CONTACT

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/apply.html

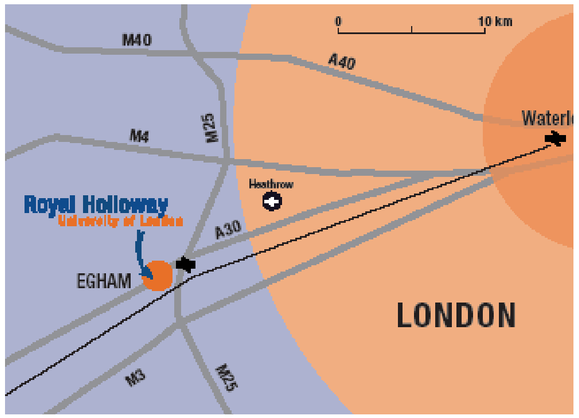
For more specific queries about the Information Security Group and postgraduate admissions, please contact:

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

HOW TO GET TO ROYAL HOLLOWAY:

Royal Holloway's location is on the A30 between the village of Englefield Green and the town of Egham.
It is just 19 miles from the centre of London, minutes from the M25, M3, M4 and M40 motorways.

London Heathrow Airport is seven miles away and trains from Egham to Waterloo, central London (and Eurostar), take 35 minutes. College buses run to and from Egham station during term.

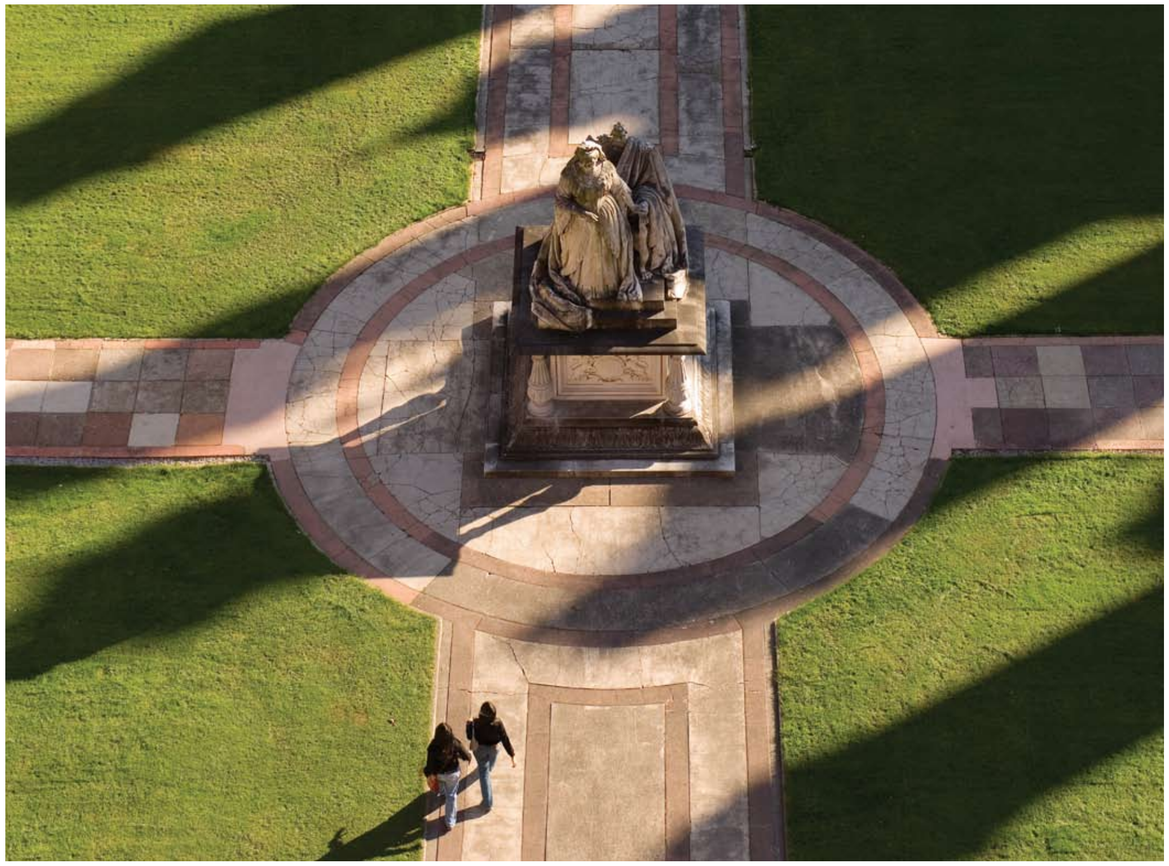


This newsletter has been printed on Cyclus Offset 100% recycled paper.
Design: Allyson Waller / Appleyard Media Ltd

Royal Holloway
University of London

Information Security Group

Review 06 / 07



CONTENTS

NEWS IN BRIEF:

- **Prof. Fred Piper has received the accolade of being admitted to the Information Systems Security Association (ISSA) Hall of Fame for his services to the UK IT security community.**
- **Prof. Michael Walker has been elected Fellow of the Royal Academy of Engineering. Election to the Academy is by invitation only and is granted to the UK's most distinguished and knowledgeable engineers.**
- **Dr Steven Galbraith has been awarded a prestigious five-year EPSRC Advanced Fellowship to look at the future uses of elliptic curves in cryptography.**
- **Royal Holloway's Department of Computer Science has teamed up with the ISG to launch an undergraduate BSc Computer Science with Information Security programme. This pioneering programme recognises that information security is now a fundamental computing issue and is no longer solely an area of specialisation.**

MIXED MODE STUDY: ONE GRADUATION, THREE WAYS TO TRAVEL THERE

Two exciting new developments have made Royal Holloway's MSc in Information Security easier to access for students who find it difficult to regularly attend the Egham campus.

