://www.isg.rhul.ac.uk/alumni/chapters

• Chapter locations

PHD PROFILES

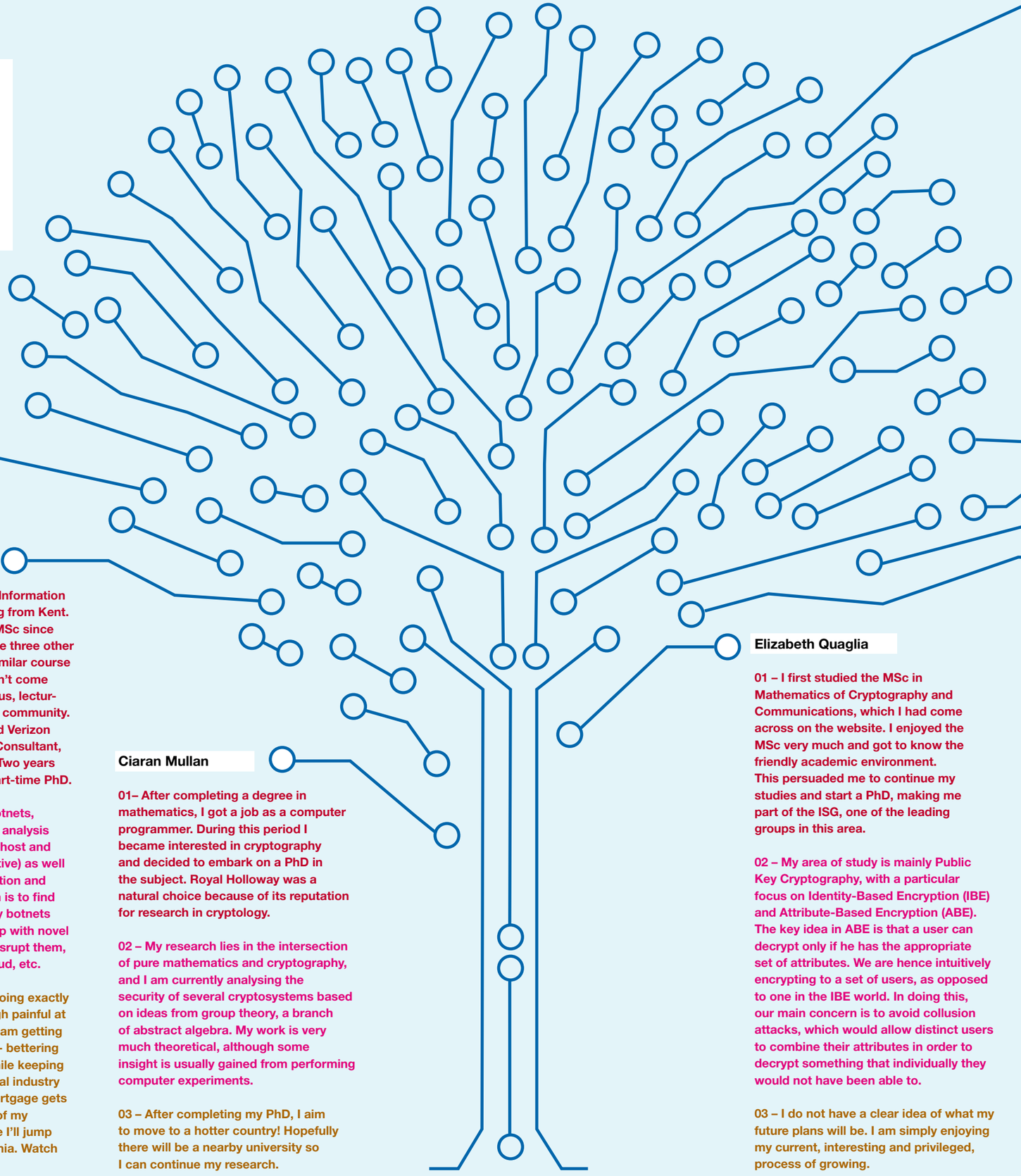
The ISG is proud of its strong cohort of PhD researchers, but who are they and what do they do?

We asked the 2008 intake:

01. Why did you come to Royal Holloway?

02. What is your research about?

03. What do you want to be when you grow up?



Nick Humphrey

01 – I'd heard of the ISG whilst I was working at the Ministry of Defence. Colleagues both inside and outside government considered the ISG to be of very high quality. After graduating from the MSc, coming back to study a PhD seemed the natural thing to do.

02 – My research is looking at protective monitoring. This concerns how we are able to audit access to information and systems, ultimately holding individuals accountable for their actions. Protective monitoring involves technology and business processes, requiring consideration of operational needs, legislation and governance, in addition to systems design and network architecture. One of the major problems is a lack of standards around the taxonomy, syntax and transport of audit data. Having to consolidate disparate, large, inconsistent and poor quality audit data sources makes the difficult task of auditing even harder still.

03 – I've been working happily in information security since 1998 and feel very fortunate to work in a field I genuinely find fascinating. In terms of the future beyond the PhD, I hope that some of the research I do may play a part, however small, in improving how we deal with issues of accountability, trust and the secure sharing of information.

Tom Neaves

01 – I came on the MSc Information Security after graduating from Kent. I had wanted to do the MSc since my A-Levels! There were three other universities offering a similar course at the time, but they didn't come close to the ISG's syllabus, lecturers, and active research community. After graduation, I joined Verizon Business as a Security Consultant, but couldn't stay away. Two years later I signed up for a part-time PhD.

02 – I am looking into botnets, which includes in-depth analysis of the bots (from both a host and network based perspective) as well as looking at their evolution and possible trends. My aim is to find vulnerabilities in the way botnets work in order to come up with novel ways to detect and to disrupt them, thus reducing spam, fraud, etc.

03 – I want to carry on doing exactly what I'm doing. Although painful at times (and hard work), I am getting the best of both worlds - bettering myself academically, while keeping current in the commercial industry and making sure the mortgage gets paid! After completion of my PhD who knows? Maybe I'll jump a little more into academia. Watch this space…

Ciaran Mullan

01– After completing a degree in mathematics, I got a job as a computer programmer. During this period I became interested in cryptography and decided to embark on a PhD in the subject. Royal Holloway was a natural choice because of its reputation for research in cryptology.

02 – My research lies in the intersection of pure mathematics and cryptography, and I am currently analysing the security of several cryptosystems based on ideas from group theory, a branch of abstract algebra. My work is very much theoretical, although some insight is usually gained from performing computer experiments.

