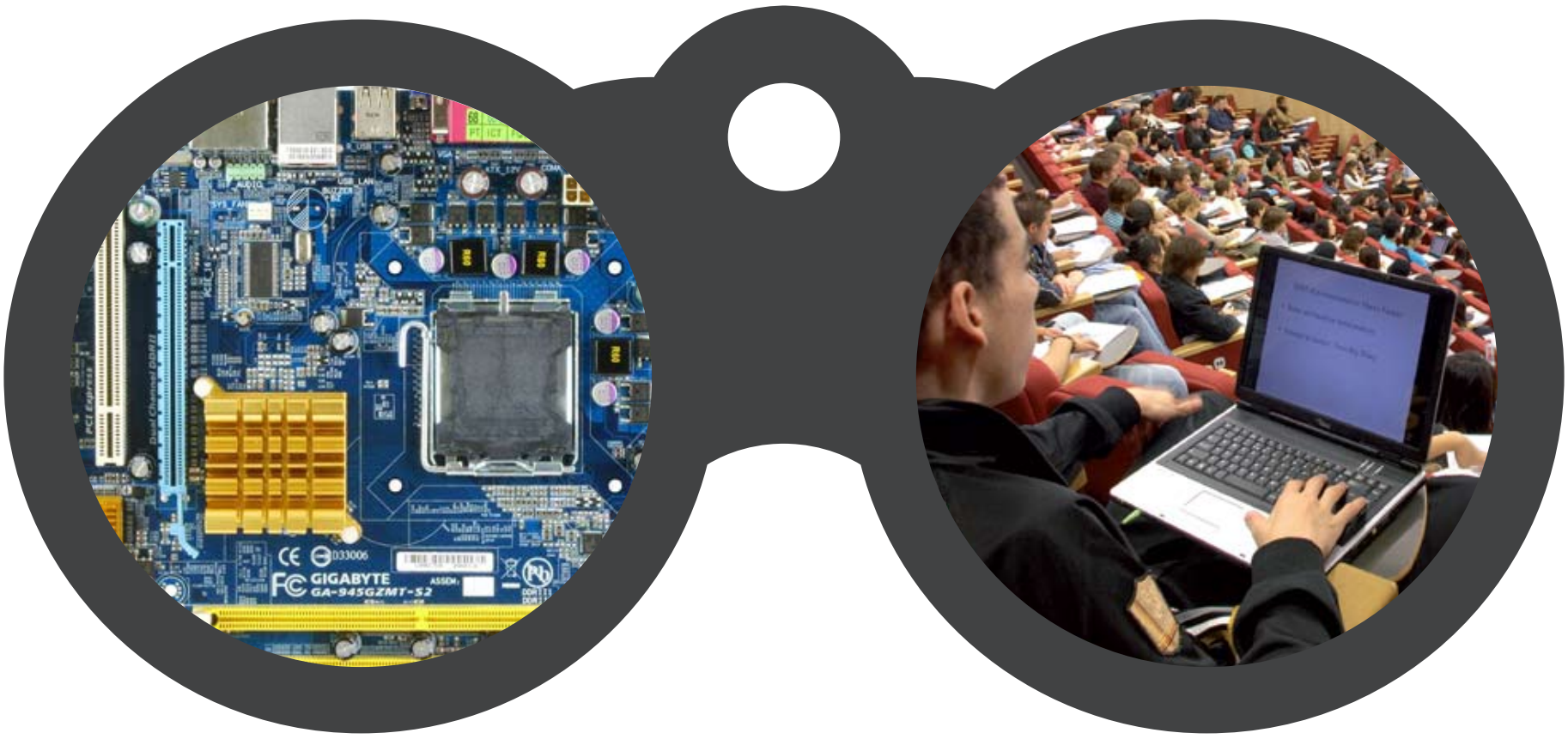
Information Security Group

Review 08/09



Royal Holloway
University of London

CONTENTS

03
Letter from the ISG Director
ISG and its Alumni in Partnership

04
An Eventful Year for the Smart Card Centre
Short News

05
Profile: Jason Crampton

06
Taking Information Security to Schools
The Case for Authenticated Encryption

07
De-perimeterisation
Working With Industry

08/09
Where Are They Now?

10
A Maltese Partnership
Instant Knowledge

11
Malaysian Connections

12
State of the Art Research in Trusted Computing
The Cyberspace Frontier Has Closed!
Conference Report: Pairing 2008

13
Book Review: Virtual Shadows
Socio-technical Studies in the ISG

14
The Nineteenth Hewlett-Packard Colloquium on Information Security
Cryptography Meets Network Security Part 2: SSH

15
Securing Mobile Voice End to End
Studying in Block Mode

16
Honorary Degree Awarded to Prof Whitfield Diffie
Farewell to Scarlet
Contact Information

LETTER FROM THE ISG DIRECTOR

Welcome to the latest annual review newsletter of the Information Security Group at Royal Holloway. In it you will find news of some of our activities over the past year, as well as information relating to our teaching programmes, research and outreach activities.

The most exciting event in the last year was our first alumni conference, which was well attended. It demonstrated how strong and wide-reaching our international alumni network now is. We have built on the success of this event by formalising the establishment of alumni chapters throughout the world. We hope that these will provide a local focus for information security expertise as well as maintaining strong connections with our alumni. International links are the focus of several of this year's review articles.

We are also aware of the challenges facing new graduates seeking a career in information security. Hence we have asked a number of recent graduates about how they obtained their current positions and how they are faring in their professional careers. This is a fascinating read.

This review also showcases some of the research work being undertaken in the ISG, from socio-technical research programmes on the human aspects of information security through to technical analysis of network security protocols and smartcard technologies.

We hope that you enjoy this latest review. As always, we are very keen to engage with anyone who is interested in our activities. Please do not hesitate to contact myself or any of the members of the ISG should you wish further information.

Prof. Peter Wild

ISG AND ITS ALUMNI IN PARTNERSHIP

BY FRED PIPER, DIRECTOR OF EXTERNAL RELATIONS FOR THE ISG

When we introduced our MSc in 1992 it was the first of its type in the world and had a class of only 10 students (7 full-time and 3 part-time). Things have moved on from then and the profile of Information Security has risen. The number of students taking our MSc has increased dramatically, peaking at about 250 in 2002, and similar programmes have now been introduced at other universities all over the world.

Throughout this expansion the international reputation of the Royal Holloway MSc has remained high. Employers continue to look for experienced candidates with the MSc from Royal Holloway "badge" and the number of our alumni holding influential positions in the Information Security profession has increased.

For many years the ISG has recognised that the quality and achievements of our alumni are one of the best forms of advertisement for the MSc. Reciprocally, the high reputation of the MSc is crucial to the employment prospects of alumni. Ever since it was established, the ISG has always had "Academia and Industry in Harmony" as a central theme. A second theme of "ISG and its Alumni in Partnership" has now emerged.

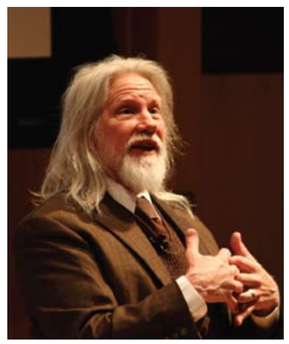
In July 2008 we held the first reunion conference for ISG alumni. The conference lasted two and a half days and received sponsorship from BT, HBOS, HP Labs, KPMG, Thales, VISA, and Vodafone. All 28 session speakers and (about 160) attendees were either alumni or ISG members and there were two keynote sessions from Whit Diffie (Visiting Professor with the ISG) and Robert Carolina (Senior Visiting Fellow with the ISG and regular lecturer on the MSc).

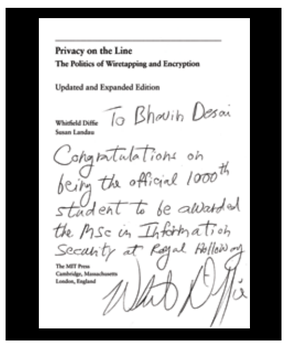
This was a high calibre conference that met the standards of "normal" open academic or commercial meetings. The ISG is very proud of the quality of the talks. It also provided an opportunity for alumni to re-establish lost links, establish new links, and of course to socialise during (and after) the two conference dinners. The overwhelming feeling from our alumni was "can we please have more events like this" so a second conference has already been planned for July 2010.

One of the features of the reunion conference was a presentation by Whit Diffie of a signed copy of his book "Privacy on The Line: The Politics of Wiretapping and Encryption" to Bhavin Desai, who was the 1000th MSc graduate. This landmark was achieved in 2006 and there are now more than 1500 ISG alumni worldwide. This makes our alumni a potentially powerful influence in the world of Information Security. However, these alumni are distributed across more than 50 countries and, historically, there has not been any attempt to unite them into a single community. Furthermore, when we were setting up the alumni reunion conference we discovered that the ISG had lost contact with many of them.

As a result, it was decided to establish alumni chapters throughout the world. Alumni chapters have now been established in 38 countries. (See www.isg.rhul.ac.uk/alumni for more details and a list of contacts). The precise role of a chapter will depend upon the country and the number of members. However, they already form focal points for networking and some are already arranging events for local members. We hope that they will not only provide us with international contacts, but also grow as local communities of expertise for information security professionals around the world.

To see the full alumni reunion conference programme go to the back page.





