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 443076
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

Royal Holloway’s location is on the A30 between the village of Englefield Green and the town of Egham. It is just 16 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.
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 Sobralt 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 the popular degree programme in 1992 and has now seen over 1,000 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 first offered for three of the core MSc modules and for the first time in the 2006-07 study year. Block mode teaching was offered for 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.”

Wiedenmayer 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 fulfill 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”, 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 degree. It is widely anticipated that there will be a high demand for mixed mode study. MSc Programme Director, Chris Cechinanosvci is certainly convinced: “This type of blended learning is undoubtedly the way of the future for information security education.”
is in his third year of the programme and exchange notes and plan their new study. However, more than anything, participants

machines by Carlos Cid. Misuse Act by Owen Brady of the FSA; an
corresponded online. Attendees enjoyed
Latvia and the U.A.E., to meet one another. MSc in Information Security, arriving from
the opportunity for around
Royal Holloway on the weekend of the
Security Summer School was held at
The second Distance Learning Information
SCHOOL
MEET AT SUMMER
DISTANCE STUDENTS

interest. Well over 1000 individuals
have joined as associate security professionals with the support of more than 40 corporations 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 profession 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, the 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 the 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 the IISP should imply that an 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 and experience to acquire further skills and competencies and to become leaders of the profession.

For more information, www.iisp.org.
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)

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.

Lizzie Cole-Kamp 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 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 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 Psychology, 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.

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 more about 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 that the Open Day offered. Visitors to the exhibition provided an opportunity for students in a friendly academic environment.

The 4th Smart Card Centre Open Day will be held on September 10th 2007. The format will remain similar to previous years and so interested visitors 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 keith.mayes@rhul.ac.uk.
They are small, potentially fragile, have low computing power, limited memory and you may not even know exactly where you have deployed them or there may be 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.

**DubDol consortium**

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

The ISG-led consortium successfully won one of the “International Technology Alliance” (ITA) programme, which 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 will be in excess of £1 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 coalition forces 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 high-velocity 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 Wolfmann. Funds from the programme are being used by the ISG to employ Shone Balle as a research assistant and fund a PhD student, as well as to establish collaborative research with staff at the ISG at Royal Holloway, 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 go their own way without communication. So what is the most effective means of preloading 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 in order 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 Candace Bichon, who completed her PhD in 2003, about life before — and after — a PhD.

**Why do 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 what is the doing of 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?**

It is the largest and most well-known UK academic group working on information security. I think that’s a great thing for students because it means that there is a wealth of experience to draw on and learn from. There’s 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 protocols I was working with, and also looked at how to prove that a given 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’m 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 picked 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 isn’t about that. It’s about teaching, marking and re-marking, none of which particularly appealed to me. Academics 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 want to work on things that people other than cryptographers felt was important and the contact between research and practicality isn’t something I’m good at. 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 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 to present my findings with clarity and importance. I also learnt to find my own solutions. I discovered that if you just sit down and give yourself the time to think things through properly, you 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 what you want to do. If you like the sound of the title ‘Doctor’, then you want to impress your friends, and you’re 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 you’re not sure then it’s not something you’ll be able to try. It’s about deciding whether you want to go into academia or to industry, and what research is likely to be for you 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. In my case, it is this 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 who are looking to use their PhD skills to make it through the day, so there must be life after a PhD. The future of a PhD is likely to be great if finally to have that enthusiasm to write a PhD, but it’s got to be to have a genuine interest in the subject. I encourage you not to have to think about it again until someone starts asking you questions about it!

---

**RECENTLY COMPLETED PHD THESSES...**

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 HMRC), and most recently, the unique challenge of being a Resident Training 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 participating 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 am too busy to fly to 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 in information security 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 such technology presents.

Although I am located a long distance from Royal Holloway, whenever I go to Europe and the Middle East, I am always bumping into alumni or current members of the ISG in Information Security. What bonds 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 a uniquely special and unique place to partake in “closed doors” conferences, which is crucial to the security of the MSc in Information Security. It is for this reason that I am delighted to be able to write a few words about the ISG and the challenges that we face in the area of information security.

I therefore often find myself acting as a trusted advisor to another country and as such it is vital that we provide assurance to the ISG’s MSc in Information Security.

SECURE SOFTWARE

The ISG has recently launched a new MSc module on Software Security, which is being led by Andreas Fuchsbauer. The module builds on recent commercial and academic 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 mission 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 module explores techniques for attempting to improve the security of software development. In particular, the support provided to programmers by both Java Technology and the JET 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 Talend computer laboratory.

AUTENTICATION 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 using PKI 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 next UK passport, the UK i-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 used for.
• There is a 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 the implementation and social aspects of biometrics.

For more information, please contact gerrit.price@ucl.ac.uk.

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 Lindsey Memorial Prize was awarded by the BCS Information Security Specialist Group at the EOC/ Hancock Cupcake Competition in December 2006. The winner of the award was Daniel Hawk 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 Swann (Microsoft Research), Elisa Bertino (Purdue), Diet Gollman (Hamburg) and Kai Ramme (Frankfurt).

• The ISG Smart Card Centre is hosting CARDIS 2008, the foremost international conference dedicated to smart card research and applications. The ISG is also co-organiser of the Workshop on Smart Cards, Mobile and Ubiquitous Computing Systems in Heraklion, Crete, 9-11 May, 2007.