03 – After completing my PhD, I aim to move to a hotter country! Hopefully there will be a nearby university so I can continue my research.

Rosli Daud

01 – I came to know about the ISG when I was internet searching for places to do my PhD research in cryptography. The ISG is one of the most reputable academic security research groups in the world, so I decided to be part of it.

02 – My research is on cryptographic access control and its applications. One way to enforce an access control policy is to encrypt the objects and then allocate the decryption keys to users in an appropriate way. My project models this problem mathematically, with the intention of comparing different schemes for the provision of cryptographic access control.

03 – Well, this is quite simple. I want to be happy, be a better person for my loved ones, contribute to society, have a better career, and many friends! (That's not asking too much is it?)

Elizabeth Quaglia

01 – I first studied the MSc in Mathematics of Cryptography and Communications, which I had come across on the website. I enjoyed the MSc very much and got to know the friendly academic environment. This persuaded me to continue my studies and start a PhD, making me part of the ISG, one of the leading groups in this area.

02 – My area of study is mainly Public Key Cryptography, with a particular focus on Identity-Based Encryption (IBE) and Attribute-Based Encryption (ABE). The key idea in ABE is that a user can decrypt only if he has the appropriate set of attributes. We are hence intuitively encrypting to a set of users, as opposed to one in the IBE world. In doing this, our main concern is to avoid collusion attacks, which would allow distinct users to combine their attributes in order to decrypt something that individually they would not have been able to.

03 – I do not have a clear idea of what my future plans will be. I am simply enjoying my current, interesting and privileged, process of growing.

Amizah Malip

01 – A few months before completing my first degree, I came across a poster about an International Symposium related to Cryptography and Information Security posted on the faculty's board. I chose to continue with an MSc and a PhD at Royal Holloway because the ISG offers recognised expertise in theoretical foundations and practical applications of cryptography.

02 – I am currently studying the security of message authentication protocols using two-channel cryptography. The two channels are comprised of an insecure broadband channel, such as a wireless channel, and an authenticated narrowband channel, such as voice over internet protocol (VoIP). When two small devices intend to establish a secure key, and we assume there is no public key infrastructure or available secure channel, the flow of information will be sent over these two channels. The authenticated tag transmitted over the narrowband channel will then be used to authenticate the long message sent over the broadband channel.

03 – My goal is to teach mathematics, especially related to cryptography, and hopefully be able to convey to my students my own passion for the subject. The best teachers I have known have been those whose fascination with their own subject has shone through and animated them.

Qin Li

01 – Before my PhD studies , I studied a Master's degree in Information Security at RMIT, Australia. I became fascinated by the art of information security there. After consulting with some professors, I learned that Royal Holloway is one of a few universities which are academically excellent, and have strong connections with the information security industry. Then I made a life-changing decision to pursue a PhD degree.

02 – My PhD research topic is about security of feedback mechanisms, for example the well-known eBay feedback forum. As online activities have become more popular, feedback mechanisms become increasingly important as a means of establishing trust among entities who barely know each other. So I am devoting my efforts to making feedback mechanisms more secure, accurate and efficient.

03 – Although I don't know exactly where I am going to be, I would like to continue to challenge and excel myself in the field of information security. Changing the world is probably too ambitious, so I will settle for any position where my intellectual and professional contribution will make a real difference.

Saif Alkuwari

01 – Royal Holloway was recommended to me by another PhD student. The decision to come was one of the best decisions I ever made. What really attracted me is the quality of research being undertaken in the ISG. I envisioned a unique research experience here, and this is exactly what I have had so far. The ISG has around 40 PhD students and 20 staff, making it one of the biggest security research groups. That, on its own, was a sufficient reason for me to join.

02 – I am mainly interested in cybercrime and digital forensics. In my research, I try to investigate and develop algorithms for crime detection and prevention. In particular, I've done some work in the localization and tracking of criminals in mobile and vehicular ad hoc networks. Currently, I am conducting research on digital forensics, where we try to extract electronic evidence from digital devices left at crime scenes.

03 – After graduation I will go back to work in my country (Qatar) for the Ministry of Foreign Affairs, which has been sponsoring me since I started this degree. If time allows, I also hope to teach at Carnegie Mellon University, which has recently opened a branch in Qatar.

Wei Zhang

01 – I came to Royal Holloway because the ISG is world famous. I have a mathematical background. I enjoyed number theory very much and wanted to apply it to cryptography. The ISG is one of the best places in the world to study cryptography. The first time I heard about its fame was when I read the book 'The Da Vinci Code'. Then I looked it up on the internet and I was amazed by Founder's Building!

02 – My research is about provable security and digital signatures. A digital signature scheme can be used to demonstrate the authenticity of a digital message or document. Provable security is about proving that a cryptographic scheme is 'secure' mathematically. We model the real-life scenario mathematically and try to prove that the scheme meets all the security requirements.

03 – Perhaps I will become a secret agent who works for justice! Alternatively, I would be very happy if I could solve the Goldbach's Conjecture or the twin prime problem… Yes, I'm a dreamer!

RECENTLY COMPLETED PHD THESES…

Raminder Ruprai
Improvements to the Gaudry-Schost Algorithm for Multidimensional Discrete Logarithm Problems and Applications

Boyeon Song
RFID Authentication Protocols Using Symmetric Cryptography

Markku Saarinen
Cryptanalysis of Dedicated Cryptographic Hash Functions

Hemanth Khambhammettu
Enforcing Complex Policies in Role-based Access Control

Steffen Reidt
Efficient, Reliable and Secure Distributed Protocols for MANETs

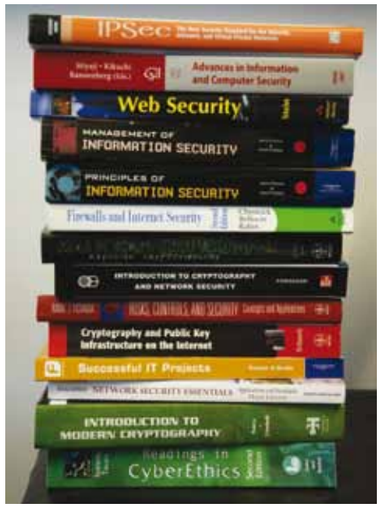
Thomas Page
The Application of Hash Chains and Hash Structures to Cryptography

Adrian Leung
Securing Mobile Services Using Trusted Computing

Geong Sen Poh
Design and Analysis of Fair Content Tracing Protocols

Arnold Yau
Side Channel Analyses of CBC Mode Encryption

Sharon Nachtigal
E-business Information Systems Security Design Paradigm and Model



NEW STUDY FINDS FLAW WITH INTERNET SECURITY

A new study has revealed a security flaw within the network protocol SSH which could allow attackers to access sensitive data even though it is encrypted using state-of-the-art techniques. Prof. Kenny Paterson presented the findings at the leading annual security conference, the IEEE Symposium on Security and Privacy in California, USA, on 18 May 2009.

