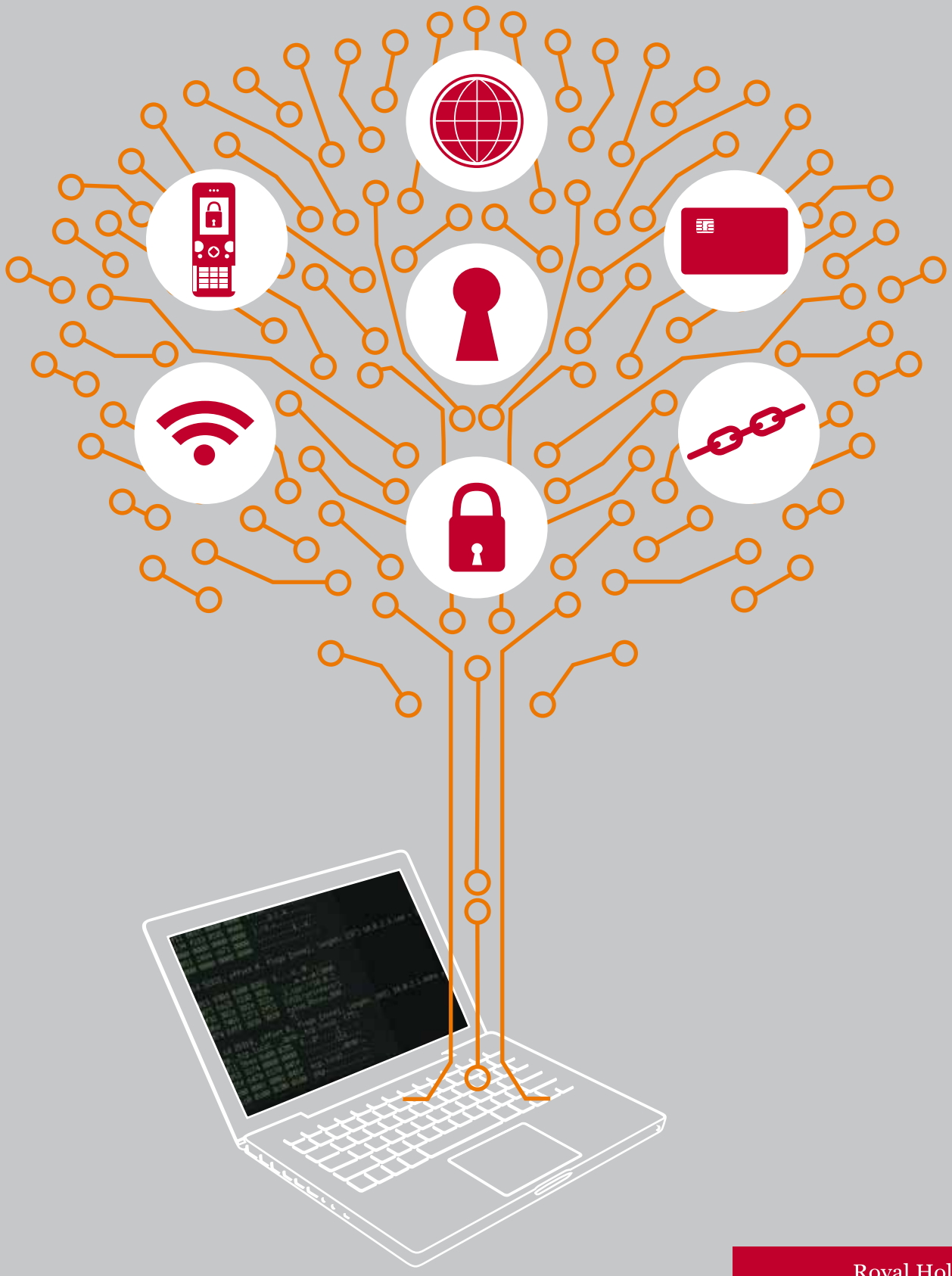
Information Security Group

Review 10/11



Royal Holloway
University of London

LETTER FROM THE ISG DIRECTOR

It is a pleasure to introduce this review of activities of the Information Security Group at Royal Holloway over the past year. I am always impressed by the range of different activities that we engage in and I hope that you will find plenty of interest in this newsletter.

From a personal perspective, the most significant change for me over the last year has been taking over the Directorship of the ISG from Peter Wild. I appreciate, even more than I did before, exactly what Peter did for the ISG during his six years in the post. The last year has also seen the retirement of Pauline Stoner, who for many people ``personified" the ISG, since she was the first point of contact for so many of our activities. I wish Peter and Pauline well in their future plans and am sure that we will still be seeing them both on a regular basis. However the past year has not all been about farewells a nd we have welcomed two new staff to the ISG, Dusko Pavlovic and Emma Mosley.