The Information Security Group at Royal Holloway was essentially founded around this popular degree programme in 1992 and has now seen over 1000 students graduate and enter the security profession around the world.

Block Mode

The first of the new modes of teaching is the establishment of "block mode" teaching, which allows students to attend Royal Holloway's campus for intensive study weeks. Thus, rather than obtaining day-release to come to campus for a half day per week for 11 consecutive weeks, students can come to campus for one full week and cover all the required material for one MSc module.

Block mode teaching was offered for the first time in the 2006-07 study year for three of the core MSc modules and has proved so successful that there are now plans to extend this teaching mode.

Yvette Du Toit from Ernst & Young was one of the first block mode students: "Block mode has been a huge help because it provides me with the much needed flexibility to juggle a very busy work schedule, my studies and my personal life and, as a result, I can manage my studies more successfully".

A further advantage of block mode teaching is that it opens up the possibility of delivering MSc courses at off-campus venues. According to Professor Fred Piper, Director of External Relations: "There is considerable interest from certain organisations in having employees attending some of our MSc modules as continuous professional development courses, without studying for the whole programme – block mode allows us to take a module to their premises and deliver on site".

Moodle Learning

A second major development has been Royal Holloway's recent adoption of the Moodle learning environment across campus. This allows registered students to access course materials, learning resources, study forums and tutor support in a cleanly integrated web environment both on and off campus. It also facilitates an online study community, where students studying the new block mode can meet students attending weekly on campus and share experiences and support.

Aparna Murali is a full-time student who travels to the campus from north London on a weekly basis: "The discussion forums make it possible to debate related issues with fellow students at my own time of convenience, and I have also found them a good place to meet course colleagues and make friends".

"Mixed mode" Teaching

Block mode teaching has provided the third and final component required to fulfil the ISG's vision for delivering the MSc in Information Security in a manner sufficiently flexible for the needs of modern students, who are often constrained both financially and by the demands of professional careers. (The second of these components was realised in 2003 with the launch of the distance learning version of the course, which now has over 150 registered students studying the programme from around the world.)

This vision, which is often referred to as "mixed mode", is for students to pick and choose between day-release campus attendance, block mode and distance study, as they assemble the modules necessary to obtain their degree. It is widely anticipated that there will be a high demand for mixed mode study. MSc Programme Director Chez Ciechanowicz is certainly convinced: "This type of blended learning is undoubtedly the way of the future for information security education".

Royal Holloway
University of London

MSc in Information Security

2006/07 – ONE-WEEK 'BLOCK MODE' COURSES

The Information Security Group (ISG) is pleased to announce that, starting in the academic year 2006/07, it will be possible for part-time students to study the taught modules of the Royal Holloway University of London postgraduate MSc in Information Security by attending one week (5 day) courses.

This new (block) mode of delivery will be an alternative to the existing delivery mode of half a day per week for 11 weeks which continues to be available.

Initially, i.e for the year 2006/07, only three of the core courses will be available in block mode. However, it is planned to introduce the new delivery of the remaining core course and some of the options from 2007/08.

Students will be able to 'mix and match' the two modes of delivery if they wish. All (block and traditional) students sit the same exams during the normal university examination term. There is no difference in the degrees awarded between block and traditional students.

Places on the new block mode course will be limited. Interested students should contact the ISG secretary directly.

The block mode courses may also interest professionals wishing to deepen their understanding in the Information Security field.

The ISG is able to offer block mode courses throughout the year by prior arrangement as a CPD (continuing professional development) course either on campus or off-site.

Photography: Victor Fieldhouse

DISTANCE STUDENTS MEET AT SUMMER SCHOOL

The second Distance Learning Information Security Summer School was held at Royal Holloway on the weekend of the 16/17th September 2006. This event provided the opportunity for around 40 students of the distance learning MSc in Information Security, arriving from 16 countries, including Algeria, Iceland, Latvia and the U.A.E., to meet one another.

Some students were new starters but most were old hands, many meeting one another for the first time after having corresponded online. Attendees enjoyed a series of presentations on diverse subjects, including an update on the Computer Misuse Act by Owen Brady of the FSA; an overview of location-based security issues by Chris Mayers from Citrix Systems, and the history and analysis of Hagelin cipher machines by Carlos Cid.

However, more than anything, participants enjoyed the opportunity to meet staff and fellow students from the programme, exchange notes and plan their new study year. According to Siddhartha Arora, who is in his third year of the programme and studies from Switzerland while working for IBM in Zurich, the best thing about the summer school was meeting faces, old and new. "Nothing beats face-to-face encounters," says Sid, "and the summer school provided me with the perfect motivation to kick off the new term".