Originally designed as a replacement for insecure remote login procedures such as rlogin and telnet, SSH was regarded as impenetrable. SSH aims to provide a secure channel between networked devices by encrypting and integrity-protecting data. SSH is widely used by system administrators to allow them to securely access remote systems and to transfer sensitive data across the Internet. OpenSSH is the leading SSH implementation, accounting for more than 80% of SSH implementations on the Internet.

Working with two PhD students from the ISG, Martin Albrecht and Gaven Watson, who is sponsored by BT Research, Kenny and his team discovered a basic design flaw which opens up the possibility of limited plaintext recovery attacks against SSH. "It is amazing to think that a short e-mail from Kenny suggesting a paper I should take a look at, resulted in us researching exactly how SSH is implemented and ultimately led us to finding attacks against SSH", says Gaven Watson.

The team's attacks against the Open SSH implementation of SSH exploit subtle differences in the way in which the software reacts when it encounters errors during cryptographic processing. Kenny comments, "While the attacks have low success probabilities, it should be kept in mind that SSH is regarded as being a bullet-proof protocol and is widely used to protect remote logins to sensitive systems. So it's arguable that finding any chink in SSH's armour represents a significant result".

Paul Kearney, Chief Security Research Professional in BT's Centre for Information and Security Systems Research, comments, "SSH is one of the main pillars of internet security, so it is vital that any vulnerability is picked up early and eradicated. Professor Paterson's team are playing an important role in protecting the digital networked economy, and I'm delighted that BT's sponsorship has enabled this work to be done. This is a great example of BT's open innovation strategy in action". The ISG team worked with the UK's Centre for Protection of National Infrastructure (CPNI) to disclose the attacks and ways of protecting systems against them. Since our work had the potential of making an impact on real world implementations, we chose to do the responsible thing and contacted the CPNI', explains Martin Albrecht.
"They were very helpful in contacting SSH vendors and by now virtually every vendor out there has both acknowledged and addressed the vulnerability in a new release of its product. We couldn't have covered so many corporate vendors without the help of the CPNI".

At the end of February 2009, the Open SSH team released a new version of their software – version 5.2 – containing several countermeasures to protect against the attacks, fixing the problems identified by the ISG team. Kenny concludes, "The flaws that we found in SSH illustrate in a clear way the limitations that current theory has with respect to practice in the whole area of cryptographic protocol design. We need to develop better theory to help us study these kinds of attacks, and we need to develop better lines of communication to make sure that the theory gets translated into practice".

Read the technical paper here:
http://www.isg.rhul.ac.uk/~kp/SandPfinal.pdf

TO CONSENT OR NOT CONSENT, THAT IS MY QUESTION...

By Christian Bonnici

Visualisation and Other Methods of Expression (VOME) is a three-year project sponsored by EPSRC, ESRC and TSB. Its aim is to develop methods of engagement that help users and service providers negotiate privacy and consent. VOME is a socially-rooted research project, which means that the social theory developed in the project drives the technological design. My PhD studies focus on understanding the ways in which consent is currently negotiated and developing approaches to managing consent. This is what is known as socio-technical research, since it crosses the discipline boundary between science and social science.

At the start of my studies it was a little overwhelming to be given such a huge space to work in. Defining and refining the problem space for research is a key skill for a socio-technical researcher. Socio-technical studies are inevitably complex. One of the main problems is that the social research theories that need to be worked with do not easily map onto technological designs. For this reason, socio-technical design is typically a combination of technology, human processes and practices.

I have had to read extremely widely, learning how to relate literature relating to consent in other areas to information systems. I have also started fieldwork with Sunderland City Council, a VOME partner, who delivers on-line services to communities in Sunderland. Ironically, the very services that I study have also proved a useful source of research material. Together with a colleague from Cranfield, I have started a Facebook community to discuss privacy and consent issues.

So here's my problem space:
Terms and conditions: would you like to read this 20-page document, or would you like to skip it? Either way, you have two options: consent to the terms and conditions, or else refuse. The options sound simple, but can, in fact, be quite complex. Consider the following two scenarios that might be presented to you when signing up to an on-line service (although almost certainly not worded in the same way):

• If you do consent, you will be required to provide us with the following information: your name, surname, home address, email address, and telephone number. You will also be offered the opportunity to provide us with the following information: political views, sexual preferences, date of birth, and anything else you might wish to share with us, your friends, and potentially, everyone else. Changes to the current terms and conditions may occur. If this happens we will change this document. It is up to you to visit this page from time to time.

• If you refuse to consent, then you will not be able to use the service. Although, you might still be reminded to consent from time to time. True, you did not disclose your email address, but we have coded a component to enable your friends to easily load their email address books to the service. This component should automatically trigger the service to send invitations to your mailbox. No, you may not opt out from this one.

This is a confusing scenario for even the most skilled of on-line service users. Both the focus group work and the survey conducted by VOME show that people react to this complexity by simply opting out of any meaningful consent dialogue. In a study conducted by Culnan and Milne, it was reported that 39% of the respondents agreed and 14% strongly agreed to the idea that web privacy notices often use legal language that is hard to understand or is confusing. Further, 47% agreed and 21% strongly agreed with the suggestion that web privacy notices are often too long to be useful.

It's easy to think of design features that should be included in on-line services, for example:

• "Should users be reminded to join services that they would have already refused to consent to? If no, should this occur without the services storing the consumers' email addresses in opt out lists?"

• "Should the consumers be adequately notified about privacy notice changes?"

• "Could changes to business processes lead to the same products and services without the need for private information collection?"

• "Could infrastructural developments enable the development of consent-friendly business processes and information systems?"

