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
Tel: +44 (0)1784 443093
Fax: +44 (0)1784 430766
Email: isg-secretary@rhul.ac.uk
Web: 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
Tel: +44 (0)1784 443101
Email: p.stoner@rhul.ac.uk

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.
Mixed mode study: One graduation, three ways to travel there
News in Brief

**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 Sobral 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 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 modes” 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.”

**Blended 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 clearly 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 100 registered students studying the programme from around the world.)

This vision, which is often referred to as “mixed mode”, allows students to pick and choose between day-release campus attendance, block mode and distance study, as they assemble the modules necessary to obtain their degrees. 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”. 
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 formal or structure. Industry leaders were self-trained and many individuals had the label of IS specialist, whenever 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 MISc 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 exponential increase in the number of viruses, trojans and other high profile security breaches.

As the number of security specialists increased, discussions about the depth of information security research and 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 accepting 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 2008 and has attracted much interest. Well over 1000 individuals have joined as associate members. It has the support of more than 40 corporations and government departments.

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

In addition, IISP is 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 MISc 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.iisp.org.

COMMMENT: THE TIMELY EMERGENCE OF IISP BY PROF. FRED PIPER

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 uncracked codes and ciphers? His publishers, Orion Books, had acquired a World War II Enigma machine, with around $39,000, and intended to give it to the first person to solve the puzzles.

Carlos Cot, Laurence O’Hare and Kenny Paterson, who all have professional and personal interest in ciphers and cipher machines, began brainstorming 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 puzzle-solvers attempting to crack the ciphers. This suggested that a certain amount of interest in cracking 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 cryptography.

As is so 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, risks 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 ciphers 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.iisp.org.uk/engima.

STAFF PROFILE: STEPHEN WOLTHUSEN

Dr Stephen Wolthusen became our newest member of staff last year when he joined the Information Security Group in 2008.

Broadly, what are your research interests? My current research interests fall into two main categories. One is the modelling and simulation of complex infrastructures and their interdependencies. The second is network security; particularly the design and implementation of defence mechanisms against security threats.

By what route did you discover information security as a research discipline? I specialised 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 very clearly aware of the limitations of both government-directed research and collaborations with industry, but on balance find that close collaboration with industry 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 in 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 researchers.

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 these themes from the day I started are still as true today as ever and are more pronounced than they were. However, the support of more than 40 corporates and government departments, why is that? I see one of the key challenges facing the ISG as it comes to mind.

What do you think the big research challenges are at the moment? I see one of the key challenges facing the ISG as it comes to mind.

What's the best single thing about living in the UK? For me, the best single thing about living in the UK is the fact that the ISG is a very collegiate environment makes this not just exciting, but enjoyable.

What do you enjoy 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 collegiate environment makes this not just exciting, but enjoyable.
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)

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 as 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.

Lizette Cole-Kamp from the ISG is one of the researchers participating in the project. Lizette has recently joined the ISG, having previously been employed in a consulting role, and her wide research interests include risk assessment and organization 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.”

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

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

Last year on September 13th, 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 more about some of the latest developments in smart card technology and industry research, both emerging 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 Pino Paradiso from CNAM-Cedric, Paris, on measuring the performance of the Java CardFPM platform.

The 4th Smart Card Centre Open Day will be held on September 10th 2007. The format will remain similar to previous years and as all interested in smart card security are advised to get 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.isg.rhul.ac.uk or email both.lody@rhul.ac.uk.

Professional Training

• Bespoke specialist security training
• Postgraduate Diploma in Information Security
  (in partnership with QCC Information Security Training)
SECRETING 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 (there is no hope for security in 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.

MobiDo: consortium

In 2006, the ISG joined a consortium of around 25 organisations to bid for part UK Ministry of Defence, United States Defence Department Defence 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, entitled “International Technology Alliance” (ITA) programme. The programme was officially launched in September 2006. The ITA project will run for five years in the first instance, with a possible extension for a second five-year period. The ISG’s funding under ITA FAPMD is some £1.5 million over 10 years.

The project spans four interconnected research 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 cycle times 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 Wolfewson. Funds from the programme are being used by the ISG to employ Shane Balle as a research assistent 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 other universities.

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 pre-load sensors with all the key material that they will need to work from that point forward. What is the most effective means of pre-distributing key 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 by the project in order to assist in finding out.

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

WAS SOPHIE NEVER 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 both 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 on Channel 4 News for comments following the revelation that the judge in the case was working with, and also looked into and learned from. There is also more information security press on the subject of cryptography, an area which seems to be of great interest to national security. I think that’s a good thing for students because it means that there is a wealth of experience to drawn on and learn from. There is also some 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 final 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 protocols I was working with, and also looked at how to prove that a given signature scheme or protocol is secure within these security models.

What are you doing now?

After completing my PhD, I was offered a job with Vocalise 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 my research in cryptography, and after my PhD I moved into 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 do you choose to study with the ISG?

The ISG 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 drawn 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 final 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 protocols I was working with, and also looked at how to prove that a given signature scheme or protocol is secure within these security models.

What are you doing now?

After completing my PhD, I was offered a job with Vocalise 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 my research in cryptography, and after my PhD I moved into 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 do you choose to study with the ISG?

The ISG 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 drawn 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 final 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 protocols I was working with, and also looked at how to prove that a given signature scheme or protocol is secure within these security models.

What are you doing now?

After completing my PhD, I was offered a job with Vocalise 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 my research in cryptography, and after my PhD I moved into 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 do you choose to study with the ISG?

The ISG 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 drawn 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 final 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 protocols I was working with, and also looked at how to prove that a given signature scheme or protocol is secure within these security models.

What are you doing now?

After completing my PhD, I was offered a job with Vocalise 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 my research in cryptography, and after my PhD I moved into 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 do you choose to study with the ISG?

The ISG 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 drawn on and learn from. There is also more variety in the kind of research going on, which is inspirational and gives students more options.
Tolansky computer laboratory.

A MATTTER 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 to use 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 published in a book on trusted computing, published by the IEE. The workshop was followed by a series of conferences, workshops and research projects at ISG.

The first project, Open Trusted Computing (OTC), is a large European collaborative project, with around 25 partners, which started in late 2004 and is due to end in 2008 (see www.opengroup.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 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).

The project has led to a series of publications and the development of a range of tools and components for trusted computing, as well as the development of training material. The project has also resulted in a number of collaborations with other projects and with industry, particularly focusing on the area of mobile platforms.

The potential for using this hardware presents both academia and the security industry with a major research challenge.

The potential for using this hardware presents both academia and the security industry with a major research challenge.