This year has seen some significant changes to our security training provision, including the launch of two new modules on the MSc Information Security, as well as an overhaul of our short course programme. We have also continued our external engagement initiatives, becoming the first academic partner of the Information Security Forum and an official sponsor of the Cyber Security Challenge. As always, the ISG has continued to produce excellent research across the information security spectrum, involving both academic and industrial partners. You can read more about some of these projects in this newsletter, which also features our first engagement with performance art, as well as some "comment" articles from two of the ISG's distinguished Visiting Professors: Paul Dorey and Richard Walton.

Next year will be the 20th anniversary of Royal Holloway's MSc in Information Security and so we are planning a celebratory party at the 2012 Alumni Conference, to be held from the 25th to the 27th of June 2012. We have included details of the 2010 event in this newsletter, just to whet the appetite for our own "London 2012" event.

As always, we are interested in connecting with anyone who wishes to learn more about the ISG and our activities. We are continuously seeking new partnerships and would be very interested in discussing opportunities wherever, and however, these might arise. Please do not hesitate to get in touch.

Prof. Keith Martin

INDEX

SHORT NEWS BITES:

ISG Visiting Professor Whitfield Diffie was a co-recipient of the prestigious IEEE Richard W. Hamming Medal for the invention of public-key cryptography and its application to secure communications.

Prof. Chris Mitchell has been honoured with an International Electrotechnical Commission (IEC) 1906 Award for his substantial contribution to international security standardisation work.

Dr Alex Dent contributed an online presentation entitled "Can Compliance Kill Security? The Case for Ignoring Standards" as part of the Information Systems Security Association (ISSA) web conference on Information Security Standards. His session examined ways in which an information security management system (ISMS) develops over time and the ways in which this development is supported/hindered by use of standards. Alex has prepared an article based on this presentation, which you can read on page 25.

Prof. Kenny Paterson discussed the unsolved Kryptos codes on BBC Radio 4's "The World Tonight" programme. In his interview, Kenny also mentioned Dan Brown's "Da Vinci Code" and its Royal Holloway connections, and where he gets his best research ideas...

Dr Lizzie Coles-Kemp, Dr Allan Tomlinson and Prof. Kenny Paterson each gave presentations at InfoSec Europe 2010, while Prof. Fred Piper was a member of the "professionalism panel" which discussed the role of information security professionals in organisations.

Rob Carolina (Senior Visiting Fellow) lectured on online safety at the London School of Economics on the 19th October 2010. You can view a podcast of his presentation (along with others in the same series) at: http://www.lse.ac.uk/resources/podcasts/publicLecturesAndEvents.htm

Dr Carlos Cid spoke about end-to-end encryption in the payment card industry at the first Financial Sector Technology Payments conference in London in November 2010.

Dr Keith Mayes has been invited to act as an expert evaluator for the Agence Nationale de Recherche for the programme Digital Engineering and Security 2011, which will shape future security research in France.

Prof. Keith Martin spent the spring semester of 2010 as a Visiting Erskine Fellow at the University of Canterbury in Christchurch, New Zealand. Both Keith and Prof. Chris Mitchell, who held this position in previous years, have been shocked by the recent earthquakes in Christchurch and have extended their best wishes to colleagues there.

Dr Jason Crampton is Programme Co-Chair of the ACM Symposium on Access Control Models and Technologies, to be held in Innsbruck, Austria in June 2011.

Prof. Kenny Paterson is Programme Chair of Eurocrypt 2011, to be held in May 2011 in Tallinn, Estonia.

In September 2010, the ISG hosted the Fifth European Trusted Infrastructure Summer School (ETISS 2010). The summer school was sponsored by HP Labs, Microsoft, Infineon and the Trusted Computing Group, and covered a variety of fields related to creating a trusted infrastructure to cope with the demands of current and future information processing. This included trusted computing, machine virtualization, new hardware architectures, and new network security architectures. The aim of the summer school was to provide a programme for both new and established researchers in the area. The summer school ran for one week and included a series of lecture from leading European and US researchers from both industry and academia. There were also a series of specialized workshops and practical sessions. Keynote speakers included Joanna Rutkowska from Invisible Things Labs and Ian White from CESG.

The ISG has become the first academic partner of the Information Security Forum (ISF), which is a member-based organisation dedicated to best practice in information security. We are involved in the ISF's Forward Work Programme, which conducts focussed research on topics selected by the membership. The ISF is also supporting a number of MSc projects on topics that contribute to this programme. The ISG is a sponsor of the ISF's 22nd Annual World Congress, which will take place from 16th-20th September 2011 in Berlin. From the ISG's perspective, becoming a member of the ISF is an excellent opportunity to continue the work that we engage in with our industrial partners.