However, consent is multi-faceted and depends on the sense in which consent is meant. This makes any such design questions amazingly difficult to respond to. Some service providers might advocate that the development of consent-friendly services is overly difficult, costly or ineffective. They might argue, for instance, that the collection of private information, such as email addresses, leads to customer retention. Nonetheless, it might also be argued that the development of consent-friendly services could build trust, and that this also could lead to consumer retention. The development of consent-friendly intellectual property is also one means towards other benefits, such as commercial competitive advantage.

The tensions for service providers are compounded when the user perspective is factored in to the design. Coming to the end of my first year, my problem space has come into focus and I am edging towards the development of a mechanism for negotiating consent policies where the mechanism balances consent principles, rules and rights within the requirements of a given context. It feels great to have sculpted my own research space out of such a wild, complex intellectual terrain. I feel that I have come to the end of my first year having developed skills that will endure for the rest of my research career.

CHANGING THE WAY WE DISCOVER THE PUBLIC'S ATTITUDES TOWARDS PRIVACY AND CONSENT

By Lizzie Coles-Kemp and Claire Hudson

A year ago the ISG started work on a research project that set out to investigate privacy and consent dialogues and develop new ways to agree and communicate levels of privacy and consent in on-line services. The project is entitled Visualisation and Other Methods of Expression (VOME) and we partner with social scientists at Salford and Cranfield Universities, Sunderland City Council and Consult Hyperion to provide the service user and service provider input. Conn Crawford at Sunderland City Council put forward the following scenario when we were preparing the project proposal:

"Consider the case of a young person, aged 13 years, who is 'at risk' of offending. They are one of the target groups for the Empowering Young People programme which will shortly commence. Some of their peers have heard about the scheme and are saying it will be used by the police to keep track of them. Our young person is shy, reserved and has some learning difficulties. How will they express their concerns about how their data will be used, or will they simply choose not to engage? How might this be further complicated if the young person were to be a member of a minority ethnic group? Would a set of tools available to targeted youth work support workers help clarify the issue, and engage the young person? How might the youngster explain how the scheme safeguards information rights to their peers?"

The original hypothesis was that ***many users cannot and do not engage sufficiently with issues of privacy and consent in their interactions with ICT. Consequently they are not able to adequately assess the risks they run and organisations cannot develop services which adequately address users' privacy and consent needs.***
After a year of focus groups and surveys, a more complex picture has emerged causing us to re-think our hypothesis and recognise a need for negotiated privacy and consent when using on-line services.

Researching the use of on-line services has not proved easy, particularly when the focus of the research is those communities that typically do not benefit from deployment of ICT. The traditional methods of research in this area are focus groups and surveys. Focus groups and surveys have proved challenging for VOME due to the fluid nature of on-line communities, the enmeshed and elastic nature of both the privacy and consent concepts, and the fact that these are topics as a society we just don't talk about. These challenges have caused us to re-think and diversify our research approaches.

VOME was successful in deploying a survey using traditional methods of measurement for privacy and consent attitudes, beliefs and behaviours when it used ***UK online*** as its survey partner. We implemented an online survey through UK online and its ***Myopinion*** online research panel and received 1048 valid responses out of a total of 7,452 invitations to participate. 1,048 is a respectable response and, as is typical for consumer surveys, the response rate was helped by the incentive of a prize draw for an iPod or High Street voucher.

We then implemented the same survey in smaller numbers through a network of volunteers in order to obtain a comparative sample. Here the incentives were a lot smaller and the surveys were implemented in person, not on-line. One of our volunteers was Claire Hudson, VOME project co-ordinator, and she discovered firsthand the difficulties in getting people to think about a subject that for many of us is intuitive and, in fact, private:

"I volunteered to gather survey data in the local area. How difficult could it be I thought..... It's a subject I believe to be of particular relevance in today's online society, so thought the general public would be enthusiastic about sharing their views on this subject with me.

My first choice of setting was a local children's park, but quickly became aware that this venue was particularly time consuming due to the many frequent interruptions from the children while the parents were attempting to complete the surveys. I tried leaving surveys at my local library and Internet cafe, but users tended to ignore them. As an alternative approach I collected free text comments from people based on prompts, including a Word Cloud (wordle) that reflected some of the ways participants had talked about privacy. In order to try this out, I went along to a busy shopping centre, and sat at a popular eating area, again with the belief that people may be more willing to participate if they are not heading somewhere. Bingo!! Success at last! Once I explained the nature of the research and advised that I will only require their input for 1 minute, the majority of people agreed to take part."

The VOME researchers were fascinated by the experiences of our volunteer task force. Much of what we know about the impact of ICT on privacy and consent attitudes, beliefs and behaviours comes from the use of surveys over the last 20 years, where the surveys are often delivered using the methods we deployed through UK online. However, if we want to obtain a broader view from the community, it is clear from the experiences of our volunteers that we perhaps need to change the way we survey and quantify the public's views. As a result, using her experiences in the field, Claire has helped VOME's social scientists to design an approach for taking VOME on the road and running a series of small citizen panels around the country where we put together service providers and service users and use a combination of interactive engagements, as well as short surveys, to elicit the public's attitudes and beliefs towards privacy and consent in on-line services. As part of this activity, in March VOME will be taking part in ESRC's Festival of Social Science, where we are teaming up with the physical theatre company, Bimbilibausa, in order to develop an interactive story in which the audience votes on the privacy and consent strategies of the main characters.

If you would like to take part, either as a service user or service provider, in our public engagement activities, please contact Claire Hudson: claire.hudson@rhul.ac.uk

More details on VOME can be found at www.vome.org.uk VOME is funded by ESRC, EPSRC and Technology Strategy Board.

INSTANT KNOWLEDGE
By Po-Wah Yau

The ISG is involved in the 'Instant Knowledge' (IK) research programme, which is supported by Mobile Virtual Centre of Excellence and the TSB. This is a three-year research programme, the main output of which is a secure autonomous business collaboration service.

The proliferation of smart portable network devices within enterprises is creating a wealth of personal contact information, which is essentially a collection of work-based 'social networks'. The IK service attempts to leverage these personal contact networks to recommend potentially useful work colleagues that an IK user may not have had direct contact with.

It is essential that the effort required to create and maintain an IK user profile is minimal. An IK user's profile is a description based on the IK user's current device context. The context is established through monitoring user interaction with an IK enabled device, both gathering information as it is entered by the user and extracting it from any documents placed in the device storage. The context can include location information, the applications that are being used and keywords of interest.