AN EVENTFUL YEAR FOR THE SMART CARD CENTRE

BY KEITH MAYES
DIRECTOR ISG SMART CARD CENTRE

The year 2008 was a very eventful one for the Smart Card Centre (SCC). At the start of the year our new course book (Smart Cards, Tokens, Security and Applications) hit the on-line stores in time for the MSc module of the same name. However this was not the biggest event in the smart card world around that time.

There were great concerns in the Netherlands concerning the impact of some publicised attacks on the MIFARE Classic smart card used in the Dutch transport system. The Dutch transport ministry, and indeed the government, were so concerned that they decided to seek an independent expert opinion on the problem. They approached several leading centres throughout the world and it was with great pride that the SCC, and a team drawn from across the ISG, was selected to carry out this high profile task. Our report was well received and was instrumental in initiating migration planning activities for the Dutch Transport system. As a result the team has been congratulated for its work and commissioned by the Dutch transport ministry to carry out further formal reviews during 2009.

On a related topic, and in recognition of our long standing links with the transport industry, the SCC was delighted to welcome two new associate members in the form of Transport for London (TfL) and ITSO (the smart card standardisation body). Both TfL and ITSO have committed to a minimum three-year involvement with the SCC.

Another industry-related initiative (although lower profile) was a study commissioned by members of the mobile communication industry to investigate the future of SIMs/USIMs and alternative security solutions for mobile devices, especially for machine-to-machine applications. This work was publicised in an Elsevier Technical Report.

In the summer we hosted visiting researchers from Limoges and NTUST (Taiwan). This followed on from previous visits and collaborations that have resulted in joint research publications and on-going work.

The work of the SCC staff received recognition in 2008 when Kostas Markantonakis was promoted to Reader and Keith Mayes became a Fellow of the Institution of Engineering and Technology. However, there was very little time for self-congratulation as preparations were underway for CARDIS2008 in September 2008. This was the 8th Smart Card Research and Advanced Application IFIP Conference and the SCC was very privileged to have been selected to host this prestigious event. The conference was well attended and there were many impressive papers and presenters, making for an interesting and enjoyable event.

Taking into account student supervision, guest lectures and visits to other academic institutions, 2008 was a highly productive year. Indeed 2009 is likely to be just as busy, as we prepare for further transport related work, the commissioning of our RFID/NFC lab and the re-launch of the SCC Open Day Exhibition on the 15th Sep 2009.

SHORT NEWS:

- **Chris Mitchell has been appointed as an Associate Editor for IEEE Communications Letters as an expert in communications and security. This journal publishes fast turnaround short papers relating to research in communications.**

- **Hilary Ganley has retired from the post of Programme Director for the distance learning MSc Information Security. Hilary was instrumental in the design and smooth running of the programme, thanks to a precious combination of her vast experience of directing postgraduate courses at the University of Glasgow, and her first-hand experience of being an MSc student at Royal Holloway. Hilary will be missed by colleagues and all the students whose studies she has both facilitated and helped in the five years since the programme launched.**

- **Steffen Reidt, in his third and final year as a PhD student with the ISG, completed a three-month summer internship at the IBM T.J. Watson Research Center in Hawthorne, New York within the framework of the International Technology Alliance research program, co-sponsored by the US Department of Defense and the UK Ministry of Defence. This trans-Atlantic research collaboration yielded a number of interesting results, including a publication at the ESORICS 2008 conference.**

- **Stephen Wolthusen was awarded an honorary guest professorship in the Department of Computer Science at Harbin Institute of Technology, one of the top ten research universities in China, in November 2008.**

- **Stephen Wolthusen gave an invited talk on the detection of subversion-type attacks in offshore control systems at the Maritime Infrastructure Protection Symposium (MIPS) hosted by United States Naval Forces Central Command in Manama, Bahrain in February 2008. Senior diplomatic and military personnel, including chiefs of staff and chiefs of naval operations from 27 nations, were in attendance.**

- **Keith Martin has been appointed to the Editorial Board of the IEEE Transactions in Information Theory, as an Associate Editor in the area of complexity and cryptography. IEEE Transactions in Information Theory has published a number of the most influential research articles in cryptography, including Whit Diffie and Martin Hellman's classic New Directions in Cryptography, which first publicly outlined the blueprint for public key cryptography.**

- **Chez Ciechanowicz was invited by the Korean National Police Agency as a guest speaker at their Symposium on Cyber Crime in Seoul in November 2008. The purpose of this annual symposium is to bring together senior investigators from law enforcement agencies, international organizations, academia and private companies dealing with computer- and Internet-related crime. It was a very impressive event, attended by representatives from more than 50 countries (and of course quite a few ISG alumni). Equally impressive were the presentations illustrating the worldwide cooperation that is involved in fighting and investigating cyber-crime. Chez thoroughly enjoyed the hospitality of both the organizers and MSc alumni in Korea.**

- **Alex Dent was invited to speak on the history of public-key cryptography at the inaugural Africacrypt 2008 conference in Casablanca. To mark the occasion, Alex planted a tree in the gardens of the Mathematics Department of the Ecole Normale Supérieure de Casablanca before the gala dinner.**

Question 01

Here's a nice puzzle from Chris Maslanka's Pyrgic Puzzles in The Guardian:
**Find a four-digit number with the following properties:
(i) the first (leftmost) digit is equal to the number of 0s in the number
(ii) the second digit is equal to the number of 1s in the number
(iii) the third digit is equal to the number of 2s in the number
(iv) the fourth (rightmost) digit is equal to the number of 3s in the number. Are there any other numbers with these properties?**

Question 02

This is a very old crossword clue from The Times that I really like:
HIJKLMNO (5)

PROFILE: JASON CRAMPTON

You took a slightly unconventional route into academic research. In what ways do you think that has benefitted your work as a teacher and researcher?
I spent four years teaching mathematics and then seven years working as an administrator in the Finance Department of one of the country's biggest trade unions. I think this experience has had two distinct effects on my attitudes as an academic. First, it is very important to remember what one found difficult about a particular subject and to remember how and why "the penny dropped": using those insights when teaching the subject can be very valuable. Second, when developing a research idea, try to have a compelling practical reason for doing it and, wherever possible, provide a feasible solution.

What are your research interests?
My research focuses on access control, which is concerned with restricting the extent to which authenticated users are allowed to interact with protected resources. Generally speaking, user requests to access protected resources are mediated by a trusted software component, which enforces an access control policy. The policy specifies, explicitly or otherwise, which requests are authorized (and hence should be permitted). It is usually impractical to explicitly enumerate all authorized (or, equivalently, all prohibited) requests. Hence, my research concentrates on finding economical representations of authorized requests. This typically involves grouping either users or protected resources, which, in turn, means that a certain amount of precision is lost. Finding reasonable compromises between the expressivity and economy of an authorization policy is therefore at the heart of much research in access control, including my own.

In addition, there is increasing interest in what might be called "higher order" authorization policies. In this context, we are interested in identifying policy configurations that are undesirable, perhaps because they would undermine or compromise complex enterprise security requirements. The standard example is that of separation of duty, where it may be reasonable for a user to be authorized for either one of two actions, but not to be authorized for both. Finding appropriate formalisms for such authorization policies and, more importantly, finding efficient methods for ensuring that such policies are enforced, are of considerable interest to the research community.

What aspects of your research do you think have the potential to influence information security in practice?
I have a project with Michael Huth at Imperial College, which is concerned with developing a programming language for authorization policies. This work is intended to demonstrate that existing languages and technologies for access control, such as XACML, are likely to be difficult to deploy and maintain and that a new approach is required. One particularly important aspect of our work is that it could lead to distributed enforcement of authorization policies and hence provide support for "authorization-as-a-service".

You've worked a lot on role-based access control. In what application environments do you think we will see more implementation of role-based access control?
Perhaps the most obvious application of role-based access control (RBAC) is in enterprise user provisioning. In large corporate environments in which users may have access to a number of different applications residing on multiple platforms, it is desirable to have a single point of administration for controlling the interaction users have with these applications. RBAC, which associates users with roles (access control abstractions that correspond to particular job functions), and roles with access to certain resources, provides a structured way of associating users with accounts (and hence resources) on different platforms.

How did you come to be working in the general area of information security?
My PhD studies began by continuing the work of Greg O'Shea (now at Microsoft Research) on a logical representation for access control. Over the course of my PhD I began to focus more specifically on RBAC and particularly administration in RBAC. I was honoured to be offered a position in the Information Security Group after my PhD, where I have been able to continue my work on access control.

What do you like about working in academia?
I love the variety and the freedom that academia provides: one day I will be teaching, the next I will be supervising really interesting work by MSc or PhD students, the next working on my own research. One particular benefit of working in the ISG is the strong links it maintains with business and government, which means that a wider variety of opportunities for interesting work arise: for example, I have done some consulting work for PricewaterhouseCoopers, and I helped to develop the Enigma puzzles for the book "Can You Crack The Enigma Code?" by Richard Belfield.

You have been teaching Computer Security on the MSc Information Security – what are the particular challenges involved in teaching that module?
Perhaps the biggest challenge in teaching Computer Security is that modern hardware and software is extremely complex. Moreover, the technology is always developing. Keeping abreast of these developments can be difficult and time-consuming. Distilling the wealth of technological information, as well as the academic literature, into a set of appropriate course materials represents a considerable challenge!