Stephen Thornber, who is based in Leicester, felt that the atmosphere and the quality of the presentations made his trip more than worthwhile. "My worst experience was the hangover on Sunday morning," he added.

COMMENT: THE TIMELY EMERGENCE OF IISP BY PROF FRED PIPER

Although information security (IS) has always been important, the concept of specialist qualifications in this area is fairly recent. The IS "profession" began to emerge in the 1980s, albeit in an ad hoc and piecemeal fashion and with little formality or structure. Industry leaders were self-trained and many individuals had the label of IS specialist, whereas in reality they had a particular focus on only one area of IS. At the end of the 1980s, both CISSP (Certified Information Systems Security Professional) and the Royal Holloway MSc were under development. These were, I believe, the first dedicated qualifications available in the public domain.

Since then, the number of people specialising in IS has increased at an amazing rate, prompted by many positive events, including our increasing reliance on IT and the advent of the Internet and electronic trading, coupled with an unacceptably large number of viruses, trojans and other high profile security breaches.

As the number of security specialists increased, directors and managers in government and industry needed to trust that those who were responsible for IS in their organisation were competent, in the sense that they had the necessary knowledge and skills, and would behave in a professional and ethical manner.

"How do you recognise a competent IS professional?" was a question acquiring ever increasing importance by the late 1990s. It was this that prompted a small group of people to propose the formation of a professional body for IS. Their ideas were published in a document called: "The Institute for Information Security professionals: A Blueprint", dated 7th December 2004, in which a professional institute was proposed to "promote information security as a recognised discipline through the provision of a framework for developing, improving and measuring the competence of information security practitioners, recognised by employers, regulators and other professional bodies". The Institute of Information Security Professionals (IISP) was launched in February 2006 and has attracted much interest. Well over 1000 individuals have joined as associates and it has the support of more than 40 corporates and government departments.

Although in its infancy, the IISP has the ambitious principal objective to "advance the professionalism of information security practitioners and thereby the professionalism of the industry as a whole. By the year 2010, the Institute aims to provide a universally accepted focal point for the information security profession".

In addition, IISP aims "to act as an accreditation authority for the industry, and Membership and Fellowship of the Institute will be the internationally accepted gold standard for information security professionals".

In my view, it is its role as an accreditation body that justifies IISP. There are now numerous knowledge-based qualifications, including some high quality university degrees. However, these merely provide an indication of someone's level of knowledge, skills and/or competencies at a given time. Many of these qualifications, for example, university degrees, are awarded 'for life' with no obligation on the recipient to practice the discipline or to keep informed about advances in the area. However, membership of a professional body like IISP should imply that the individual has followed a CPD programme which, as one of its aims and objectives, ensures that they have maintained an active interest in the discipline.

Joining IISP should enable graduates from programmes such as the Royal Holloway MSc in Information Security to build on this sound knowledge-based qualification, to acquire further skills and competencies and to become leaders of the profession.

For more information, www.instisp.org.

STAFF PROFILE: STEPHEN WOLTHUSEN

Dr Stephen Wolthusen became our newest member of staff when he joined the Information Security Group in 2006.

Broadly, what are your research interests?
My current research interests fall into two main categories. One is the modelling and simulation of critical infrastructures and their inter-dependencies. The second is network security: particularly the deduction of adversary behaviour from incomplete and limited information sources, and the security of tactical networks.

By what route did you discover information security as a research discipline?
I specialised quite early by starting a part-time position at a newly formed information security department at a government lab in Germany and have been in the field ever since. It is an extremely rich area of research with many fascinating and difficult questions that has retained its fascination for me from the day I started.

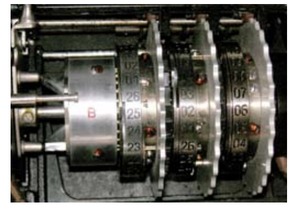
You clearly believe in working closely with industry and government, why is that?
After more than a decade working in a government research environment, I am clearly aware of the limitations of both government-directed research and collaborations with industry, but on balance find that close collaboration with both can yield highly interesting research questions. Neither industry nor government can of course be purely curiosity-driven, and must focus on concrete problems. However, there is often a surprising degree of flexibility to pursue new lines of inquiry if a convincing case can be made. In addition, some research areas require levels of effort and funding that are simply beyond the scope of the funding instruments available to academic research.

What contribution do you think academic research in information security makes to practitioners in the field?
The practice of information security suffers from being rather less evidence-based than might be acceptable in other areas. Some of this stems from the fact that threats and risks tend to be very difficult to characterise and quantify, so information security in the field is quite often a faith-based activity. At the same time, uptake of results from research by industry and practitioners tends to be quite slow. Academic information security can contribute in a number of important ways, beginning with the establishment of more rigorous approaches to characterising adversaries and threats which allow a better assessment of the efficacy of security measures, and by trying to stay (or advance) one step ahead of attackers and new threats in devising new defensive mechanisms, algorithms and protocols. All this, of course, also requires practitioners, including the information security industry, to engage academic information security in a more meaningful fashion. In the past, it has sometimes taken several decades for research results to be taken up by industry – such delays are simply no longer acceptable.