Device monitoring is also used to autonomously build the user's personal network through implicit means. This includes recording communication with other IK users via their IK enabled devices, as a result of either natural workflow or using contacts recommended by the IK service. Distributed machine learning algorithms process IK user profiles and personal networks to make real-time recommendations as a user works on their IK enabled device.

The ISG is responsible for IK security and privacy. IK security relates to providing conventional security services such as confidentiality, integrity and availability to IK communications. The security work has centred on using the device Subscriber Identity Module (SIM) as a basis for providing the aforementioned security services. The privacy aspect of this project aims to protect user privacy, while at the same time allowing personal information to be shared with different groups.

The SIM based IK security is a precursor to providing privacy whilst using the IK service. IK privacy will be the focus of our work for the next two years. There are many aspects of privacy, including anonymity, which is the protection of a user's identity, and controlling the sharing of other personal data. The IK service will also have to be aware of, and implement, privacy policies specified at many levels. A privacy architecture is being developed to accommodate all possible privacy requirements, and will utilise technologies such as OASIS's Security Aware Markup Language (SAML) and Trusted Computing. It is essential that the privacy architecture has no adverse impact on either the quality of recommendations made by the IK service, or an IK device's usability. For more details of this, and other programmes of research within Mobile VCE, please visit www.mobilevce.com

STAFF PROFILE:
Carlos Cid

01. What professional work were you doing before you joined the ISG?
My academic background is in pure mathematics. After finishing my PhD in Brazil, I came to Europe in 2000 for a postdoctoral fellowship in computational algebra in Germany. A combination of the scarcity of academic positions in Europe and the variety of interesting positions in the IT area in the early noughties motivated my move to industry soon after that. That was when I first got seriously involved with the Information Security field, working as a software engineer in an Irish network security start-up. But it was the beginning of the end of the dot-com boom, so by mid-2003 I was looking for other opportunities in the InfoSec area. I wanted somewhere I could apply the skills that I had acquired, both in industry and academia. I was fortunate enough to be offered a position at the ISG, and have been working here since October 2003.

02. Do you think your time spent in industry has influenced your academic career?
Certainly! Besides being my entry into the Information Security field, it has shaped my career in several ways: I am now involved in more applied aspects of mathematics, it has provided me with skills which would have been hard to get only in the academic world, and it has given me an insight into how the subjects we teach in academia are used in the real world. I hope this experience helps my teaching to be more relevant to many of our students.

03. You still maintain close links with industrial organisations through consultancy work. Can you tell us a little bit about some of these relationships?
I believe one of the most attractive features of the ISG is its strong links with industry. Kudos to Fred Piper for working very hard over the years to establish and strengthen these relationships! These links give, in my opinion, invaluable opportunities to students and staff to interact with security professionals and to understand the real-world problems and constraints with which they have to work. In the past few years I have been involved in a few consultancy jobs, mostly related to cryptographic algorithm/protocol evaluation and design for the Telecom and Financial industries. This has given me a great insight into some of those industries' security challenges, common mistakes, as well as some ingenious ideas. It has also provided me with the opportunity to apply my more theoretical background to solving real-world problems. I invariably learn a lot during these jobs and, as I said, I hope some of this experience can be passed to our students through my teaching.

04. What are your main research interests?
I am mostly involved in research in symmetric cryptography, e.g. design and analysis of stream ciphers and block ciphers, as well as applications of computational algebra to cryptography. But I find Information Security a fascinating field, and my wider interests cover a spectrum of topics in the area, including socio-economic aspects of security.

05. The economics of security is a relatively new research field. What do you think the main research challenges are?
I find this a very exciting new area of research, investigating the boundary between information security and economic sciences. There are several aspects of interest, e.g. the role of incentives in the design and deployment of security mechanisms, externalities, and user behaviour. I am personally interested in applications of game theory to security. Economics of Information Security is an area of research that will certainly grow in the next few years, probably incorporating more techniques from behavioural economics.

06. Do you think we will still be using AES in 20 years time?
I believe so. Despite a few recent cryptanalytic results (mostly of theoretical interest, I must say), I personally believe the AES is a strong algorithm, with a robust and very elegant design. I believe the algorithm's simple design actually makes its security analysis more approachable. It has attracted a lot of attention in the 10 years since being published as a NIST standard, and this will undoubtedly continue, probably increasing confidence in the algorithm. Besides, it is increasingly being deployed by the industry, so even if some weakness is discovered in the next few years, it is very likely we will be using products whose security is based on the AES for a long time to come.

07. What advice would you give to someone contemplating a research career?
Particularly in Information Security, research is a great career path; very dynamic and with plenty of opportunities. You will be continuously reading and studying, and will often be frustrated that some great ideas do not work out (it happens often with me). Information Security is interdisciplinary by nature, so I think it is a good idea to have a variety of skills, ranging from technical hands-on to theoretical, as well as soft skills. I personally believe this is likely to be the profile of researchers (and professionals) working in this field in the near future.

08. Tell us about your interest in historical cipher machines.
Several years ago we undertook a small, informal project, in which we studied historical cipher machines, such as the Enigma. These machines were loaned to us by a private collector. I find it fascinating how designers were able to implement reasonably strong algorithms (though not unbreakable, as they often believed), within the physical constraints of those often small, compact electromechanical machines. The ISG has actually just acquired its first machine. We have received a kind donation of a Hagelin M-209, a machine used by the Americans during WWII.

09. What do you miss most about Brazil, and what do you appreciate most about.. umm.. Egham?
I miss the usual things: family and friends, the weather, exciting football… but I must say that, at the moment, I am happy living in the UK and working at the ISG. I very much enjoy the multinational work environment we have at the college, and the wide range of opportunities that can emerge by living and working so close to London, which is certainly one of the most exciting, vibrant and tolerant cities in the world.

The ISG was donated a Hagelin M-209 cipher machine from a private collector in the United States. The M-209 was designed by Swedish cryptographer Boris Hagelin and was used by the US military during the Second World War. The M-209 was one of the first cipher machines sufficiently portable to be easily taken into the field.

A CONSULTATION ON OFFLINE ENCIPHERED PIN

By Geraint Price

In early 2009 the UK Cards Association asked the ISG to conduct a piece of research on offline enciphered PIN for Chip and PIN transactions.