There is a cliché that on the Internet nobody knows that you are a dog. That's particularly relevant to your office, is it not?
Ha ha! Yes, I have a Weimaraner dog called Bo who is often in my office, although he hasn't figured out how to use a web browser yet.

You have developed a reputation in the ISG for being a great solver and setter of quizzes and puzzles. Can you leave us with a few of your favourites?
Sure. Here are two.

(See speech bubbles and back page for the answers!)

TAKING INFORMATION SECURITY TO SCHOOLS

Keith Martin was the guest speaker at the Bexley Excellence Cluster Event in October. About 100 pupils from schools in the Bexley Excellence Cluster, which consists of 16 primary and secondary schools, learnt about cryptography and Dan Brown's *The Da Vinci Code* through a range of activities.

Keith shared his cryptography expertise with the pupils by explaining how simple mathematical techniques can be used to scramble information. To emphasise the prevalence of cryptography, he highlighted that anyone who has used a mobile phone or the internet had used cryptography, albeit unknowingly. He added that cryptography was crucial for sending electronic messages securely, while it also played an invaluable role in maintaining the security of bank accounts and in validating information.

***The Da Vinci Code*, which mentions Royal Holloway as a centre of excellence for cryptography, was also discussed during the talk. However, Keith suggested that serious cryptography was in fact lacking in the book, owing to the ease with which the ciphers mentioned there could be broken.**

Simon Prynne, Co-Chairman of the Bexley Excellence Cluster and Head Teacher of Jubilee Primary School, thanked Keith for his interesting talk, commenting, "We didn't realise how important cryptography is in our every day lives, but Professor Martin has shown us how it is used in our mobile phones and computers."

Keith enjoyed the day but told his Royal Holloway MSc students: "It's much more nerve-racking discussing cryptography with primary school students than with post-graduates. For one thing, they always ask much more difficult questions!"

THE CASE FOR AUTHENTICATED ENCRYPTION
BY ALEX DENT

Suppose a business wants the ability to send confidential documents securely over the Internet to some form of digital archive. In order to do this, we're clearly going to need some form of secure communication channel between the business and the digital archive. But what does it mean to say that a communication channel is secure? It's often not as easy to build a secure channel as it appears at first glance.

We're taught that information security is about assuring CIA: confidentiality, integrity, and availability. In the case of the digital archive, it is reasonable to suppose that the communication channel should satisfy all of these security requirements. We want the documents to be kept confidential during transmission, either to meet regulatory or contractual obligations, or to preserve some business advantage. We want the documents to be integrity protected, so that we can be sure that the documents placed into the archive are the same as those sent by the business. We want the documents to be available in the sense that the delivery mechanism should be as efficient as possible.

There are many ways to achieve these aims. Perhaps the most obvious is to use some form of cryptography. We may, for example, encrypt the documents to provide confidentiality and apply some kind of checksum mechanism, such as a MAC or a digital signature, to ensure that the documents are integrity protected. If these cryptographic operations are relatively efficient then, on the surface, we appear to have achieved our security goals.

But have we really?

The process of combining cryptographic algorithms to achieve multiple security goals is notoriously tricky. It is the cryptographic equivalent of patting your head and rubbing your stomach: while you're concentrating on achieving one security goal, you're probably making mistakes with the other. Consider an encrypted and digitally signed document that is being sent to the archive. What happens if an attacker strips off the original digital signature and appends his own signature to the encrypted document? The digital archive will now think that the document was sent by the attacker, and will place the document in the attacker's archive. Since the attacker can request copies of documents in his own archive, it is easy for the attacker to break the confidentiality of the system, despite our use of encryption.

The problem here isn't that the encryption scheme was insecure or that the digital signature scheme could be broken: the problem was that we assumed that by simply combing two operations we would get the best of both worlds. In the security world, it is more sensible to assume that if you combine two security operations, then you end up with the worst of both worlds!

Instead of attempting to build an ad hoc scheme from encryption and digital signatures, we should have been trying to build a combined scheme that simultaneously provides integrity protection and encryption. These types of schemes are called authenticated encryption schemes. Authenticated encryption schemes not only provide better security guarantees but, by combining two security operations into a single phase, often provide much more efficient schemes. The problem is that they're not very well-known or well-used, despite these advantages.

During the last two years, the ISG has been working with the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) to produce new standards for business to implement authenticated encryption schemes. Chris Mitchell is the editor of the new ISO/IEC 19772 standard, which describes authenticated encryption techniques based on symmetric cryptography. This standard was published at the beginning of the year. I have been working very closely with the editor of the new ISO/IEC 29150 standard, which describes authenticated encryption techniques based on public-key cryptography. The editor of this standard, Prof. Yuliang Zheng of the University of North Carolina, and I are also working on a new book on the theory behind public-key authenticated encryption, which should be released by Springer in late 2009.

We hope that these initiatives will raise the profile of authenticated encryption schemes and facilitate their wider adoption in security applications.

DE-PERIMETERISATION
BY GERAINT PRICE

Over the past couple of years there have been a number of activities which focus on the changing role of the security perimeter. There have been many fronts for this, but probably the most widely recognised is that of the role of the Jericho Forum, who coined the phrase "De-Perimeterisation".

Having an interest in the requirements for, and the design of, security architectures, I have got involved in work in this area over the past three and a half years or so. My initial contact with this area started when I edited an issue of the Information Security Technical Report (v.10 n.4) on "The Security Perimeter". In soliciting articles in this area, it was very interesting to talk to industry professionals with diverse views. While there seems to be an almost universal agreement on the scale and nature of the problem, what clearly divides people is how to deal with it. We had an article from the firewall community defending the requirements for some evolution of the security perimeter. We also had an article from David Lacey, one of the key proponents from the Jericho Forum, pressing the case for the long-term removal of the perimeter. What I found most interesting from reading the authors' contributions was how much else impacted on the discussion, from cross-site scripting to web services and the patch-fix cycle of dealing with security bugs.

A few years later, Terry Bebbington, one of our MSc students, did his MSc project on De-Perimeterisation. In his dissertation, he presented an extensive review of the Jericho Forum proposals, along with an analysis of how a proposed De-Perimeterised model (the Appgate Model) fared when measured against their requirements. The conclusion he drew from this analysis was that the Appgate Model did not meet the requirements of the Jericho Forum in full, and continued his work by designing an alternative framework. His alternative model uses existing standards to deliver an architecture which could possibly deliver on areas where the Appgate Model falls short.

While working as Terry's supervisor I became intrigued by the problems which were evident when you tried to follow the path set out by the Jericho Forum. In response to this stimulus, I turned to the Jericho Forum "roadmap" to carry out my own analysis of De-Perimeterisation. I then presented my findings at InfoSec '08. A short précis is that, while some of their goals were being met (e.g. developing products which allow portable devices to use corporate security services away from the corporate network), there were others which were likely to require much more intense research before they could work (e.g. the continued development of trust models; context-based marking for layered security on documents which are to be released outside the corporate network). The long and the short of it is that we can view the Jericho Forum's proposals as a useful stimulus for debate and the starting point for design, but that it is very much work-in-progress.

The latest development on this front from a personal perspective, is that I have a new research student, Graham Palmer (an ex-ISG MSc student, no less) who started in January '09 and is interested in De-Perimeterisation. Given that the problems faced by those with any type of corporate presence on the Internet are certainly not going to go away, I think that Graham is in for a very busy and productive time over the next few years...

WORKING WITH INDUSTRY
BY GERAINT PRICE

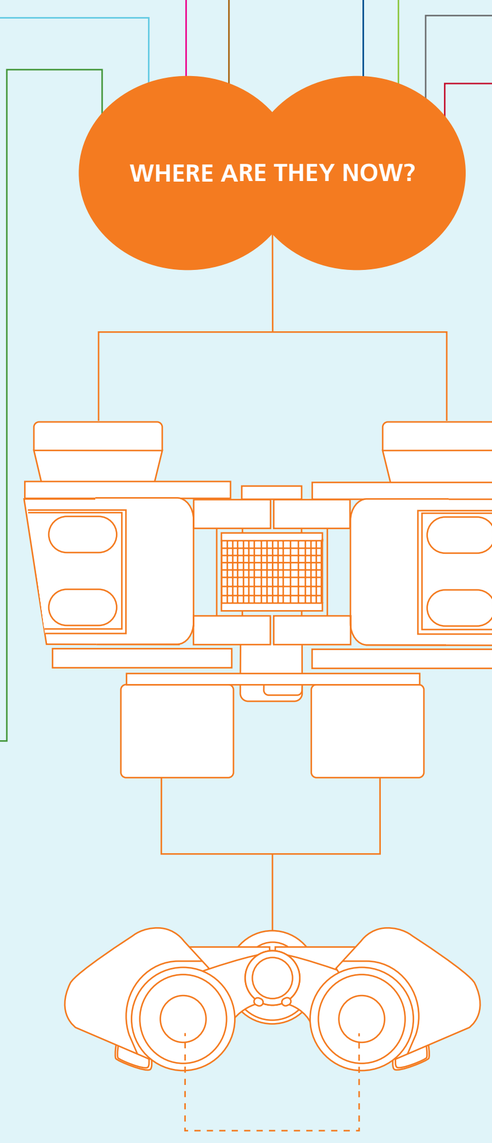
One of the things I enjoy most about being part of the ISG is how industry interaction forms a core part of my personal view on the problems that I tackle as an academic. In the past couple of years, I have been increasingly interested in how industry's view on identity and authentication shape the development and implementation of security services. Being given a free rein to interact with many industry bodies on these issues has been a great way of informing my own opinion on these debates.