What do you think the big research challenges in security are for the coming decade?
I see one of the key challenges emanating from ubiquitous computing: the distribution of networked computing facilities, often embedded invisibly in devices from toasters to main battle tanks. Current information security paradigms and assumptions imperfectly capture this type of environment, and there may even be emergent properties relevant to information security which we cannot yet see with sufficient clarity.

Are you enjoying working in the ISG?
One of the most compelling arguments for my joining the ISG was, in my view, the unique breadth and depth of information security research conducted here. It takes a critical mass of interacting researchers to create a highly productive research environment in which ideas can be elaborated and tested, and I have found this to be the case and the fact that the ISG is a very collegial environment makes this not just exciting, but enjoyable.

What's the best single thing about living in the UK?
So far I've only worked here and haven't quite got around to the living part just yet...



A CODE WORTH CRACKING

In early 2006, the ISG was approached by author and film director Richard Belfield, who had an intriguing request: could we design some puzzles for his forthcoming book on famous unsolved codes and ciphers? His publishers, Orion Books, had acquired a World War II Enigma machine, worth around $30,000, and intended to give it to the first person to solve the puzzles.

Carlos Cid, Laurence O'Toole and Kenny Paterson, who all have professional and personal interest in ciphers and cipher machines, began discussing the proposal in more depth. One of the most challenging aspects of designing the puzzles was that Richard did not want people with access to large amounts of computing power to enjoy a significant advantage over other people attempting to solve the puzzles. This suggested that a certain amount of lateral thinking would need to be employed in both setting and solving the puzzles. At this point, Jason Crampton was added to the puzzle team because of his interest in cryptic crosswords.

As is often the case, the hardest part of constructing the puzzles was getting started. After a number of false starts, the team developed an "architecture" for the set of puzzles and then set about designing the individual puzzles. As the work progressed, roles emerged for each member of the team: Jason played a creative role in proposing ideas for the puzzles, and tested out his ideas with Kenny and other team members, while Carlos and Laurence wrote the computer programs that produced the ciphertexts for most of the puzzles.

The book was published on 28 September 2006. No-one has yet claimed the prize. Could it be you? Further details about the competition, including forums for puzzle-solvers, are available from www.isg.rhul.ac.uk/enigma.

MSc in Information Security

Pioneering group within Information Security research, education and training, offering independent expertise in a field where trust and integrity are paramount.

World-leading Masters Programme in Information Security

- Taught by experts from industry and academia
- Available part-time, full-time or in block mode
- Available worldwide by online learning
- Flexible entry requirements
- Unique association with (ISC)²

One of the largest Academic Security Groups in the world

- Thriving PhD programme
- Strong research and consultancy links with industry and government
- Smart Card Centre funded by Vodafone and Giesecke & Devrient

Professional Training

- Bespoke specialist security training
- Postgraduate Diploma in Information Security (in partnership with QCC Information Security Training)

Royal Holloway University of London

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

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

THE INFLUENCE OF HUMAN BEHAVIOUR ON SECURITY

Members of the Information Security Group and the Psychology Department at Royal Holloway are joining forces as part of a new government-funded programme designed to investigate the human factor in online security threats. The investigation will look at internet users' vulnerability to fraudulent schemes, viruses and hacking, as well helping to stop information theft that could so easily be avoided with the right knowledge.

The programme, developed under the UK government-funded Cyber Security Knowledge Transfer Network, is managed and directed by QinetiQ, a leading international defence and security technology company. It brings together 11 leading research partners from the fields of technology and human security, as well as eight security researchers from UK companies including BT, HP, Microsoft and Vodafone.

Lizzie Coles-Kemp from the ISG is one of the researchers participating in the project. Lizzie has recently joined the ISG, having previously been employed in a consulting role, and her wide research interests include risk assessment and organisation theory, as well as information security management systems. Commenting on the collaborative nature of the project, she said: "This project gives the Information Security Group an opportunity to present some of its thinking on information governance models and explore further how human factors affect the security management systems that an organisation chooses to deploy. We hope to contribute to the design of strategies for evaluating human stakeholder risks, as well as methods for the triangulation and contextualisation of human and non-human stakeholder risk perspectives. We are very excited about how this project allows us to undertake Information Security research with other disciplines including Computer Science, Social Science and even Criminology."

Dr Marco Cinnirella, Senior Lecturer in the Department of Psychology, adds: "This is an excellent opportunity to synthesise psychological research on beliefs, social influence and communication with relevant interconnected work in other disciplines such as Information Security. It presents an ideal vehicle for forging productive collaborations between researchers in these and related fields." With the involvement of the Psychology Department, the project hopes to answer the questions surrounding human vulnerability and susceptibility to cons and online scams, which often only require human ignorance in order to be spread and become a massive problem.

This project represents a new direction in research activities for the ISG. "Social engineering is arguably the biggest threat to your bank account," says Professor Fred Piper. "You may hear clichés such as computers don't commit crimes, people do, and the problem is – they're true. That's why it's so important that we get involved in human factors."