The current implementation of the EMVCo specification uses Static Data Authentication (SDA). In SDA, the card contains a record of the card's information signed by the issuing bank. However, Dynamic Data Authentication (DDA) has been mandated for use in future Chip and PIN transaction authentication. In the move to DDA, each card will now have its own signing key to authenticate each transaction directly. Rolling out cards with full public key capabilities also makes it significantly easier to add PIN encipherment to the PIN authentication process for offline transactions. The UK Cards Association wanted to know whether this should be promoted as part of the DDA rollout.

The UK Cards Association wanted an independent organisation to be involved so that the current "industry position" could be presented to their members, based on assessing and consolidating the views of the individual stakeholders. The first phase was to issue a questionnaire to an agreed list of stakeholders, including card schemes, issuing banks, acquiring banks, card manufacturers and personalisation bureaux, terminal manufacturers, independent security experts in the relevant fields, and Government. After the responses had been collated, we followed up with interviews to discuss any specific issues raised by the respondents during the questionnaire phase. Once this phase was complete, we analysed all responses to provide an aggregated and anonymised view.

When discussing the scope of the consultation with the UK Cards Association, it was clear that they wanted to include a wide variety of concerns. In drawing up the questionnaire, we separated the discussion into the following areas: security and fraud; operational impacts; business costs; media and consumer perception; industry reputational impacts; legal and regulatory impacts. In conducting this research, it was not our own opinions on these matters that were sought, but rather our ability to act as independent reviewers (and information gatherers) on the consensus opinion in a trusted manner. Our expertise allowed us to ask the pertinent questions and engage in effective dialogue during the interview phase.

Although our own opinions did not influence the final recommendation, which are confidential, I found the ability to sit back and survey the landscape through this role to be an extremely interesting experience. As an academic, it is quite a natural initial reaction to throw extra security at any existing problem or perceived serious threat to a system.

However, the key to the discussion was – how much of a benefit does the additional security provide, and what types of threats can you actually mitigate with the implementation of enciphered PIN? To thoroughly understand the impact of any new security mechanism we add, we need to take into account how an attacker would attempt to bypass these additional mechanisms (in this case enciphering the PIN). Technical solutions can only provide a worthy addition if we also take a holistic approach to the security which you are trying to implement, otherwise we are no more useful than King Canute.

Ultimately, I firmly believe that we, as security architects and engineers, should never forget the breadth of key areas which impact on the final technical decision.

THE ISG SMART CARD CENTRE YEARLY REVIEW

Perhaps the most public activity of the Smart Card Centre (SCC) in 2009 was the return of the SCC Open-Day on September 15th after a one year absence (the SCC hosted CARDIS in 2008). Fortunately our sponsors and supporters came back with undiminished enthusiasm for the event and exhibitors included Giesecke & Devrient (G&D), Vodafone, Transport for London, ITSO, O2, Comprion, Barnes International, Cubic, Thales, RFI Global, Burall Infosmart, Multos International and Oberthur. As always the industry participants were matched by exhibits from SCC masters and PhD students. Of course an exhibition needs visitors and luckily there was no shortage, in fact attendance in 2009 exceeded all previous years and lasted throughout the day to the guest lecture by Professor Michael Walker. Visitors voted for their favourite industry and student exhibits and once again G&D was awarded the Crisp Telecom award in the industry class with Lishoy Francis (NFC phone to attack payment transaction) winning the student class. There were also three special awards from Vodafone and G&D for the SCC's best MSc projects in 2008. In descending order they went to Walid Fakim (Side-Channel Attacks), Lazaros Kyrillidis (Server on SIM) and Graham Hili (Security in Virtual Worlds).

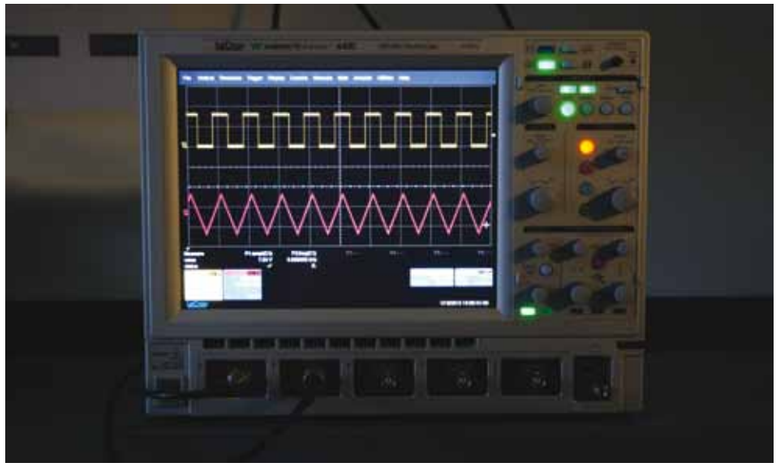
Of course the Open-day is just a showcase and a lot of hard work goes on throughout the year, especially with respect to projects and research activities. In 2009 the SCC had around 15 MSc projects, although in 2010 we will be supervising nearly 30! Clearly smart cards and RFIDs are still hot topics and student interest may also be stimulated by some new capabilities and opportunities in the SCC. We have re-furbished one of the SCC rooms to become the SCC RFID lab, which was helped in no small way by a College grant of £25k to purchase good quality equipment. We now also have a scheme whereby if Information Security MSc students take the SCC taught module and complete a SCC project, they are deemed to have "mastered" in Smart Cards and RFIDs.

PhD/staff research activity has generated around 10 published papers in 2009 (www.scc.rhul.ac.uk/publications.php), covering diverse topics including protocols, attacks, transport systems, proximity/location techniques and application security management. We were also pleased to welcome back two of our past MSc students (Graham Hili and Wael Malek) to carry on their research to PhD level. Perhaps the most interesting and practical piece of research work (L. Francis et al) was on exposing the potential for misuse of mobile phones as clone platforms to attack payment systems. It was also good to see continuation of co-operation and publication with past visiting researchers to the SCC, including Michael Tunstall (Bristol), Damian Sauveron (Limoges) and Yuanhung Lien (NTUST/Taiwan).

The SCC has also been trying to extend international co-operation (and funding) by participation in three EU funding bids. We led one project bid involving the Fraunhofer Institute, we participated in a bid led by the Czech Technical University and involving IBM, and we also participated in a French led consortium bid involving Professor David Naccache. In 2009 the SCC and the Royal Holloway Enterprise unit were successful in a PARK funding bid, aiming to turn some existing SCC RFID related IP into a prototype product during 2010.