The key events I have been involved in over the past 12 months are:

- Joining the Enterprise Privacy Group (EPG). The EPG is an affiliation of member organisations throughout the public and private sector, which meets to promote discussion related to privacy and identity. The sessions are very informative and debate is very lively!
- An invitation to take part in a round table discussion hosted by Verisign. The discussion centred on the area of consumer authentication, which really got to the heart of some of the problems facing those making money out of the Internet for consumer facing services.
- I have written a couple of pieces for a Computer Weekly blog which the ISG has contributed to. My aim here was to contribute an analysis on the ID Card plans. My key feeling from the discussion in this area is that there is no clear business reason for why ID Cards are being implemented, or at the very least, the shifting emphasis of the requirements makes it very difficult to carry out a thorough analysis on this topic.
- I spoke at the Universities and Colleges Information Systems Association (UCISA) annual conference in Glasgow on identity. Although not directly an industrial body, UCISA does take a service-led view of their role in providing computing facilities at the UK's Universities. After my presentation, I was engaged in quite lively discussion with a number of the delegates, and it was again interesting to get yet another perspective on the issues surrounding the management of identity.

I think that one of the key lessons I have learnt from these varied interactions is how we are only really just scratching the surface when it comes to shaping our understanding of how to manage identity securely and efficiently in a truly widespread environment. While there are solutions which make use of well known cryptographic and security engineering principles, making these fit in the modern heterogeneous world of the consumer focused Internet is still something of a challenge.

WHERE ARE THEY NOW?



Name: Aparna Murali
Year of Graduation: 2008

Where have you worked since graduation and in what roles?
I work with The Connect Partnership, a software consultancy dealing with financial data management. While studying, I started as a Quality Assurance Tester. After graduation I became a QA/Security Analyst. Given that it is a small company (about 20 people), I have taken up roles including tea-girl, event organizer, security guru, salesperson and recruiter! My security role includes pen-testing, BCP/DR, formulating security policy, providing security input for software development and R&D.

How did you find your job?
Personal contacts.

How has the MSc helped you in your career? It was a turning point in my career, giving me new direction at a time when I was fed up with software development.

Has your career in Information Security met your expectations, or not? So far, it has.

What advice would you give to ISG graduates entering the workplace?
Even if you are recruited as an infosec professional, your actual job may include some non-security work. Also, as security is usually at the bottom of the pile of priorities, be prepared to fight for your corner.

Name: Withheld
Year of Graduation: 2008

Where have you worked since graduation and in what roles?
Second Line Support Analyst.

How did you find your job?
I attended a careers fair.

How has the MSc helped you in your career? The MSc helped me get this job, since it is much more business related and relevant than my previous BSc in Computer Science. It's also quite well known in the industry and seen as desirable.

Has your career in Information Security met your expectations, or not? Due to a delay in my security clearance I am not yet able to work on any security-related projects! However, I hope that things will pan out in the long run.

What advice would you give to ISG graduates entering the workplace?
If you have no previous information security experience, my advice would be to look carefully at companies to ensure that you are joining one that will provide you with good security experience as well as some quality training. Graduate schemes can be a good way of getting your foot in the door, but try and contact someone on the inside to find out what the scheme is really like.

Name: Christopher McLaughlin
Year of Graduation: 2007

Where have you worked since graduation and in what roles?
Accenture: Security Analyst; EDS: Security Architect; and now IBM Global Business Services: Managing Consultant, Security & Privacy.

How did you find your job?
Tapping into the network of RHUL Alumni that are working in industry. Everyone I talked to was incredibly helpful and opportunities abound if you get involved.

How has the MSc helped you in your career? Definitely! It is well respected throughout industry and you will always meet alumni wherever you go.

Has your career in Information Security met your expectations, or not? After a few false starts, IBM is offering everything and more I wanted from a career in information security.

What advice would you give to ISG graduates entering the workplace?
Network, Network, Network! If you want to find a job in information security use the RHUL Forum, Alumni and Linkedin Groups. You will find someone who works in the industry sector or company you want to work for and they may well be able to help. Join security groups such as BCS ISSG, ISSA, IISP; these are all good ways of getting involved with the information security community.

Name: Terry Bebbington
Year of Graduation: 2007

Where have you worked since graduation and in what roles?
Security Architect on a major MoD project. Now a Security Consultant for Gartner.

How did you find your job?
My professional network.

How has the MSc helped you in your career? I have moved into positions and levels of role that would have been difficult to achieve without the MSc.

Has your career in Information Security met your expectations, or not? More than met them. I believe that every security professional should attend the MSc.

What advice would you give to ISG graduates entering the workplace?
Don't expect the degree to give you a right to a senior level position. The MSc provides a good level of understanding and will complement your career as you progress. The MSc is held in high regard within the market.

Name: Bhupesh Rana
Year of Graduation: 2007

Where have you worked since graduation and in what roles?
I am working as a Security Consultant on a Ministry of Defence project responsible for assessing engineering changes from a security perspective.

How did you find your job?
Through another MSc friend.

How has the MSc helped you in your career? Immensely. The degree is held in high esteem throughout the industry. It gave me the foundation towards a full-fledged security career. As I did not have a security role previously, at first it was a catch-22 situation for me. However, once I was in my current job then offers came flowing in from every corner!

Has your career in Information Security met your expectations, or not? Yes, it has been rewarding both professionally and intellectually.

What advice would you give to ISG graduates entering the workplace?
Use your network of friends and acquaintances in the industry and do not be shy of flaunting the Royal Holloway MSc reputation! Reinforce your MSc with interview techniques. Go for industry level professional certifications (e.g. CISSP/CISM/CISA etc.) in addition to your MSc, as this gives out the message that you are aware of industry requirements and are capable of building your knowledge base even further.

Name: Abhijeet Udas
Year of Graduation: 2007

Where have you worked since graduation and in what roles?
As an Information Security Consultant and Ethical Security and Penetration Tester.

How did you find your job?
Job Portals like Monster and recruitment agents.

How has the MSc helped you in your career? The MSc is an excellent course and I would recommend it to everyone. It helped me understand IT Security from a risk management perspective, which I was completely unaware of. It also gave me a broad understanding of business continuity and laws relating to information security.

Has your career in Information Security met your expectations, or not? My expectations will be 100% achieved the day I get a £750,000 pension!

What advice would you give to ISG graduates entering the workplace? Get your basics right. Make sure you network with people a lot! The class is full of people from all levels - senior management to fresh graduates. I wish I could study again at some point. It is an excellent way to network with peers and meet eminent figures in the IT security world. And not to mention the quickest way to get up to speed on new topics the right way!

Name: Mohammed Yousif
Year of Graduation: 2005

Where have you worked since graduation and in what roles?
I joined a security practice and the first project I landed on was the evaluation of the HP-UX O/S in line with EAL4. I then undertook a project on security-related functional tests. Next I joined the MOD's Defence Information Infrastructure (Future) project. Since then I have been working in a variety of different roles including vulnerability management, providing information security assurance, and security auditing.

How did you find your job?
Through speaking to other MSc students who were already doing similar work.

How has the MSc helped you in your career? It provided me with a broad and thorough understanding of Information Security.

Has your career in Information Security met your expectations, or not? Yes.

What advice would you give to ISG graduates entering the workplace?
I recommend you try to gain as much experience in different fields of information security as possible. The MSc is very well appreciated within the industry. Apart from the excellent teaching materials and the lectures given by individuals who are very highly regarded within the industry, another gem is your fellow students. Make sure you NETWORK on the course!!!

Name: Mark Stables
Year of Graduation: 2007

Where have you worked since graduation and in what roles?
Risk / threat analysis of systems, site tests / assessments.

How did you find your job? I knew of the company I work for through previous roles. I looked up the main person responsible for security and sent a CV directly.

How has the MSc helped you in your career? It showed the sheer range of careers within InfoSec. The qualification seems to be well respected and changed my career direction.

Has your career in Information Security met your expectations, or not? Absolutely. The work and people are extremely interesting, and roles allow you to work at multiple levels of project (e.g. from ``customer facing to computer facing).

What advice would you give to ISG graduates entering the workplace?
Try to establish a good idea of where you want to go career-wise; this puts you on much stronger footing when accepting and declining roles. It is relatively easy to move around, so if you go for the wrong job initially, it's really not the end of the world. I've found it really useful to keep in contact with other people from the course, both in order to discuss how we've found our various roles and find out when new jobs are open.

A MALTESE PARTNERSHIP

The small island state of Malta has provided a disproportionately large number of distance learning MSc Information Security graduates over the six years since the course was launched. This interest in information security has now been formally recognised through a partnership with St Martin's Institute of Information Technology, to provide local support for Maltese distance learning students.

St Martin's will provide application and scholarship assistance, access to the institute's computer laboratory and library. In addition, St Martin's offers meeting rooms and a small cafeteria, where distance learning students can arrange to study together. Royal Holloway is providing occasional weekend tutorial classes, where distance learning tutors will visit the local students and discuss their study progress.