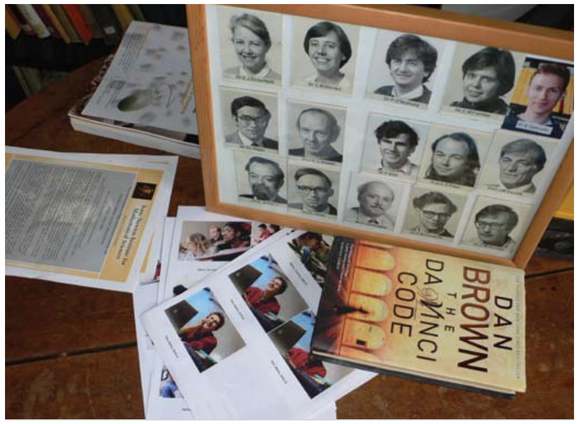
For further information, www.isg.rhul.ac.uk / www.ktn.qinetiq-tim.net.

Cyber Security
Knowledge Transfer Network

THE ISG SMART CARD CENTRE OPEN DAY: 10th SEPTEMBER 2007

Last year on September 12th, the Smart Card Centre at Royal Holloway held the third of its annual open days. This free exhibition provided an opportunity for visitors to find out some of the latest developments in smart card technology and industry research, both emanating from Royal Holloway and beyond. Visitors were able to watch practical demonstrations from industrial exhibitors and Smart Card Centre research projects, as well as benefit from the excellent networking opportunity to meet clients, competitors, staff and students in a friendly academic environment. In addition, visitors enjoyed a buffet lunch and an introductory tour of the famous Picture Gallery. The event culminated in a presentation by Professor Pierre Paradinas from CNAM-Cedric, Paris, on measuring the performance of the Java CardTM platform.

The 4th Smart Card Centre Open Day will be held on September 10th 2007. The format will remain similar to previous years and so all interested in smart card security are advised to put this date in the diary. The 2007 Open Day address will be given by Brian Dobson from Transport for London on the London Transport Oyster Card. Entrance to the exhibition is free however a donation of £25 per person to help cover refreshment costs, including buffet lunch, is requested. Payment should be made on the day by cash or cheque (cheques should be made payable to Royal Holloway, University of London). For more details, visit www.scc.rhul.ac.uk or email keith.mayes@rhul.ac.uk.



WAS SOPHIE NEVEU AN ISG PHD STUDENT?

This is just one of a number of interesting questions that the ISG has been asked since the publication of Dan Brown's *The Da Vinci Code*, which mentions on several occasions that the heroine studied cryptography at (the) Royal Holloway.

Under the assumption that no publicity is bad publicity, here is a brief round-up of some of the ISG meetings with the media over the past year.

On *The Da Vinci Code*, Fred Piper spoke to BBC3 about whether codes and ciphers played important roles on modern society. Fred also gave radio interviews to a number of stations on the occasion of *The Da Vinci Code* DVD release.

Keith Martin was interviewed on Channel 4's series *Decoding Da Vinci*, as part of their investigation into the truth behind some of the codes and symbols used in Dan Brown's novel. He also provided comment to teenage science magazine *Flipside* on whether cryptographic claims made in Dan Brown's *Digital Fortress* had any grounding in reality.

Meanwhile, Kenny Paterson appeared in a local newspaper feature, where they compared life as a "real cryptographer" with that of Dan Brown's heroine.

Elsewhere, Fred Piper was interviewed live on Channel 4 News for comments following the revelation that the judge in the intellectual property court case between Dan Brown and the authors of *The Holy Blood and the Holy Grail* had encoded a message in his final deliberation. Fred also discussed security research training on Radio Singapore International and in the Singapore Sunday Times.

Kenny Paterson featured widely in the information security press on the subject of vulnerabilities in IPsec.

Finally, Keith Martin was interviewed by BBC World's News Hour to explain what the implications were of Xiaoyun Wang's well-publicised attacks on hash functions. But even this had a Sophie Neveu theme when Keith was asked if he thought she was a "cryptographic heroine"...

SECURING WIRELESS SENSOR NETWORKS

They are small, potentially fragile, have low computing power, limited memory and you may not even know exactly where you have deployed them! Is there any hope for securing wireless sensor networks? With applications ranging from military intelligence gathering to environmental monitoring, wireless sensor networks have the potential to change all our lives.

The ISG has commenced two major projects that will attempt to at least partially answer questions concerning wireless sensor networks' security.

MoD/DoD consortium

In 2006, the ISG joined a consortium of around 25 organisations to bid for joint UK Ministry of Defence/ United States Department of Defense funds to undertake a research programme exploring advanced technology for secure wireless and sensor networks to support future coalition operations.

The IBM-led consortium successfully won the contract, and the "International Technology Alliance" (ITA) programme was officially launched in September 2006. The ITA project will run for five years in the first instance, with a possible renewal for a second five year period. The ISG's funding under ITA could total more than £1 million over 10 years.

The project spans four interconnected technical areas, with the ISG's contribution falling under the area entitled: "Security Across a System of Systems". This title reflects the fact that successful future military operations will depend on the capability of coalition forces from several countries to quickly gather, interpret and share battlefield information to co-ordinate actions. So the research faces the challenges of enabling interoperability and communications across disparate military units, in harsh military environments, using mobile ad hoc networking and sensor technologies.