During 2009 the SCC/ISG has continued to provide expert support to the Dutch Transport Ministry with respect to the OV-Chipkaart used in transportation systems in the Netherlands. A major element to the work has been the migration planning review which is due to complete in early 2010 and will have a major impact on Dutch transportation for years to come. What does 2010 hold in store? Well we know we have a lecture module to run, exams to write, 30 MSc project students to supervise, the next Open-day (7th Sep 2010) to plan as well as the PARK development and various research projects and funding bids, so the only safe prediction is that we will not be bored!

Keith Mayes is the Director ISG Smart Card Centre



WHEN GERAINT MET IAIN

Dr Iain Crinson is a Lecturer in Sociology of Health and Illness at St George's, University of London, who is currently visiting the ISG. Dr Geraint Price of the ISG discusses with him some of the challenges of interdisciplinary research dialogue:

GP: Speaking as a dyed-in-the-wool computer scientist, I guess the first thing I'd like to ask is: how would you define a socio-technical research perspective?

IC: It's a cross-disciplinary approach to understanding this field of study. It seeks to move beyond the assumption that 'technology' and 'human factors' within organisations somehow occupy separate domains. This perspective is based on the recognition that whilst formally or analytically distinct, the relationship between technology and 'human factors' is a dynamic one, shaped through interactions that are emergent over time.

GP: How does using a socio-technical viewpoint allow you to understand the environments which you're analysing?

IC: The approach demands that the first step in the assessment of any information system is that it is studied in the field, within the organisational context. This approach is determined by a key assumption of social –technical studies that information systems are constituted by a set of practices involving social actors interacting with the technical architecture of the system.

GP: When I think about an information processing system, the first thing I generally consider is how the different parts which store, process and transmit the data fit together. How does this differ from the way you first view such a system?

IC: Again, a different set of assumptions would be at work. Rather than seeing the information processing system as a discrete or bounded set of technical mechanisms, a socio-technical perspective assumes that human factors necessarily engage in an interactive relationship with that system. So by definition, technical mechanisms will always be subject to change, and will never function purely as designed.

GP: Probably the second thing I would consider is how each of those processing elements in a system might interact, which should then influence the design of the security services I might want to put in place. What would be the analogous process in your field be?

IC: Well, interaction is certainly the key to understanding how the processing elements within the system operate, but interaction goes beyond the formal architecture of the system. Social actors necessarily interact with the system, and not purely as 'operatives' or as an extension of the technical processes themselves. Attempting to predict how these social and technical elements might interact when designing a security system is fraught with many difficulties, not least because of the differences in organisational context within which nominally similar information systems might operate. However, a detailed social scientific assessment of an organisation's cultural and behavioural norms combined with an understanding of its overarching operational activities, may allow designers to build-in a set of realistic parameters to interaction, if not predictors as such, because of the dynamic nature of the operating context.

GP: Given that you've now had a chance to see how a scientist might view a security management system, what are the initial differences you see in how we observe and understand a system?

IC: The differences flow from philosophy. Where your drive is to seek to abstract out or isolate key variables or technical mechanisms in an understanding of how information systems function, I focus on the contextual (human/social and technical) conditions or factors that are necessary to trigger the operation of these mechanisms. Both approaches necessitate moving from theory to hypothesis testing in order to inform generalisations. What is distinctive about my approach is that hypotheses concerning the operation of an information system would be framed in terms of a series of propositions concerning how key socio-technical mechanisms in the specified context influence the production of observed outcomes.

GP: From a personal perspective, I've slowly come to realise that no matter how systems are designed from a technical perspective, they are rarely used as initially intended. I appreciate that for you this might seem like an obvious statement! However, what are the most obvious differences between a technical and sociological viewpoint which I should aim to understand?

IC: I'll try and address this question in a different way. While there are important differences between an engineering or computing science perspective and the sociological view, this is primarily a function of the very different objects of knowledge or concern. On the other hand, the very reason socio-technical studies emerged over thirty years ago was a realisation that an understanding of the application of the technological products of human ingenuity and innovation cannot be separated from the practices of utilising that technology. In this sense, socio-technical studies seek to enhance both traditional sociological and information security understanding of the operation of information systems within organisations, by applying a research methodology which assumes an interdependence or, if you like, an entanglement of both technical and social /organisational worlds.

GP: I guess a long term goal for me would be to design systems that are more in tune with a business process and more intuitive for a non-specialist user. Is there any existing research looking at these types of goals from a socio-technical perspective?

IC: Very much so, in fact this was the initial impulse for the development of socio-technical studies in the 1970s. Socio-technical studies are nearly always funded precisely with these business / innovation goals in mind. Thank you for giving me this opportunity to expound some of the principles underpinning the socio-technical approach that I am seeking to develop with Lizzie Coles-Kemp of the ISG in relation to the introduction of Electronic Health Records in the health care system. I have 12 months still to run on my EPSRC funded 'discipline hop' here at RHUL, and it is proving to be both enjoyable and stimulating. Everyone I have had contact with here at RHUL has been very tolerant of my limited understanding of Information Security!

ENGAGING WITH I-4
By Geraint Price

What is I-4? The moniker stands for the International Information Integrity Institute. In essence it is a membership organisation, to which companies pay a fee to join each year. In return, they have access to all the activities that the I-4 organisation offers. 1-4's aim is to allow their members to discuss any issues related to information security (in the broadest sense).

The key ways in which I-4 fosters interaction between their members are:

• **Forums:** essentially workshops with programmes tailored to discuss the issues set out by the I-4 organising committee. There are three per year (East coast US; West coast US; Europe), and are usually 2-3 days in length.

• **Regional Meetings:** one day meetings aimed at allowing active member discussions on a few select topics which are at the forefront of the issues being dealt with by the members.

• **Online Interaction:** a variety of different means of providing short discussions, or member-led queries around individual selected topics. The current interactions include members' queries, where a member who wishes to find out more information on how other organisations have dealt with a particular issue can submit a query to other members, and teleconferences.

I-4 as an entity has been 'owned' by a number of different organisations over the past couple of years, and has just entered a new phase. Over the summer KPMG, under the direction of Malcolm Marshall have bought I-4. Their goal in taking it over is to elevate I-4 to be the premier organisation for discussing corporate security concerns for higher echelon security professionals in large organisations.

What is the ISG's involvement with I-4? As well as regular membership, there are a few associate members. The ISG, along with Carnegie Mellon University in the USA, are associate academic members. As associate members, we are encouraged to actively participate and provide our input as academics in the field of information security.