The first batch of eight students started their study in October 2008. Keith Martin, who tutors on the module Introduction to Cryptography, said that the experience of meeting the Maltese students had been very positive. "While the tutorial class provided a good opportunity for the students to ask questions concerning their study, by far the greatest benefit was putting them all in touch with one another. St Martin's provides ideal facilities to locally support distance learning students and I am sure that they will benefit from them in the run up to the examination period." Robert Farrugia, a student who works for KPMG in Malta, commented: "The Maltese education system is very different from the UK system and so I really enjoyed the interactive aspects of the tutorials. The interaction with the tutor and my fellow students really helped in evolving my thoughts and understanding".

The strong interest in information security in Malta does not come as a surprise to Melody Morgan-Busher from KPMG. "The Government of Malta has an ambitious strategy to put the island in the top ten information societies globally by 2010. The show piece of this strategy is a major project known as Smart City Malta, which is backed by a Dubai telecommunications consortium". She points out that there are several drivers behind the desire of Maltese students to seek degrees from beyond the island shores. "Culturally Malta has a high regard for further education and especially for foreign tuition. Most parents are keen to see their children enter an IT career because there is a public perception here that it is a road to riches". She also points out that there are current financial incentives to enter further study. "The Government of Malta is actively supporting students willing to pursue a career in IT via schemes such as the MyPotential programme, where fees can be reimbursed. These schemes are designed to foster knowledge workers and so concentrate on sophisticated skills such as information security".

Chris Bonnici is a graduate of the campus programme in 2008: "I think that there might be several reasons for the interest in information security in Malta. During the last decade the Maltese economy has experienced a steep transition towards research and development, with a particular focus on pharmaceutical and ICT services and products. Such transition has led to an increased demand for a suitably qualified workforce. This, coupled with Maltese students' desire to acquire knowledge, has encouraged more students to pursue graduate studies, especially in ICT. The Maltese students' attraction to information security may therefore be explained as a mixture of two strong forces: a strong desire to acquire ICT knowledge, and an information security aware society which is increasingly becoming ICT infrastructure reliant".

Another driver for Maltese students is the future job prospects. According to Chris Bonnici, "The Maltese National ICT strategy aims to establish Malta as a regional leader in the provision of information security services by developing a physical hub for information security facilities, which will help Malta adopt a proactive, low-risk stance towards national security threats and day-to-day information security concerns. In addition, Malta intends to have 20% of its households connected to the next generation network (i.e. fibre by 2010)." Keith Cauchi, the MSc Alumni Chapter Leader for Malta, is Information Security Officer for the Malta Information Technology Agency: "Foreign companies have invested locally in the last few years, mainly offering software development services, although we have an ever increasing influx of online gaming companies hosting their services on the island. The Smart City Malta project is estimated to employ over 5000 IT professionals (such a figure is a very big number for the local industry). The future looks brighter than ever for IS graduates!"

It is hoped that the partnership with St Martin's Institute will continue to foster this interest and help to train the information security professionals that Malta needs for the further development of its IT industry. Charles Theuma, Principal of St Martin's Institute and architect of the partnership, believes that it will be a success. "Malta's history has left us with a strong notion of the need for security. Our island still has many of the remains of historical brick and mortar security mechanisms. In the twenty-first century it is a different type of security that we will need, and I am delighted that this partnership will equip Maltese students with the right skills for this challenge".

Recent Completed PhD Theses...

David Mireles "Efficient arithmetic on hyperelliptic curves with real representation."...
Waldyr Dias Benits Junior "Applications of Frobenius Expansions in EllipticCurve Cryptography."...
Shane Balfe "Secure Payment Architectures and Other Applications of Trusted Computing."...
Jiqiang Lu "Cryptanalysis of Block Ciphers."...
Miss Laiha Mat Kia "A Key Management Framework for Secure Group Communication in Wireless Mobile Environments."...
Imad Mahmoud Aref Abbadi "Digital Rights Management for Personal Networks."...
Paulo Sergio Pagliusi "Internet Authentication for Remote Access."...
Illana Shah "Quantum key exchange and mutually unbiased bases. "...

INSTANT KNOWLEDGE

The ISG is contributing to the Mobile VCE Core 4 research programme on "Instant Knowledge". This project is jointly funded by the Mobile VCE consortium, the Technology Strategy Board (TSB) and the EPSRC. It was launched in 2008 and builds upon previous work with the Mobile VCE to develop some of the key security issues which emerged during the recently completed Core 3 research project. Allan Tomlinson, who leads the ISG contribution, explained that "the project centres on the notion of a personal distributed environment involving mobile devices (such as phones, PDA's, laptops etc.) that uses context-sensitive information to extract and share knowledge in a useful way, whilst simultaneously addressing security and privacy issues".

This is a multi-disciplinary project lead by the Mobile VCE, whose membership consists of several industrial partners, including many mobile phone operators. The University of Strathclyde and University of Southampton are the two other academic partners involved in the project. The role of the ISG is to investigate the use of privacy enhancing technology in mobile devices to provide users with confidence that the mobile Instant Knowledge network can be trusted to protect the privacy of personal information shared within this environment.

MALAYSIAN CONNECTIONS
BY KEITH MARTIN

I am hurtling through the Kuala Lumpur evening traffic watching the colourful street stalls selling their wares and the taxis dodging lanes, while the diamond Petronas Towers sparkle high above the city centre. But, most impressively, there is a Royal Holloway bumper sticker on the back of the car in which I am being escorted to an evening dinner date.

This shouldn't be surprising, since this is Malaysia, a country which the ISG has been providing information security education services to since 1984, when Fred Piper first delivered a residential course on cryptography in London for a number of Malaysian organisations. He has subsequently made many visits to Malaysia and the ISG have hosted numerous Malaysian students and short-term research visitors.

My host for the evening is Lt. Col. Asmuni Yusof (MSc Graduate 2005), who is a Staff Officer Grade 1 (Cyberwar) in the Malaysian Joint Force Headquarters, as well as being Malaysian Alumni Chapter Leader. "I really enjoyed my time at Royal Holloway", reminisces Col. Asmuni. "I acquired knowledge from real experts in the field. This has helped me implement a sound information security strategy for the Malaysian Armed Forces." It's nice to meet a satisfied customer.

I am in Kuala Lumpur to speak at Cryptology 2008, a fledgling international workshop and conference in cryptology being held at the Putra World Trade Center. It is the very fact that the workshop is being held at all that is most impressive, since it demonstrates the rising interest in information security in Malaysia, not just as a subject of practice, but also as a research discipline.

Amongst the delegates is Dr Rabiah Ahmad (MSc Graduate 1998), now an academic in the Center for Advanced Software Engineering at the Universiti Teknologi Malaysia (UTM). I am curious why there is suddenly a great deal of interest in information security education in Malaysia. "There are probably two reasons", says Rabiah. "Firstly, many ICT organisations in Malaysia are only just beginning to realise the importance of building security into their systems. Secondly, we are seeing a huge influx of industrially sponsored students from the Middle East, which we assume are not able to currently study in western countries". Rabiah still has very fond memories of her time at Royal Holloway. "I am proud to have studied there", she says. "Royal Holloway's reputation remains very high in this area. The military and many government agencies prefer to send their staff to Royal Holloway for information security training".

My subject for the workshop sessions that I deliver is key management. Hence it is of more than passing interest that two of the other invited speakers are addressing the topic of quantum key distribution. One of them is Prof. Dr. Mohamed Ridza Wahiddin, who is Head of the Information Security Cluster of Mimos, a national applied research centre that focuses on information and communication technologies. "Our National Cyber Security Policy stresses that our Critical National Information Infrastructure will be secure, resilient and self-reliant. To this end quantum cryptography is important because it will be able to confront threats from the next generation super computers, which include quantum computers". Prof. Wahiddin has sent some of his employees to Royal Holloway for postgraduate studies. "There are already a significant number of Malaysian information security professionals that have successfully graduated from Royal Holloway. The ISG is always a preferred choice of ours for higher education in information security".

The Information Security Group has also been contributing to the development of research capability in Malaysian institutions through the training of PhD researchers. Recent graduates include Dr Miss Laiha Mat Kiah, who is Senior Lecturer and Head of the Computer System and Technology Department at the Universiti Malaya. Her family entertain me at a wonderful open air restaurant one evening. "I miss the people and facilities at Royal Holloway and, believe it or not, the weather!" She notes that the experience of conducting a PhD has greatly benefitted her professional life. "My experience in the ISG acquainted me with researchers from different backgrounds, cultures and intellects, and greatly improved my writing, communication and inter-personal skills, as well as my research work".

After the two-day workshop ends, the conference begins. One of the first speakers is one of my current Malaysian PhD research students, Geong-Sen Poh, who aims to complete in 2009 and return to work for his employer and sponsor, Mimos. He explains to me the value of a PhD in Malaysia: "There is a great emphasis on human capital development by both the government and the private sectors, in the quest to enhance the R&D capability of the nation. This means that there is a huge demand for PhD holders in the public and private higher education institutes and research institutions, as well as the industrial sector. Malaysia is aiming to be self-reliant in specialist areas such as information security". According to Geong-Sen, one of the crucial elements to successfully achieving this will be to forge partnerships and research collaborations with leading research organisations around the world, so he hopes to maintain his links with Royal Holloway when he returns home.