The programme will provide open collaborative research cutting across national, institutional and technical area boundaries and, with 25 partners, is one of the world's largest collaborative technology programmes. The ISG's involvement is led by Kenny Paterson and Stephen Wolthusen. Funds from the programme are being used by the ISG to employ Shane Balfe as a research assistant and fund a PhD student, as well as to establish collaborative research with staff at IBM Research, the University of Maryland, City University of New York, the University of York and others.

Further details from Kenny Paterson (kenny.paterson@rhul.ac.uk).

Three year project

A second independent three year project, funded by the EPSRC and led by Keith Martin, is looking at cryptographic key management for wireless sensor networks. The lack of organisational structure in a typical wireless sensor network means that it can be highly advantageous to preload sensors with all the keying material that they will need to see out their functional lives. So what is the most effective means of predistributing keying material in order to support the security services that will be required by the network after deployment?

Maura Paterson, who recently completed a PhD with the ISG, has been employed on this project to assist in finding out.

Further information from Keith Martin (keith.martin@rhul.ac.uk).

LIFE AFTER PHD?

The ISG has over 70 PhD research students, working on a wide variety of information security research topics. A PhD degree often appears to be a long lonely road. So why are people doing it? And what are the benefits? We spoke to Caroline Belrose, who completed her PhD in 2006, about life before – and after – a PhD.

Why did you choose to do a PhD?

Good question! I'm not someone who always wanted to do a PhD but I was always interested in cryptography, and after my MSc in Information Security, I worked for six months with HP Labs in Bristol. I ended up publishing a research paper with one of my HP colleagues and I got a real kick from that. So I started to consider the idea of doing a PhD. My main problem was funding, so when HP generously agreed to sponsor my PhD, I decided to go ahead with it.

Why did you choose to study with the ISG?

It is the largest and most well-known UK academic group working on information security. I think that's a good thing for students because it means that there is a wealth of experience to draw on and learn from. There is also more variety in the kind of research going on, which is inspirational and gives students more options.

Dare we ask what your PhD was about?

To provide a short answer I'll discuss my thesis, but a PhD is about far more than the thesis! The first part was about special kinds of signature schemes which involve multiple parties and where you can't determine who from a group of people actually produced the signature. The second part was about key agreement protocols, an area which seems pretty simple, but isn't. In both parts of the thesis I examined how to formulate good security models for the primitives I was working with, and also looked at how to prove that a given signature scheme or protocol was secure within these security models.

What are you doing now?

After completing my PhD, I was offered a job with Vodafone in their R&D security team and I took it because it offered a good balance between research and industry. I have a lot of variety in my role and a lot of interaction with all sorts of people both inside and outside of Vodafone, which I like. I am involved in managing the security requirements for the phones Vodafone purchases and sells on to customers; security work in industry for standards bodies; investigating new mobile security technologies for phones in the future, and a lot of other small things that crop up that require security expertise.

You could have pursued an academic career, why have you joined industry?

I realised during my PhD that I wouldn't be happy in academia. I enjoy working on problems and coming up with solutions but everyday academic work is seldom about that. It's also about lecturing, marking and reviewing, none of which particularly appealed to me. Academia offers you a great deal of freedom in what you study but a lot of academic research can be very far removed from current reality, and this became even clearer to me through my regular contact with HP. I wanted to work on things that people other than cryptographers felt was important and that mattered now (patience is not something I'm known for). So, although the world of industry did look a little scary from the safety of academia, I felt that I needed a change and a new challenge.

Are there any skills that you acquired during your PhD that are useful in your current role?

I learnt to question things and keep an open mind to new ideas. I learnt to reason about problems in order to develop logical solutions, and then to present my findings. And very importantly, I also learnt to trust my own abilities. I discovered that if you just sit down and give yourself the time to think things through properly, you can often come up with some surprising results. The thing is, most of us don't usually bother to try, or don't have the time, so we never really explore what we're capable of doing. A PhD gives you a unique opportunity to learn these skills, and they'll be useful wherever you go.

Any advice for anyone contemplating starting a PhD?

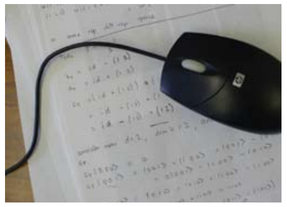
Firstly, I would say be honest with yourself about why you want to do it. If you like the sound of the title "Doctor", or you want to impress your friends, or you just don't know what to do next, then I would recommend finding something else. A PhD takes a lot of self motivation, and if your heart's not in it, you may not make it, and even if you do, you probably won't enjoy it. If you want to make loads of money, a PhD is unlikely to put you ahead either, because experience usually counts for more than academic qualifications. If, however, you have a genuine interest in your chosen topic, you enjoy the freedom of being able to explore your own ideas and you think you may want to go into academia or just experience what research is like for a few years, then go for it. I think a lot of people worry about not knowing exactly what they actually want to study, or that they don't know if they'll be able to come up with original new ideas. But these are things that you work out as you go along with the help of your supervisor and fellow students. To me, this is part of the PhD experience. I would also recommend speaking to someone who has completed a PhD to clarify any questions you may have. It's a three-year commitment, so be as informed as possible beforehand.