PETER HEADS FOR THE SUN
By Chris Mitchell

> Prof. Chris Mitchell is Director of Graduate Studies for the ISG.

September 2010 marked the end of an era for the ISG with the retirement of Prof. Peter Wild. The arrival of Peter and Fred Piper at Royal Holloway in the mid-1980s saw the founding of the information security research group which became the ISG. After Fred retired back in 2004, Peter became the sole founding member of the group still working at Royal Holloway, and also its director and "father figure".

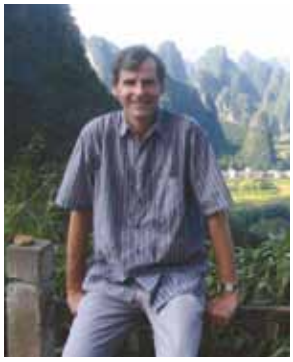
In the 26 years that he was at Royal Holloway, Peter played a key role in just about every significant development in the ISG. In the late 1980s, Peter and Fred founded what became a vitally important PhD research school, in which they jointly supervised a very large number of students. The graduates from this school have since gone on to take up positions of great importance in industry and academia. Indeed, four current ISG staff were supervised by Peter and Fred, namely Alex Dent, Keith Martin, Siaw-Lynn Ng and Kenny Paterson, not forgetting a former member of staff, Matt Robshaw, now working for Orange in France. This ensures that Peter's influence will live on after his retirement.

The early 1990s saw the introduction of the Information Security MSc, with Peter again playing a key role. I believe that Peter is the only person to have taught at least one MSc module every year since its inception in 1992 until 2010. He has also been in charge of MSc projects and the MSc examination process since the very beginning. This means that there is hardly an MSc graduate who has not come into contact with Peter. Indeed, it is hard to imagine that we could have ever run the MSc without Peter's involvement.

In 2004, to add to his many other tasks, Peter took over the role of ISG Director from Fred, and continued to play a critical role in the ISG's ongoing development and success. He worked very long hours in the service of the ISG, often almost invisibly to the rest of the group, taking on a huge proportion of the many mundane, but absolutely vital, jobs that have been necessary for the ISG's health, allowing the rest of us the time and space to take on more exciting tasks in research and teaching. We all owe him a huge debt for his selfless and uncomplaining service over the last six years.

Peter is, of course, a proud South Australian and graduate of the University of Adelaide. He first appeared on the UK academic scene in 1976, when he enrolled as a PhD student at Westfield College, University of London, under the supervision of Dan Hughes. Fred also played an important role in his supervision, as Dan spent a year away during Peter's PhD research. After graduating in 1979, Peter spent time as a post-doctoral researcher in Ohio, Adelaide, Sydney, Edinburgh, Rothamsted and Southampton, before taking up a lectureship at Royal Holloway in 1984. He became a professor in 1996. Since joining Royal Holloway he has made research visits to a wide range of institutions in Australia, the US, Switzerland, China, South Africa and Malaysia, among others.

We will all miss Peter a very great deal. I know I will greatly miss Peter as a close friend and colleague; we have known each other for 35 years, since we were PhD students together at the sadly long-defunct Westfield College in Hampstead. Worst of all, Peter has not been around during the recent Ashes series, so I have lost a rare opportunity for a gloat. Still, it's not so bad for him – no doubt he is going for a swim in the warm waters of Adelaide, just a few minutes from his home, even as you are reading this!



WELCOME TO EMMA

The ISG is very pleased to welcome Emma Mosley as the new ISG Administrator. Emma is an experienced academic administrator who was previously employed by London Metropolitan University. Emma started her position in January 2011 and has settled well into the role.

Emma commented on the challenges ahead: "I am looking forward to becoming part of the team at the Information Security Group and seeing the group continue to grow and develop. I am most looking forward to getting to know the students and academics, and ensuring a happy, productive and efficient environment for work and study.
I am also looking forward to building relationships with external contacts and alumni."

FAREWELL TO PAULINE: "FIRST LADY" OF THE ISG
By Fred Piper

> Prof. Fred Piper is the founder and former Director of the ISG. He is currently Director of External Relations.

In November 1991, the Mathematics Department advertised for a part-time secretary. Enter Pauline! I had no idea how important that appointment was to prove to be...