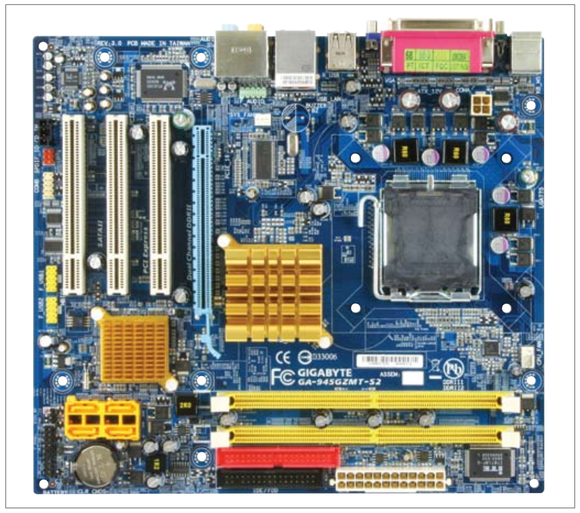
The Royal Holloway connections continue, as the delegate sitting in the back row in a leather jacket is Rosli Daud, an academic at MARA University of Technology, who will begin his research studies at Royal Holloway in a few months time. Rosli is one of the founders of the new Malaysian Society for Cryptology Research, which was established in 2007 to promote cryptology in Malaysia. Rosli explains: "Cryptography research is fairly new in Malaysia but increasing in popularity. The Malaysian government has put a lot of effort into grooming local experts in this area, as one of their strategies to strengthen self-reliance in the provision of future information security services".

Finally my allotted slot for an invited talk on key management research arrives. I am introduced by a smiling man wearing formal batik. He is Husin Jazri, Director of CyberSecurity Malaysia, the national co-ordination centre for computer emergency response, computer forensics, security assurance and training. And of course he is a Royal Holloway MSc graduate of 1997, arguably the most influential of our Malaysian alumni. When I visit the CyberSecurity offices later in the week, I am impressed by how much has been achieved to get information security onto the national agenda. I am shown the rows of monitors tracking global incidents twenty-four hours a day and a brand new forensic laboratory. Husin told me that the Malaysian government have been supportive in getting information security onto the national agenda: "The importance of information security and internet safety has fortunately been well understood by Malaysia's leaders". I am also impressed by some very readable information security leaflets designed to raise the national awareness of safe computing. "We are making some success in schools, organisations and banking sectors, however challenges still lie ahead in creating security awareness among SMEs".

After a relaxing weekend it is back on the presentation trail, with visits to Universiti Putra Malaysia (UPM), UTM and Multimedia University (MMU). It has been great to see information security on the rise in Malaysia and to meet so many friends, old and new, of the ISG.

The ISG's links with Malaysia continue to strengthen. In December 2008 two new Malaysian PhD students, Amizah Malip and Imran Suid, began their studies. In February 2009, Fred Piper visited UTM to teach a course, as well as to deliver a presentation to the Prime Minister's Office and attend a meeting of the Advisory Board of IMPACT (the International Multilateral Programme Against Cyber Threats), a UN initiative hosted by Malaysia. His host Rabiah Ahmad noted, "The students were really happy with Fred's visit. For those who wanted to visit Royal Holloway, but could not, this was the closest experience to being in the U.K.!"

And there is of course one more Malaysian link that I almost forgot to mention. Siaw-Lynn Ng, who is a part-time lecturer in the ISG, is originally from Sarawak. Some Malaysians who come to Royal Holloway like it so much that they never leave...



STATE OF THE ART RESEARCH IN TRUSTED COMPUTING

The Trust 2009 international conference was held at St. Hugh's College, Oxford from 6th - 8th April 2009. Building on the success of Trust 2008 (held in Villach, Austria, in March 2008), Trust 2009 (http://www.softeng.ox.ac.uk/trust2009/) focussed on trusted and trustworthy computing. The conference had two main strands, one devoted to technical aspects and the other devoted to the socio-economic aspects of trusted computing. Chris Mitchell acted as co-chair of the programme committee for the technical strand (along with Liqun Chen from HP Labs in Bristol). He was also co-editor of the conference proceedings, published by Springer.

The distinguished invited speakers included Prof. Sean Smith (Dartmouth College, US) and Prof. Eugene H. Spafford (Purdue University, US). Out of a total of around 25 research papers selected from those submitted, 15 were presented in the technical strand. Two of these 15 technical papers reported results of recent ISG research activities in this exciting area of security research.

The first is by Paul England and Talha Tariq (both from Microsoft Research), and is entitled Towards a Programmable TPM. Talha is a 2008 Royal Holloway Information Security MSc graduate, and the paper is based on work he conducted for his MSc project whilst an intern at Microsoft Research in Redmond. The paper describes a new architecture for trusted computing, in which an existing fixed-function Trusted Platform Module (TPM) is coupled with user application code running on a programmable smart card.

The second paper, A Property-dependent Agent Transfer Protocol, is by Eimear Gallery, Aarthi Nagarajan (Macquarie University) and Vijay Varadharajan (Macquarie University). Eimear, like Tariq, is a Royal Holloway Information Security MSc graduate (from 2002), who was awarded her PhD from Royal Holloway in 2006. For the last three years she has been working as a post-doctoral researcher on the EU-funded Open Trusted Computing project at Royal Holloway. This paper, which examines how a secure agent transfer protocol based upon TCG-defined mechanisms can be improved using property-based platform state information, is based on work conducted while Eimear was visiting Macquarie University in Sydney in late 2007.

THE CYBERSPACE FRONTIER HAS CLOSED!

The Information Security Group Alumni Conference included a stark assessment and surprising announcement by cyberspace legal expert Robert Carolina, who said that the "Cyberspace Frontier" has closed.

"The alumni conference gave me an opportunity to reflect on developments in cyberspace laws over the past 20 years", said Robert. "Like so many others in the early 1990s, I thought of the Internet as a brave new frontier that needed to be settled and tamed. In the same way that the US Census Bureau stated in 1890 that the US Western Frontier no longer existed, it is time for us to acknowledge that the Cyberspace Frontier is now closed".

Robert observed that governments, law enforcement officials, lawyers, judges, and policy makers in 1990 were generally unaware of the Internet's existence, or mode of operation. Nearly 20 years on, cyberspace experience has become commonplace. That knowledge has brought routine investigation and enforcement of the rules of society on activity that previously seemed to take place in a lawless void.

He stated that "Cyberspace now has borders" and that they are the same as the borders found in the real world. "For better or for worse, we as a species have chosen to organise our international existence around the theory of geographical sovereign states. These sovereigns continue to apply their laws as appropriate to online activity".

Robert concluded with a claim that the Internet has entered an age of de-globalisation. "The way in which we experience the Internet is increasingly driven by our physical location", he said. Examples cited included the different experience of the BBC News web site using the same URL from the UK and US. Robert also mentioned the increasingly common practice of automatically redirecting end-users to "local market" web sites. "We are too accustomed to the idea that the Internet is inherently international.

We have entered an age of "deglobalisation", or "regionalisation", of the Internet. This might one day extend to domain name or IP number allocation practices, although I hope things don't go that far".

In short, Robert noted in closing, "Cyberspace has come back down to Earth – where it always was".

CONFERENCE REPORT: PAIRING 2008

The International Conference on Pairing-based Cryptography (Pairing 2008) was held at Royal Holloway on September 1-3, 2008. The organisers were Steven Galbraith and Kenny Paterson from the Information Security Group. This was the third in a series of events on pairing-based cryptography (the first was held in Dublin in 2005 and the second in Tokyo in 2007).

Pairing-based cryptography is currently a hot topic in theoretical cryptography and the fact that Royal Holloway hosted the event is testament to the ISG's reputation as a leading player in this subject area.

The 74 participants hailed from various countries within Europe, as well as Canada, China, India, Indonesia, Japan, Taiwan and the USA. There were three invited talks, given by Nigel Smart (University of Bristol), Florian Hess (Technical University of Berlin) and Xavier Boyen (Voltage Security, USA). The programme also comprised twenty contributed papers and the proceedings were published by Springer as volume 5209 of Lecture Notes in Computer Science.

The lectures were held in the stylish new Management auditorium. The conference was relaxed and friendly, and there was plenty of time for research discussions and collaboration. Highlights of the event included a brisk walk in Windsor Great Park and a champagne reception in the cloisters of the north quad of Founder's building. The event was sponsored by Microsoft Research, Voltage Inc, and the London Mathematical Society.

Pairing 2009 will be held in Stanford University, USA.

BOOK REVIEW: VIRTUAL SHADOWS

Karen Lawrence Öqvist was amongst the first intake of distance learning MSc Information Security students in 2003. During her MSc project she was inspired by the subject of privacy and since graduation she has continued her research on the subject. This has resulted in the publication of Virtual Shadows: Your Privacy in the Information Society by the British Computer Society.

Virtual Shadows is a gentle, but engaging, read. The delicate and personal journey that Karen has undertaken between fear of privacy erosion and awe of the power of modern information sharing, pervades and enhances the book. Above all, this is a reflective book, by someone with genuinely unbounded curiosity. Karen has been on an intellectual journey and she wants to share with us both the dangers and the opportunities that she encountered along the way.

