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-reach 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 of 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, Thames, VISA, and Unisys. As 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 Caica (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 feedback 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 Wintapping 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 give us local communities of expertise for information security professionals around the world.

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

TWO CONFERENCE DINNERS. The overwhelm-

03
On a related topic, and in recognition of our long-standing links with the transport industry, the SCC was delighted to welcome two 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 industry to investigate the future of SIMs/USIMs and alternative security solutions for mobile devices, especially for machine-to-machine applications. This work was published in an Elsevier Technical Report.

In the summer we hosted visiting researchers from Umeå (Sweden) and ITU-T (the ITU telecom standards body), 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 sponsorship in 2008 when Kobayashi Markantonakis was promoted to Reader in Electrical and Computer Engineering at the University of Hertfordshire. However, there was very little time for self-congratulation as preparations were underway for CARDS2008 in September.

This was the 8th Smart Card Research Conference worldwide. It is the largest international conference in the area of smart cards and led to many interesting publications and ongoing work.

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 store in time for the ETSI module of the same name. However, this was not the biggest event in the smart card world that year.

There were great concerns in the Netherlands concerning the impact of the MIFARE NL, and indeed the government, which means that a wider publicised attacks on the MIFARE system. As a result the team was commissioned by the Dutch transport ministry, and our report was well received.

This was not the biggest event in the smart card year. Our new course book (Smart Cards, Tokens, Security and Applications) hit the on-line store in time for the ETSI module of the same name. However, this was not the biggest event in the smart card world that year.

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

In the summer we hosted visiting researchers from Umeå (Sweden) and ITU-T (the ITU telecom standards body), 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 sponsorship in 2008 when Kobayashi Markantonakis was promoted to Reader in Electrical and Computer Engineering at the University of Hertfordshire. However, there was very little time for self-congratulation as preparations were underway for CARDS2008 in September. This was the 8th Smart Card Research Conference worldwide. It is the largest international conference in the area of smart cards and led to many interesting publications and ongoing work.

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 store in time for the ETSI module of the same name. However, this was not the biggest event in the smart card world that year.

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

In the summer we hosted visiting researchers from Umeå (Sweden) and ITU-T (the ITU telecom standards body), 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 sponsorship in 2008 when Kobayashi Markantonakis was promoted to Reader in Electrical and Computer Engineering at the University of Hertfordshire. However, there was very little time for self-congratulation as preparations were underway for CARDS2008 in September. This was the 8th Smart Card Research Conference worldwide. It is the largest international conference in the area of smart cards and led to many interesting publications and ongoing work.

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 store in time for the ETSI module of the same name. However, this was not the biggest event in the smart card world that year.

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

In the summer we hosted visiting researchers from Umeå (Sweden) and ITU-T (the ITU telecom standards body), 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 sponsorship in 2008 when Kobayashi Markantonakis was promoted to Reader in Electrical and Computer Engineering at the University of Hertfordshire. However, there was very little time for self-congratulation as preparations were underway for CARDS2008 in September. This was the 8th Smart Card Research Conference worldwide. It is the largest international conference in the area of smart cards and led to many interesting publications and ongoing work.

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 store in time for the ETSI module of the same name. However, this was not the biggest event in the smart card world that year.
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 CIR: 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 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 not as simple as the cryptographic equivalent of patting your head and rubbing your stomach. We are currently developing work that shows how simple mathematical techniques can be used to scramble representations of information in such a way as to prevent the uncovering of the information. Cryptography alone provides confidentiality and integrity. In the case of a digital archive, we need to provide availability as well.

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 combining 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 simulta-

ewnously 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 5G has been working with the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) to produce new standards for business to business 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 closely with the editor of the new ISO/IEC 29150 standard, which describes authenticated encryption techniques based on public-key cryptography. The editor of the standard, Prof. Yuliang Zheng of the University of North Carolina, has also written 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-PERIMETER-ISA TION BY GERÄNT 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 threats for this past year, but probably the most widely recognised is that of the role of the Ichen Jericho Forum, who coined the phrase “De-Perimetratisation”.