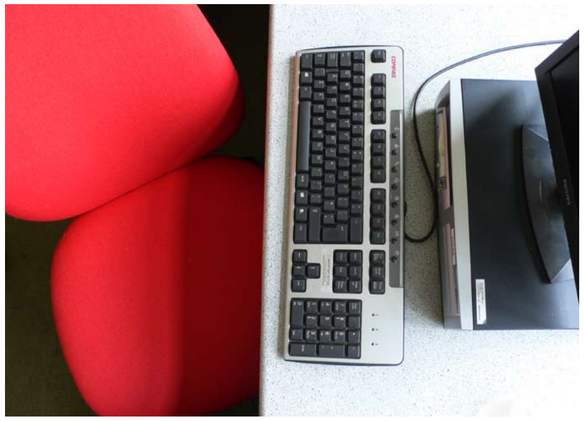
Is there life after a PhD?

There seems to be plenty of PhD graduates about who don't require Prozac to make it through the day, so there must be life after a PhD! I miss the "flexitime" of PhD life, but it's great to finally have that thesis done and dusted and not to have to think about it again (until someone starts asking you questions about it)!

RECENTLY COMPLETED PhD THESES...

Hoon Wei Lim, "On the application of identity-based cryptography in grid security"... **Andreas Pashalidis**, "Interdomain User Authentication and Privacy"... **Caroline Kudla**, "Special signature schemes and key agreement protocols"... **Su-Jeong Choi**, "Cryptanalysis of a Homomorphic Public-Key Cryptosystem"... **Anna Johnston**, "On the Difficulty of Prime Root Computation in Certain Finite Cyclic Groups"... **Adil Al Said**, "Enhancing End User Security - Attacks & Solutions"... **Eimear Gallery**, "Authorisation Issues for Mobile Code in Mobile Systems"... **William Sirett**, "Analysis, Implementation and Deployment of Behaviour-Based Temporally Aware Security in Smart Cards"... **Emmanuel Hooper**, "Intelligent Detection and Response Strategies for Network Infrastructure Attacks"...





A MATTER OF TRUST

Since late 2003, the ISG has developed a major research interest in trusted computing. This technology has the potential to have a major impact on the provision of security for PCs (as well as servers, PDAs, mobile phones, etc.), and all PCs produced by major vendors such as IBM and HP now come equipped with a Trusted Platform Module (TPM) chip, capable of a range of security functions. The potential for using this hardware presents both academia and the security industry with a major research challenge.

Our interest in this subject initially resulted in a public workshop on trusted computing held at Royal Holloway in March 2004, which had an attendance of around 100. The talks from this conference were then written up to form an edited book on trusted computing, published by the IEE in 2005, *Trusted Computing*. Since then, our involvement in the work has grown, and we are now working on two major funded research projects in the area of trusted computing, involving five members of staff (Andreas Fuchsberger, Scarlet Schwiderski-Grosche, Allan Tomlinson and Chris Mitchell) and three post-doctoral research assistants (Eimear Gallery, Stephane Lo Presti and Po-Wah Yau).

OPEN TRUSTED COMPUTING

The first project, Open Trusted Computing (OpenTC), is a large European collaborative project, with around 25 partners, which started in late 2005 and is due to end in 2009 (see www.opentc.org).

This project is primarily concerned with the development of trusted and secure computing systems based on open source software. The project targets traditional computer platforms as well as embedded systems such as mobile phones. The main involvement of the ISG is in investigating the possible uses of this technology in mobile platforms, and also in developing training material (a new MSc course on Trusted Computing has been developed as part of the project).

UK E-SCIENCE PROGRAMME

A second project with a major trusted computing element has been funded by the EPSRC as part of the UK e-science programme. The project started in 2006 and will run to 2009, and is concerned with using trusted computing technology on mobile platforms to enhance the security of the grid.

For more information, contact c.mitchell@rhul.ac.uk.

PHD STUDENT WINS RESEARCH SCHOLARSHIP FROM MICROSOFT

A PhD student with the ISG has been granted a scholarship from Microsoft Research in recognition of his potential to make an outstanding contribution to computing and science.

Aryeh Rowe, who is researching access control in open distributed computer systems, is being co-supervised by Jason Crampton (ISG) and Andy Gordon of Microsoft Research (Cambridge). Amongst his current research interests are Workflow Management Systems, particularly focusing on the area of scaleability in constraint specification schemes. In 2006, he obtained a First Class honours degree in Mathematics and Physics at Royal Holloway.

Only 22 awards were granted this year, going to students from Austria, Germany, Greece, the Netherlands, Portugal, Serbia, Spain, Sweden and the UK. The awards are part of the Microsoft Research European PhD Scholarship Programme, which is aimed at recognising and supporting exceptional students. Dr Fabien Petitcolas, who is responsible for the programme at Microsoft Research's labs in Cambridge, said: "Microsoft Research is very pleased to be able to assist scientists of tomorrow and would like to congratulate Aryeh on his success. Supporting Aryeh in his research is an example of how we can enable Europe to continue its heritage of pioneering science-based innovation."