The book begins with an introduction to some of the modern web applications that are having an impact on personal privacy. I found the insights into blogging culture fascinating. I remain astounded that a woman from Salt Lake City can write a blog about her life that is so successful that she lives off the profits of click-through advertising. Unless she is making it up, it would seem that Heather Armstrong is a proponent of the antithesis of privacy, she is a personal online soap opera. But who are the people with all this time to read her blog? Even more alien to me, and yet no more fascinating, are Karen's experiences of World of Warfare and Second Life. Yes, these are games, and the players have pseudonymous identities, but the actions of these players do reveal information about the real people that lie behind them. I am intrigued by the potential consequences of this information "getting out", perhaps to a future employer.

One of the drivers behind Karen's research for Virtual Shadows is her consideration of the relationship between privacy and online safety of children on the Internet. These are issues that I am just beginning to grapple with, and her review is a welcome wake up call. How can a parent manage a child's use of the internet without understanding how the child uses it? I don't personally visit chatrooms, so who am I to supervise my children in them? Should I just ban them? Karen's advice is, if I may say so, very *Swedish*. It is of course to travel on our children's internet journeys with them, to join them in their forums, to learn to see the brave new online world through their eyes. It certainly makes sense in theory...

The book continues with a review of various privacy eroding activities around the world. Much of this discussion doesn't make you proud to be British, as we are apparently world leaders in privacy erosion (although Karen never mentions how bravely we have been fighting national identity cards). Yet Karen is quick to point out that behind most of the applications that sound heinous to privacy advocates, there tend to lie genuine advantages that many may embrace. I know this all too well, for a young girl was murdered near my home in 2006. The police not only retraced her entire journey home from CCTVs on the bus and all along the street, but they eventually found her murderer, partially through related evidence. Is this a good or a bad thing?

Karen points out that we might be the last generation to even consider this last question. The use of surveillance is growing fast, but public resistance minimal. While massive personal data losses make terrific news stories, they don't appear to stop people signing up for loyalty cards. Karen comments that "the information age has unleashed a surveillance society that feeds on our imaginary fear fuelled by media hype – we are on the cusp of a new surveillance era", and suggests that "our children will not think to question its logic, because they have grown up accustomed to being tracked". That's Karen with her gloom hat on, first thing in the morning, before a cup of coffee. But then she drinks her brew. "From another perspective, we are part of an information society that has given us all a voice. This conversation enables us to feel part of a community where we can be sure that someone out there is listening and interested in hearing what we have to say". (I hope you are!).

Whether you are a "concerned and careful" believer in privacy, an "unfazed" Facebook addict, or someone like me with a muddled and inconsistent approach to personal privacy (no loyalty cards, but a personal website), Virtual Shadows will make you think just a little but harder about the "digital information residue" that you leave behind, and its possible consequences.

By Keith Martin

SOCIO-TECHNICAL STUDIES IN THE ISG
BY LIZZIE COLES-KEMP

The ISG has always been proud of its interdisciplinary research tradition. From the beginning we recognised that security solutions are created through a synthesis of different disciplines and that the study of security problems often requires a number of disciplinary perspectives. Traditionally we have been very strong in mathematics and computer science interdisciplinary studies, but during the past 10 years have had an increasing interest in socio-technical studies through our work with information systems.

The societal and organisational aspects of information security are of interest to a number of our staff and research students. In 2008 I was awarded a research grant for a socio-technical study in privacy and consent decision making in on-line transactions. The grant, entitled Visualisation and other Methods of Expression (VOME), is funded by the Technology Strategy Board and the two research councils: EPSRC and ESRC. It enables information systems researchers in the ISG to collaborate with social scientists and engage in community as well as technology research. Peter Wild, Director of the ISG, believes that this strengthens the ISG's research base: "VOME is an exciting extension to the research portfolio of the ISG, adding a vital social science dimension to it. This aspect of information security research is becoming increasingly important as privacy and identity issues impinge on the everyday lives of the public. We are delighted to be working with community teams in Sunderland and to be collaborating with social scientists in Salford and Cranfield".

I am now supervising four PhD students specialising in security management research on risk perception and the measurement and evaluation of security management frameworks. Said Alazri is Director of IT Security and Standards for the Royal Court of Oman: "The focus of my research is measuring the effectiveness of information security management systems (ISMS) models. Understanding effectiveness will help organisations choose the right ISMS model for their needs". Terry Walker works for a European Computer Security Incident Response Team: "I am interested in self-correcting ISMSs within complex organisations. This involves studying the interaction between technological, organisational, human and social systems. My research will hopefully enable organisations to more accurately quantify and compare the actual state of an ISMS with the desired state, and take action to align the two".

The future for socio-technical research in the ISG is looking bright. As well as the above developments, from mid-2009 the ISG is hosting a medical sociologist from St. George's Hospital, University of London as part of an EPSRC funded knowledge transfer programme. Having a medical sociologist in our midst will help us contribute still further to the study of security challenges that affect us all.

For further details on our socio-technical research programmes, please contact lizzie.coles-kemp@rhul.ac.uk.

Visualisation & other Methods of Expression

Pictured: The 19th HP Day was held at the Windsor Building, Royal Holloway

THE NINETEENTH HEWLETT-PACKARD COLLOQUIUM ON INFORMATION SECURITY

The 19th "HP Day" event was held in the Windsor Auditorium and attended by over 100 delegates from industry, academia and government. Thanks to HP's generous sponsorship, we were able to invite three distinguished speakers to the event: Prof. Arjen Lenstra from the Ecole Polytechnique Federale Lausanne (EPFL), Switzerland; Mikko Hypponen, Chief Research Officer at F-Secure Corporation; and Steve Marsh from the UK Government Cabinet Office.

In his highly entertaining lecture, Arjen Lenstra gave us fascinating insights into the mathematics of factoring algorithms. The lecture was delivered at a level that allowed everyone in the audience to gain some appreciation of the spectacular progress that has been made since the founding work of Fermat more than 300 years ago. His talk was followed by a lively discussion on the merits and demerits of elliptic curve cryptography, and the potential impact of quantum computing on public key cryptography.

Mikko Hypponen's talk focussed on the evolution of the hacker community. He gave several examples of investigations in which he was personally involved. These highlighted the increasing sophistication of malware, the emergence of targeted attacks, the internationalisation of hacking, and the manner in which hacker skills and tools are now readily available "for hire". Mikko went on to discuss the need for an agency like Interpol for the Internet. Such an agency would reduce the difficulties in policing hacker activities across international boundaries. The audience was left in no doubt about the serious threat posed to business and society by malware writers, and the organised gangs who consume their products.

Finally Steve Marsh provided an overview of the information security challenges facing government, particularly in the light of recent data loss incidents. He discussed strategies for information assurance and the problem of how to restore the public's confidence in the government's ability to securely handle personal data. As part of this, he proposed that we need to better understand the barriers to use of on-line government services, and to develop societal norms for balancing harm and benefit. Steve also gave insights into the way in which privacy impact assessments are now being built into the evaluation processes for government information handling systems.

During the breaks, posters showcased recent research by HP and ISG researchers. Prof. Kenny Paterson summed up the day: "The HP colloquium is always a great opportunity for networking and hearing from leading lights in the field. This year we were blessed with three outstanding speakers, and we are very grateful to HP whose sponsorship makes the event possible. We are now looking forward to a special 20th anniversary HP day in December 2009".

CRYPTOGRAPHY MEETS NETWORK SECURITY PART 2: SSH

BY KENNY PATERSON

Attentive readers might recall my article in last year's ISG review, reporting work on the security issues arising in encryption-only configurations of IPsec. Now with two PhD students from the ISG, Martin Albrecht and Gaven Watson, we have hit the headlines with our work analysing the security of another important protocol suite, SSH.

Originally designed as a replacement for insecure remote login procedures such as rlogin and telnet, SSH has since become a general purpose tool for securing Internet traffic. Version 2 of SSH is standardized by the Internet Engineering Task Force (IETF) in a series of RFCs, effectively Internet standards documents. Many different implementations of SSH are available, with the OpenSSH implementation accounting for more than 80% of SSH implementations on the Internet.

We discovered a basic design flaw in the SSH Binary Packet Protocol (BPP) which is responsible for providing basic encryption and integrity protection for data on an SSH connection and which is specified in RFC 4253. The flaw arises because of the way in which a particular length field is defined in the BPP packet format, in combination with SSH's default use of CBC mode encryption. The flaw opens up the possibility of limited plaintext recovery attacks against SSH.

By analysing the OpenSSH source code, we were able to translate theoretical understanding built up from studying the RFCs into attacks that work in practice against the default configurations of all versions of OpenSSH up to version 5.1. The particular attacks against OpenSSH exploit subtle differences in the way in which OpenSSH handles the different error messages that can arise during cryptographic processing of SSH packets. The OpenSSH attacks are able to recover up to 32 bits of plaintext from an SSH connection with a success probability of 2^{-18}.

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.

After prototyping and testing the attacks, we worked with the UK's Centre for Protection of National Infrastructure (CPNI) to disclose the attacks and countermeasures against them. This involved working with CPNI staff and a number of affected vendors and users ahead of CPNI's public announcement of the attacks [1]. As a consequence, vendors including OpenSSH, SSH.com, OpenSolaris, Bitvise and Dropbear issued updates to their code. In February 2009, OpenSSH released OpenSSH version 5.2; one of the main motivations for this new release was to include several countermeasures to protect against the attacks [2].

We have produced a technical paper documenting the attacks and explaining why they are possible in spite of extensive existing formal security analysis for SSH. In this sense, the research illustrates some of the limitations of current approaches to security analysis for complex protocols like SSH. The technical paper was accepted at the 2009 IEEE Symposium on Security and Privacy, a leading annual security conference. Further details are available from kenny.paterson@rhul.ac.uk.