Having an interest in the requirements for, and the design of, security architecture, I have got involved in work in this area over the past three and a half years of 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 for this area, it was interesting to talk to industry professionals with diverse views. While there seems to be an almost unanimous agreement on the scale and nature of the problem, what they agree is that people are slow to react to it. We had an article from the firewall community defining the requirements for some evolution of the security perimeter. We also had an article from David Larking, one of the key proponents from the Jericho Forum, presenting the case for the large removal of the perimeter. What I found most interesting was 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-Perimetrisation. In his presentation, he presented an extensive review of the Jericho Forum’s work, along with an analysis of how a proposed De-Perimetrised 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-Perimetrisation. 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 see 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-EGC MSc student, no less) who is now working providing computing facilities at the UK’s Universities’ Computing Network. 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 issue 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 security and efficiently and 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 consumer focused Internet is still something of a challenge.

WORKING WITH INDUSTRY BY GERÄNT PRICE

One of the things I enjoy most about being part of the 5G is how industry interaction forms a core part of my professional work. From personal perspective, is that I have had an article from the firewall community defining the requirements for some evolution of the security perimeter. We also had an article from David Larking, one of the key proponents from the Jericho Forum, presenting the case for the large removal of the perimeter. What I found most interesting was 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-Perimetrisation. In his presentation, he presented an extensive review of the Jericho Forum’s work, along with an analysis of how a proposed De-Perimetrised 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-Perimetrisation. 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 see 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-EGC MSc student, no less) who is now working providing computing facilities at the UK’s Universities’ Computing Network. 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 issue 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 security and efficiently and 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 consumer focused Internet is still something of a challenge.

TAKING INFORMATION SECURITY TO SCHOOLS

Keith Martin was the guest speaker at the Bexley Education Cluster Event in October. About working in Primary and Secondary schools in the Bexley Education Cluster, which consists of 16 primary and secondary schools, Keith talked about cryptography and Dan Miller from The Da Vinci Code through a range of activities.

Keith shared his cryptography expertise with the pupils by discussing how simple mathematical techniques can be used to scramble representations of information in such a way as to prevent the uncovering of its meaning. He explained how simple mathematical techniques can be used to scramble representations of information in such a way as to prevent the uncovering of its meaning. He explained how simple mathematical techniques can be used to scramble representations of information in such a way as to prevent the uncovering of its meaning.

Keith enjoyed the day but told his Royal Holloway MSc students: “It’s much more nerve-racking to deal with corporate security issues away from the classroom than with post- graduates. For one thing, they always ask much more difficult questions!”

Simon Pyne, Co-Chairman of the Bexley Education Cluster and Head of Information Security at Primary School, thanked Keith for his interesting talk, commenting, “We didn’t realise how important cryptography is in our everyday 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 to discussing cryptography with primary school students than with post-graduates. For one thing, they always ask much more difficult questions!”

One of the things I enjoy most about being part of the 5G is how industry interaction forms a core part of my personal work on the problems that I tackle as an academic. In the past couple of years, I have been increasingly interested in the changing role of security and identity and authentication shape the shifting emphasis of the require-
Your corner.

priorities, be prepared to fight for

Even if you are recruited as an infosec

or not?

Security met your expectations,

a time when I was fed up with software

your career?

Personal contact.

How has the MSc helped you in your career? It was incredible. I left 3 years ago at a very low salary. I wish I had stayed on the MSc. I was treated like royalty in my new job. Can I come back to the MSc for another year?

As a Senior Consultant for Gartner.

Where have you worked since graduation and in what roles?

As an Information Security Consultant

the RHUL Forum, Alumni and Linkedin

graduates entering the workplace?

What advice would you give to ISG graduates entering the workplace?

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

What advice would you give to ISG graduates entering the workplace?

Where have you worked since graduation and in what roles?

As an Information Security Consultant

the RHUL Forum, Alumni and Linkedin

graduates entering the workplace?

What advice would you give to ISG graduates entering the workplace?

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

What advice would you give to ISG graduates entering the workplace?

Where have you worked since graduation and in what roles?

As an Information Security Consultant

the RHUL Forum, Alumni and Linkedin

graduates entering the workplace?

What advice would you give to ISG graduates entering the workplace?

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

What advice would you give to ISG graduates entering the workplace?

Where have you worked since graduation and in what roles?

As an Information Security Consultant

the RHUL Forum, Alumni and Linkedin

graduates entering the workplace?

What advice would you give to ISG graduates entering the workplace?

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

What advice would you give to ISG graduates entering the workplace?

Where have you worked since graduation and in what roles?