MSC GRADUATE PROFILE
BY DUNCAN HART

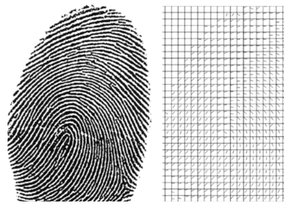
Since graduating from Royal Holloway in 2002, I have had the opportunity to work in information security for a large regional UK police force; a multinational defence and security specialist (with major programmes for MoD and HMG), and most recently, the unique challenge of being a Resident Twinning Advisor to another EU member state in order to develop their national capability in information security.

Taking on the challenge of being a trusted advisor to another country presents unique responsibilities and challenges, which often involve partaking in some high level and very weighty national or EU debates. I therefore often find myself acting as diplomat, politician and confidante, as well as my more natural role as an information security specialist. While sleep is a luxury and I sit on too many airplanes, I have absolutely relished the challenge of such a unique project, as well as the ups and downs of living and working in a new country.

For me, the Royal Holloway MSc has opened doors to a fascinating international career in information security, of which I could not previously have dreamt. It has provided the flexibility to adapt to new security technologies, to comprehend their strengths and weaknesses and, maybe most importantly, to tackle the security management problems that accompany technological implementations.

Although I am located a long distance from Royal Holloway, wherever I go in Europe and the Middle East, I am always bumping into alumni or current students of the MSc in Information Security. What binds us all together is our very strong affinity with the Information Security Group. In my opinion, the strength and depth of the ISG's reputation makes Royal Holloway quite unique and I feel proud to be part of one of the world's most prominent research and teaching centres for information security.

The ISG is currently updating its alumni database. If you know you have new details and would like to be kept up-to-date with ISG news, please email isg-secretary@rhul.ac.uk with "Alumni" in the subject line.



AUTHENTICATION AND IDENTITY MANAGEMENT

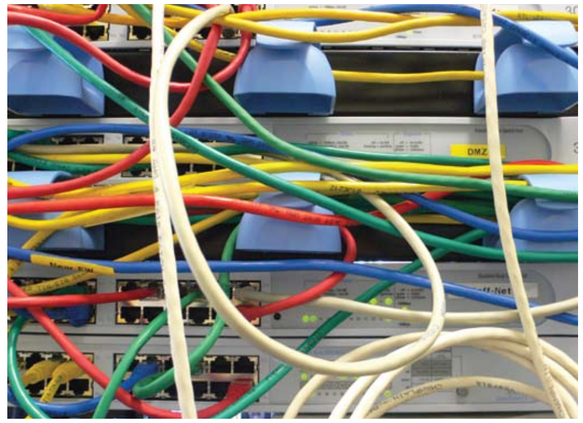
The Authentication and Identity Management (AIM) Club is an industrial forum hosted by the ISG and focused on issues concerning authentication and identity management. The AIM club evolved from a previous forum on PKI (Public Key Infrastructure), during which it emerged that practitioners predominantly use PKIs to provide authentication services.

At each meeting, an expert leads a discussion topic, which is then debated by those present in a "closed doors" environment that allows frank and insightful exchanges.

Recent meetings have covered topics such as the new UK passport, the UK ID Card, the evolution of online identity theft, and technical, economical and social aspects of biometrics. A number of common themes have emerged from discussions so far:

- Registration (identification and enrolment) is seen as a key aspect of any identity management infrastructure
- Managing access to stored data is crucial to the security of the resulting infrastructure. It can also be very difficult, depending on the size of the data set and what the data is to be used for
- There is very little current consensus on what is required as a template for an identity management scheme
- Liability is a vital issue
- Technical issues predominantly concern compatibility and standardisation, as well as biometrics

For more information, please contact geraint.price@rhul.ac.uk.



SECURE SOFTWARE

The ISG has recently launched a new MSc module on Software Security, which is being led by Andreas Fuchsberger. This module builds on recent commercial initiatives that have highlighted the need for a more methodical approach to writing secure code. Development for this module was partially supported by a grant from Microsoft Research, as part of their general campaign to raise awareness of software security issues.

As well as identifying the various programming practices of the past that have led to security vulnerabilities, the course covers techniques for attempting to improve the security of software development. In particular, the support provided to programmers by both Java Technology and the .NET Framework feature as major case studies. As well as formal lectures, this module provides a valuable opportunity for students to have "hands on" sessions in the newly-fitted Tolansky computer laboratory.

NEWS IN BRIEF:

- **The ISG is delivering two modules on information governance for an undergraduate degree programme on Biomedical Informatics in conjunction with St George's Hospital and Kingston University.**
- **As in previous years, the David Lindsay Memorial Prize was awarded by the BCS Information Security Specialist Group at the ISG's Hewlett-Packard Colloquium in December 2006. The winner of the award was David Hawks for his dissertation: "An Investigation into the Information Security Threats faced by a Small Network".**
- **The ISG hosted a workshop on current and emerging research issues in computer security (CERICS) in July 2006, which included invited talks from Andy Gordon (Microsoft Research), Elisa Bertino (Purdue), Dieter Gollman (Hamburg) and Kai Rannenberg (Frankfurt).**
- **The ISG Smart Card Centre is hosting CARDIS 2008, the foremost international conference dedicated to smart card research and application. The SCC is also co-organiser of the Workshop on Smart Cards, Mobile and Ubiquitous Computing Systems in Heraklion, Crete, 9-11th May, 2007.**