[1] CPNI Vulnerability Advisory. Plaintext Recovery Attack Against SSH. http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt, 14/11/2008 (revised 17/11/2008).

[2] OpenSSH announcement. OpenSSH 5.2. http://www.openssh.org/txt/release-5.2, 23/2/2009.

SECURING MOBILE VOICE END TO END

BY JOHN WIGLEY

Mobile telephone networks are a good example of a pragmatic approach to security, intending to be just secure "enough" for the majority of users without incurring significant costs or inconvenience. Secure "enough" in the context of a mobile telephone is frequently likened to equivalent security to a conventional land line telephone, but for some users this is not good enough.

Users that consider themselves at significant risk of interception from commercial, political, or law enforcement intelligence gathering efforts often turn to secure voice systems that can provide end to end encryption of their voice calls. These mobile secure voice systems can range from secure voice integrated into custom designed mobile phones, to add-on hardware modules that connect on to commercial mobile phones, to software-only solutions for smartphones.

Mobile secure voice systems often have significant user-experience limitations such as introducing significant delays into the call setup, poor audio quality, and delays in speech transmission reaching a second or more – all of which contribute to a poor conversational experience.

My project looked at what could be done in order to improve the user experience – particularly for commercial business users who may be mandated to use secure voice systems whilst resisting the idea. This involved looking at how latency could be reduced, how automated security policy enforcement could ease use, and how a low cost software-only implementation could achieve strong cryptographic security on a standard smartphone by using a network-based security augmentation service.

In terms of Security, limitations were also often evident in the products examined, particularly in the authenticated key establishment protocols used to protect against Man In The Middle (MITM) attacks. An authentication protocol commonly used by secure voice systems was examined that involves the callers reading a series of numbers or letters to each other. One of the aspects of this project questioned whether this "spoken hash authentication" could be relied upon to provide strong security.

Experiments were conducted to see how easy it was to spoof this authentication by cutting and pasting recorded speech together. It turns out that in some situations it's relatively easy to convincingly impersonate a person speaking digits aloud, and therefore to perform a MITM attack, thereby enabling an attacker to circumvent the authentication protocol and eavesdrop calls.

John Wigley was the 2008 BCS-ISSG David Lindsay Memorial Prize winner for his MSc project report, which can be downloaded in full at: http://www.ma.rhul.ac.uk/tech

STUDYING IN BLOCK MODE

The MSc in Information Security is now available in "block mode". This means that students in fulltime employment can come to Royal Holloway to study modules over dedicated one week periods, rather than attending the campus weekly on day release from employment.

But what is it like studying in block mode?
Stephen Khan is a senior consultant with GlaxoSmithKline. He has had a varied career in information security, most recently dealing with perimeter security and risk management. Stephen had been toying with a degree in information security for some time: "I had nothing to encapsulate my experience/knowledge within information security. I found by speaking with others that Royal Holloway was highly regarded within information security circles and offered a flexible MSc programme with a broad syllabus. I played with the idea of studying the MSc for some years but never could find the time between travelling abroad for work, family life, and of course social life".

However that all changed when the ISG launched the MSc in block mode. "The main driver for me choosing block mode was time out of the office. Block mode works very well for me as I can get away from the office and focus on my MSc studies for short periods. For people who work in industry, block mode is a great idea as you get all the course material delivered over one intensive week".

However, do block mode students "miss out" on a more leisurely campus experience? Is it not all too intense?
"I don't think this is an issue – block mode is great", enthuses Stephen. "Let me explain. I have interacted with part-time students who attend the campus on day release, so my viewpoint is informed. Day release students attend the campus for one or two sessions a week and then quickly go back to work, so they do not always get the full benefit of engaging with people from different sectors. On block mode, we tend to meet in the evenings and socialise, since many of us are resident for the week. We have used all the facilities the campus has to offer, including the student union bar and disco, not forgetting the library! We have discussions about information security, often from different perspectives, and of course forge relationships. I see this as a major advantage of block mode".

What about ongoing academic support when block mode students are not on campus?
"Most of the MSc modules are now supported by an online learning environment called Moodle", comments Chez Ciechanowicz, the MSc Programme Director. "Block mode students have access to all the learning materials that fulltime and part-time day release students have access to." Keith Martin, who presents a module on the normal campus programme, said that he has often been caught out by block mode students. "On several occasions I have been asked a question in Moodle and replied by saying that we will be covering that subject next week, only to be told that the student has already had that lecture because they have studied it in block mode... Block mode is helping to keep us on our toes".

Stephen is very pleased with his experience of block mode thus far. "The course has given a broad view of information security and the different considerations one has to take into account in practice. It has also given me the tools to review security with a different set of eyes, not just technically. I have also made some good friends. We keep in touch and bounce ideas off one another". He has a last piece of advice for anyone considering following the MSc in block mode: "Consider staying near the campus during your block mode weeks and meeting with your classmates during the evenings. I find this a useful and important enhancement to the teaching sessions during the day".

Answers to Jason Crampton's questions on p10

Answer to question 1: 1210 and 2020, but can you prove there are no others?

Answer to question 2: water – read the clue as "H to O"

The 2008 Alumni Reunion Conference Programme:

Session 1: Security education
- Fred PIPER (RHUL): Opening remarks
- Chez CIECHANOWICZ (RHUL): The RHUL Information Security Masters Degree
- Mark CURPHEY (Microsoft): How Royal Holloway Saved my Life

Session 2: Risk management
- Neil HARE-BROWN (QCC): Information Security Risk – A Natural Way of Thinking
- Martin VIRGO (Metropolitan Police): Managing Risk

Session 3: Software security
- William ROTHWELL (Abatis (UK) Limited): Non-signature Based Malware and Intrusion Prevention
- Rich SMITH (HP): A Protection Scheme Against Unknown File-Format Vulnerabilities
- Nicholas C P HUMPHREY (EBI Security Ltd.): Open Source Security for Business

Session 4: Network security
- Ian D McKINNON (Logica): Tigger Team
- Rodrigo MARCOS (SECFORCE Ltd.): Hijacking TCP Sockets in the Web

Session 5: Invited speaker
- Professor Whitfield DIFFIE (Sun Microsystems): Directions in Information Security

Session 6: Security management technology
- Matthew MARTINDALE (KPMG): A Harmonised Shield: Achieving Efficiencies Through Integrated Assurance
- James THONG: Export Controls on Information Security
- Babatunde AKINJAYEJU: Endpoints and Virtual Infrastructure Security

Session 7: Security techniques
- Henrich POEHLS (SVS, University of Hamburg and ITSEC, University of Passau): Hash-based Digital Signatures for Today's Dynamic Data: Still up to the Job?
- Chan Yeob YEUN: Ubiquitous Network Security – Evolution, Opportunities, Security Challenges and Future Directions
- Wouter VLEGELS: Cyber Defence Concept Development

Session 8: Security management
- Bandana GILL (BSkyB): WiMAX over the Horizon
- Meng-Chow KANG (Microsoft): Information Security Risk Management
- Jim HEARD (Centrica Energy): Information Security Challenges in the Upstream and Midstream Gas and Energy Production and Development Environment

Session 9: Standards
- Andrew CHURCHILL: Fraud Management Standards
- Paul MARCH: Payment Card Industry

HONORARY DEGREE AWARDED TO PROF WHITFIELD DIFFIE

Professor Whitfield Diffie has been awarded the Degree of Doctor of Science, Honoris Causa from Royal Holloway. The University of London awards Honorary Degrees to those of conspicuous merit, who are exceptional in their line of work or have provided service to the College.

Whitfield Diffie is a US cryptographer and one of the pioneers of public key cryptography. He is Chief Security Officer of Sun Microsystems, Vice-President and Sun Fellow. Best known for his 1975 discovery of the concept of public key cryptography, Whitfield Diffie spent the 1990s working primarily on the public policy aspects of cryptography. Prior to assuming his present position in 1991, he was Manager of Secure Systems Research for Northern Telecom. He is a Fellow of the Marconi Foundation and the recipient of awards from organisations including the IEEE, the Electronic Frontiers Foundation, NIST, NSA, the Franklin Institute and the ACM. He is a Visiting Professor in the Information Security Group at Royal Holloway.

FAREWELL TO SCARLET

We are very sorry to be saying goodbye to Scarlet Schwiderski-Grosche, who first joined the ISG in August 2001 as a post-doctoral researcher working with Chris Mitchell on the SHAMAN project. This project was concerned with security of mobile systems, and Scarlet co-authored two key chapters in the book Security for Mobility, which was largely based on the project results.

After playing a large part in bringing SHAMAN to a successful conclusion, Scarlet was appointed as a lecturer in the ISG in January 2003. Since then she has played a major role in the group, helping to teach a variety of MSc courses and acting as research chair for the ISG. She has somehow combined all this activity with looking after a growing young family.

She has recently been offered the post of Program Manager for External Research in the EMEA region with Microsoft Research in Cambridge. This prestigious post will, we hope, enable Scarlet to stay in regular contact with the ISG. Working in Cambridge will also be convenient for Scarlet, as her family are now based there.

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

This newsletter has been printed on Cyclus Offset 100% recycled paper.
Design: Allyson Waller / Editing: Keith Martin