As an Information Security Consultant

the RHUL Forum, Alumni and Linkedin

graduates entering the workplace?

What advice would you give to ISG graduates entering the workplace?

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

What advice would you give to ISG graduates entering the workplace?

Where have you worked since graduation and in what roles?

As an Information Security Consultant

the RHUL Forum, Alumni and Linkedin

graduates entering the workplace?

What advice would you give to ISG graduates entering the workplace?

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

What advice would you give to ISG graduates entering the workplace?

Where have you worked since graduation and in what roles?

As an Information Security Consultant

the RHUL Forum, Alumni and Linkedin

graduates entering the workplace?

What advice would you give to ISG graduates entering the workplace?

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

What advice would you give to ISG graduates entering the workplace?

Where have you worked since graduation and in what roles?

As an Information Security Consultant

the RHUL Forum, Alumni and Linkedin

graduates entering the workplace?

What advice would you give to ISG graduates entering the workplace?

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

What advice would you give to ISG graduates entering the workplace?

Where have you worked since graduation and in what roles?

As an Information Security Consultant

the RHUL Forum, Alumni and Linkedin

graduates entering the workplace?

What advice would you give to ISG graduates entering the workplace?

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

What advice would you give to ISG graduates entering the workplace?
A MALTESE PARTNERSHIP

The small island state of Malta has provided a disproportionately large number of distance learning MIS Information Security graduates over the six years since the programme 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 study to arrange together. Royal Holloway is providing occasional weekend tutorial classes, where distance learning tutors will visit the local students and discuss their progress.

The first batch of eight students started their studies in October 2008. Keith Pagliusi, who tutors on the module Introduction to Cryptography, said that the students 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, for the far greater benefit was putting them all in touch with one another. St Martin’s provides ideal facilities to locally support distance learning students and I hope that they will benefit from them in the run up to the examination period.”

Recent Completed PhD Theses...

David Mirren “Efficient arithmetic over hyperelliptic curves with real multiplication by both the genus two and genus three curves.”


Shane Bafle “Secure Payment Architectures and Other Applications of Information Theorem.”

Jinglu Li “Verifying Oracle and Cryptos.”

Mia Zahra Mia Kiah “A Key Management Framework for Secure Group Communication.”

“Using Wireless Mobile Environments, an Information Security Awareness security awareness which is increasingly becoming ICT infra-

Recent Completed PhD Theses...

Another driver for Maltese students is the chance to work in a multi-cultural environment. Hence the ISG has since collaborated with Royal Holloway and the Maltese government have provided a number of opportunities for Maltese students to seek degrees abroad. Since 2009 the ISG has provided a number of opportunities for Maltese students to seek degrees outside of Malta. In 2010 the show piece of this strategy is a major project known as Smart City Malta, which is backed by a Dubai telecommunication consortium. The project aims to provide an integrated city environment where the Maltese students to seek degrees from the island’s institutions. "Culture-

for KPMG in Malta, commented: "The G4S is now a key part of the G4S’ strategy for the Malaysian Armed Forces. We’ll need to continue to provide the right skills for this challenge." 

Instant Knowledge

The ISG is contributing to the Maltese VCE computer science programme on “Instant Knowledge”. This project is jointly funded by the Maltese VCE consortium, the Technology Strategy Board (TSB) and the EPSRC. It was launched in 2008 and builds upon previous work done for the Mobile VCE to develop some of the key security issues that must be considered for completing a successfully completed 3 Core research project. Shane Bafle, who is a part of the ISG team, explained that "the project centres on the notion of a personalised distributed environment involving mobile devices (such as phones, PDAs, 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 led by the Mobile VCE, whose membership consists of several industry partners, including many mobile phone operators. The University of Sheffield and University of Southampton are the two other academic partners involved in the project. The role of the ISG is to develop a cryptographic means of enhancing technology in mobile networks. In particular, the confidence that the mobile Instant Knowledge network can be trusted to protect the privacy of personal information exposed within this environment.

Instant Knowledge

The ISG is contributing to the Maltese VCE computer science programme on “Instant Knowledge”. This project is jointly funded by the Maltese VCE consortium, the Technology Strategy Board (TSB) and the EPSRC. It was launched in 2008 and builds upon previous work done for the Mobile VCE to develop some of the key security issues that must be considered for completing a successfully completed 3 Core research project. Shane Bafle, who is a part of the ISG team, explained that "the project centres on the notion of a personalised distributed environment involving mobile devices (such as phones, PDAs, laptops etc.) that uses context-sensitive information to extract and share knowledge in a useful way whilst simultaneously addressing security and privacy issues.