The main ways in which this happens are attendance and contribution to forums and regional meetings. We attend the regional meetings that are held in London, either as a participant or as a presenter on a topic. For example, a few years ago I gave a presentation on the work being carried out by the AIM (Authentication and Identity Management) Club at that time. We also attend some of the European forums, and again have contributed to the programme (Carlos Cid recently presented on issues related to the future of cryptography). As well as participation of the ISG with I-4, there has also been active participation in return. They became a member of the AIM Club, giving their membership vision of the work we were carrying out through the Club.

I found it incredibly useful to have a window on the emerging issues as seen by those in charge of information security in their respective organisations. For example, the most recent regional meeting I attended discussed cloud security, the effect of 'consumerisation' on an organisation's security policy, and breach disclosure notification. Hearing the thoughts and experiences of I-4's members can be an enlightening process. As well as being a learning experience, our ability to present our own expertise to an interested and motivated audience can serve as a useful and too often untapped resource for us as academics, who should never lose sight of the real world aspects of the solutions we aim to provide.

PRESTIGIOUS RESEARCH FELLOWSHIP FOR KENNY PATERSON

In March 2010, Kenny Paterson begins a five- year research fellowship funded by the EPSRC, the UK's national science funding body. Worth £1.2M, the fellowship will relieve Kenny of teaching and administration duties and allow him to build a team of postdocs and PhD students to carry out research under the banner of "Cryptography: Bridging Theory and Practice". When asked about how he plans to spend his time, Kenny commented:

"The principal aim of this research is to make a systematic attempt to bridge the divide between theory and practice in cryptography, with the ultimate objectives being to create theory that is more useful and systems that are more secure. An important aspect of the work is the involvement of industry, with significant support for the project coming from BT Laboratories, the Centre for Protection of National Infrastructure (CPNI), HP Laboratories, the International Information Integrity Institute (I-4), and Mastercard. Their participation will help to keep the research firmly in touch with the real-world issues."

While Kenny will no longer be teaching on the ISG's MSc programme on a regular basis, he will be popping up from time to time in support of ISG colleagues. As Kenny says "I would really miss lecturing on the MSc, so I hope to do a bit of that if asked. I also hope that I'll be able to come up with some good MSc project topics too. But I won't miss the exam marking one bit!"

AU REVOIR TO PROFESSOR STEVEN GALBRAITH

Professor Steven Galbraith, an internationally-recognised expert in the field of Elliptic Curve Cryptography, left the ISG in 2009 to take up a position at the University of Auckland. Steven was a postdoc in the ISG from 1996-1997, and then re-joined the team as a Lecturer in 2001, quickly rising to Reader and then Professor. A native of New Zealand, Steven made no secret of his long-term plans to return to his home country. Yet his leaving was tinged with sadness for all of us - as well as being an exceptional scientist, Steven has been a great colleague and provided an important link between the ISG and the wider mathematical community at Royal Holloway.

When asked about his experiences since returning home, Steven commented in typically irreverent fashion: "One thing I really miss is being able to discuss recent results in information security with colleagues from a wide range of subject backgrounds. Having such a diverse range of points of view in a single place is very valuable. In Auckland I am so desperate I have to read Bruce Schneier's blog!"

The good news for the ISG is that Steven is already planning to visit us in the Summer of 2010 for a couple of weeks. We are looking forward to hosting him and renewing our research collaborations.

WELCOME TO COLIN

The ISG is delighted to welcome Dr Colin Walter, who has taken up the position of Director of the distance learning version of the MSc Information Security. Colin comes to us from Comodo, a certificate authority with research laboratories in Bradford, where he was head of cryptography.

Colin adds to the Scottish flavour of the ISG (he's the fourth Scot on the current staff). He holds a degree in mathematics from Edinburgh University and a PhD in number theory from Trinity College, Cambridge, where he shared an office for part of the time with Andrew Wiles, later famous for proving Fermat's Last Theorem. Colin subsequently spent eight years in the Mathematics Department of University College, Dublin.

From 1984 to 2001, Colin was a member of the Computation Department at UMIST, which subsequently merged with University of Manchester. His mathematical background proved invaluable in a consultancy between several members of that department and Plessey-Crypto to design an RSA chip in the late '80s for electronic funds transfer at point of sale. The chip worked first time but unfortunately turned out to be an economic flop, having been marketed at the same time that cheaper unauthenticated and unencrypted Switch transactions started. We know price is more important than security!

The '90s saw a number of publications in cryptography, many related to the efficient hardware implementation of modular arithmetic. For example he was the first to apply Montgomery's modular multiplication algorithm to design a systolic array for modular exponentiation which had only local connections. This design has been used in all RSA hardware accelerator chips since then.

Colin was one of very few researchers with the right background to help solve the side channel problems which surfaced in the mid '90s. These were hardware issues which required software countermeasures in addition to the obvious hardware ones. He became a consultant for the NatWest bank while it was developing the Mondex purse and co-authored a paper explaining the leakage as being the result of the different frequencies of subtractions between squaring and non-squaring operations. This led, at the beginning of this century, to a much used side channel resistant version of Montgomery's algorithm in which there are no conditional subtractions as well as some novel, yet straight-forward and efficient, exponentiation algorithms with side channel resistance.

In 2003 he was in Canada attending the SAC conference (Selected Areas of Cryptography) when, during a talk on power attacks, all the lights went out across the whole east coast of North America! His talk there showed the counter-intuitive fact that longer keys are less secure than shorter ones when there are timing, power or electro-magnetic side channels available to the adversary.

Recent work for industry has included building parts of an identity-based encryption scheme and he continues to pursue research on side channels when not involved with running the distance learning MSc or puffing up some Scottish Munro.

CONTACT INFORMATION:

For general information about the Information Security Group and the MSc and diploma programmes offered by the ISG, please contact:

Information Security Group Secretary
Royal Holloway, University of London
Egham, Surrey, UK TW20 0EX

T: +44 (0)1784 443093
F: +44 (0)1784 430766
E: isg-secretary@rhul.ac.uk
W: www.isg.rhul.ac.uk

For an overview of the application process, please visit:
www.rhul.ac.uk/graduate-school

For more specific queries about the Information Security Group and postgraduate admissions, please contact:

Pauline Stoner
Information Security Group Administrator
T: +44 (0)1784 443101
E: p.stoner@rhul.ac.uk