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 border and military security mechanisms. In the twenty-first century it is a different type of security that we need, and I am delighted that this partnership will equip Maltese students with the right skills for this challenge.”

The Government of Malta has put a lot of effort into grooming local 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 flooding international workshop and conference on cryptography being held at the Putra World Trade Centre. It’s the first time the workshop is being held at all in 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 Centre for Advanced Software Engineering (CASe) at 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 IT 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 IT professionals who want to pursue degrees in information security.”

I am also impressed by some very good Malaysian students established, and so concentrate on sophisticated skills such as information security”. Chris Bonnici is a graduate of the campus programme in 2002. “I think that these might be several reasons for the interest in information security in Malta. During the last decade the Maltese economy has experienced a steep transformation towards research and development, with a particular focus on telecommunications and services. This 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 information security. Moreover, an information security awareness society which is increasingly becoming ICT infra-

The strong interest in information security in Malta does not come as a surprise to Malgorzata-Morgan-Rusher from KPMG. “The Government of Malta has a ambitious strategy to put the island in the top ten information societies globally by

MALAYSIAN CONNECTIONS BY KEITH MARTIN

I am hunting 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. 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 1994, 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 LI. Col. Ahmad Yusuf (MBA, Graduate 2007), who is a Staff Officer Grade 1 (C-Security) in the Malaysian Joint Force Headquar-

ters, as well as being Malaysian Armed Forces Chapter Leader. “I really enjoyed my time at Royal Holloway,” reminisces Col. Ahmad. “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!”

The Government of Malta has put a lot of effort into grooming local experts in this area, as one of their strategies to move into the top ten information societies globally by

To this end cryptographic is important in ensuring that our con-

front threats from the next generation support. As we have seen, self-sufficiency in information security services is key.

Finally my allotted slot for an invited talk on key management research arrived. I am2008 is a key part of the G4S’ strategy for the Malaysian Armed Forces. We’ll need to continue to provide the right skills for this challenge.”

The ISG has linked with Malaysia continue to strengthen. In December 2008 there was a visit of Malaysia Business and Ivan Sugh, between their studies. In February 2009, Fred Piper visited Malaysia to help set up the Systems and Multimedia (SIM) ISG. It has a PhD in Information Security in Malaysia but increasing in popularity.

The ISG’s links with Malaysia continue to strengthen. In December 2008 there was a visit of Malaysia Business and Ivan Sugh, between their studies. In February 2009, Fred Piper visited Malaysia to help set up the Systems and Multimedia (SIM) ISG. It has a PhD in Information Security in Malaysia but increasing in popularity.

The ISG has linked with Malaysia continue to strengthen. In December 2008 there was a visit of Malaysia Business and Ivan Sugh, between their studies. In February 2009, Fred Piper visited Malaysia to help set up the Systems and Multimedia (SIM) ISG. It has a PhD in Information Security in Malaysia but increasing in popularity.

The ISG has linked with Malaysia continue to strengthen. In December 2008 there was a visit of Malaysia Business and Ivan Sugh, between their studies. In February 2009, Fred Piper visited Malaysia to help set up the Systems and Multimedia (SIM) ISG. It has a PhD in Information Security in Malaysia but increasing in popularity.

The ISG has linked with Malaysia continue to strengthen. In December 2008 there was a visit of Malaysia Business and Ivan Sugh, between their studies. In February 2009, Fred Piper visited Malaysia to help set up the Systems and Multimedia (SIM) ISG. It has a PhD in Information Security in Malaysia but increasing in popularity.

The ISG has linked with Malaysia continue to strengthen. In December 2008 there was a visit of Malaysia Business and Ivan Sugh, between their studies. In February 2009, Fred Piper visited Malaysia to help set up the Systems and Multimedia (SIM) ISG. It has a PhD in Information Security in Malaysia but increasing in popularity.

The ISG has linked with Malaysia continue to strengthen. In December 2008 there was a visit of Malaysia Business and Ivan Sugh, between their studies. In February 2009, Fred Piper visited Malaysia to help set up the Systems and Multimedia (SIM) ISG. It has a PhD in Information Security in Malaysia but increasing in popularity.
BOOK REVIEW: SHADOWS

Karen Lewien-Daniel was amongst the first to make sure that the DFH was held at Royal Holloway on September 1-3, 2008. The conference was included as part of the 15 technical papers selected from those submitted, two of which were presented in the technical papers section. Two of these papers were specified for their technical excellence and were selected as the best papers for the conference. The conference was held at the University of Oxford in 2007.

Karen Lewien-Daniel was amongst the first to make sure that the DFH was held at Royal Holloway on September 1-3, 2008. The conference was included as part of the 15 technical papers selected from those submitted, two of which were presented in the technical papers section. Two of these papers were specified for their technical excellence and were selected as the best papers for the conference. The conference was held at the University of Oxford in 2007.

Karen Lewien-Daniel was amongst the first to make sure that the DFH was held at Royal Holloway on September 1-3, 2008. The conference was included as part of the 15 technical papers selected from those submitted, two of which were presented in the technical papers section. Two of these papers were specified for their technical excellence and were selected as the best papers for the conference. The conference was held at the University of Oxford in 2007.

Karen Lewien-Daniel was amongst the first to make sure that the DFH was held at Royal Holloway on September 1-3, 2008. The conference was included as part of the 15 technical papers selected from those submitted, two of which were presented in the technical papers section. Two of these papers were specified for their technical excellence and were selected as the best papers for the conference. The conference was held at the University of Oxford in 2007.
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 overview of the information security challenges facing government, particularly in the light of recent data loss incidents, he discussed strategies for improving information assurance and the problem of how to restore the public’s confidence in the government’s ability to secure data handled by public agencies. 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. What was also given insights into the way in which privacy impact assessments are now being made in the evaluation processes for government information handling systems.

During the breaks, posters showcased recent research by HP and ISG researchers. Prof. Kenny Paterson talked on the evolution of the hacker community, he gave several examples of investigations in which he was personally involved. These highlighted the increased 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 improving information assurance and explained the problem of how to restore the public’s confidence in the government’s ability to secure data handled by public agencies. 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. What was also given insights into the way in which privacy impact assessments are now being made in the evaluation processes for government information handling systems.

Securing mobile end to end
By John Wiley

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 this 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 risk of targeted attacks recently dealing with perimeter security with a different set of eyes, particularly in the authenticated key exchange process. Their project questioned whether this "spoken authentication" could be relied upon to provide strong security.

Experiments were conducted to see how easy it was to spoof this authentication by putting and pasting recorded spoken text together. It turned out that in some situations it was relatively easy to convincingly impersonate a person by reading a series of numbers or letters into 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 putting and pasting recorded spoken text together. It turned out that in some situations it was relatively easy to convincingly impersonate a person by reading a series of numbers or letters into each other. One of the aspects of this project questioned whether this "spoken hash authentication" could be relied upon to provide strong security.

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 the tools to review security with a different set of eyes, not just technically but also in more broader contexts. I find this a useful and important experience.
The 2008 Alumni Reunion Conference Programme:

Session 1: Security education
- Fred PIPER (RHUL): Opening remarks
- Chez CIECHANOWICZ (RHUL): The RHUL Information Security Masters Degree

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

Session 4: Network security
- Nicholas C P HUMPHREY (EBI Security Ltd.): Open Source Security for Business
- 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): Information Security Risk Management Standards
- Bandana GILL (BSkyB): WIMAX over the Horizon
- Meng-Chow KANG (Microsoft): Information Security Risk Management
- Jim HEARD (Centrica Energy): Information Security Challenges

Session 7: Security techniques
- Henrich POENITS (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
- Chan Yeob YEUN: Ubiquitous Network Security – Evolution, Opportunities, Security Challenges and Future Directions
- Wouter VLEGELS: Cyber Defence Concept Development

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.

Rich SMITH (HP): A Protection Scheme Against Unknown File-Format Vulnerabilities
Nicholas C P HUMPHREY (EBI Security Ltd.): Open Source Security for Business
Ian D MCKINNON (Logica): Tigger Team
Rodrigo MARCOS (SECFORCE Ltd.): Hijacking TCP Sockets in the Web
Professor Whitfield DIFFIE (Sun Microsystems): Directions in Information Security
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 POENITS (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

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 Cyclos Offset 100% recycled paper.
Design: Alyson Waller / Editing: Keith Martin