October 1992 saw the introduction of the MSc Information Security, which many people regard as the 'birth' of the ISG. At that time the ISG was nothing more than a loose collaboration between individuals in the Mathematics and Computer Science departments at Royal Holloway. After a few months Pauline's situation changed and she required full-time employment. She thus transferred to a full-time position in the Personnel Department, where she was PA to the Personnel Officer and Secretary to the Personnel Department. Soon after, I was asked to be Head of the Mathematics Department and was fortunate that the College and Pauline both agreed that she would return to the Mathematics Department as Departmental Secretary and my PA. Our 'partnership' lasted for more than 17 years, until she retired on Dec 31st 2010. As others might say, that's a long time for which I have worked for her!

During those 17 years the ISG grew dramatically and gained a certain amount of autonomy, with Pauline appointed as the dedicated Senior Administrator. Her influence on the smooth running of the ISG and the happy, relaxed atmosphere within it was immense. She soon became a focal point for students who wished to discuss their problems and this 'Aunty Pauline' role was crucial in helping to maintain the ISG's family atmosphere. At the same time, her efficient administrative skills meant that 'ask Pauline' became ISG members' stock answer to any difficult questions. On a recent visit to Singapore I had lunch with an alumnus. When I told him that Pauline would be leaving he was visibly upset. "I have never told you before", he said, "but I think I might have given up if Pauline had not been there".

He explained that he had never been away from his family before and was missing his wife and young children. He told me that, no matter how busy she was, Pauline always found the time to listen, talk, and look at his recent photos from home. As he said "these little things are very important for many overseas students".

With 'Academia and Industry in Harmony' as our motto, it is no surprise that networking events feature highly on the ISG agenda. HP days, Networking dinners, dinners for the new MSc intakes and, most recently, the important alumni conferences all need organising and liaison with attendees. Pauline played a central role in introducing and maintaining these events. She interacted in such a friendly and efficient way that when she retired, more than 60 of our industrial partners wrote short messages of thanks and good wishes which, together with the proceeds of a very generous collection, were presented to her at the HP Colloquium in December. Most of their comments to me referred to her as being a 'lovely lady' who will be missed. However the reaction of one particular industrialist is particularly informative. When told that she was retiring, he said "Fred, what on earth will you do? She's the glue that holds the place together. You'll collapse without her!" We will, of course, make sure that we do not 'collapse'. However we are losing someone who has been central to our activities for more than 17 years.

For the ISG, Pauline's retirement marks the end of an era. We are indebted to her and will miss her. No one in the ISG has relied on Pauline more than I have. She has been a reliable PA, friend and confidant who simplified my life dramatically. I owe her a lot.

RECENTLY COMPLETED PHD THESES...

Sriramkrishnan Srinivasan
New Security Notions for Identity Based Encryption

Gaven Watson
Provable Security in Practice: Analysis of SSH and CBC mode with Padding

James Birkett
On Plaintext-Aware Public-Key Encryption Schemes

Philip LENG
Lightweight RFID authentication protocols for special schemes

Martin Albrecht
Algorithmic Algebraic Techniques and their Application to Block Cipher Cryptanalysis

Waleed Alrodhan
Privacy and Practicality of Identity Management Systems

Carlo Gebhardt
Towards Trustworthy Virtualisation: Improving the Trusted Virtual Infrastructure

Liang Chen
Analyzing and Developing Role-Based Access Control Models

INFORMATION SECURITY SHORT COURSE TRAINING

Although the ISG is best known for its pioneering MSc Information Security programme, it is widely recognised that, for many individuals and organisations, the commitment required to engage with a full MSc programme is too great.

For this reason the ISG provides a range of specialist short training courses on information security. These are generally standalone courses that typically run over two days. The ISG's short course programme is operated in partnership with QCC Information Security.

Although the short courses are all offered individually and open for anyone to enrol to, they can also be accumulated in order to obtain one of two academic qualifications. The Postgraduate Certificate in Information Security is available for anyone who completes 15 days of short course training and submits three short essays. The Diploma in Information Security requires the further completion of a project dissertation supervised by a member of the ISG. Both of these qualifications are intended as a foundation for a professional career in information security.

The short courses run throughout the year at a venue close to the Royal Holloway campus. However, where there is specific demand, the short course programme can be offered on location at an external organisation. It can also be tailored to meet specific requirements and interests. In recent years dedicated programmes of this type have been delivered on the premises of a number of major financial and service organisations. The current suite of short courses is shown below. We are also willing to put together courses on specific topics, should there be sufficient demand.

Managing Information Security	3 days
Risk Assessment	2 days
Understanding Cryptography	2 days
ISO 1779/27001	2 days
Cyber Crime	2 days
Incident Response and Investigations	2 days
I.S. Law and Regulations	2 days
Identity Management	2 days
Physical Security and Technical Surveillance	1 day
Smartcard Security	2 days
Network Security	2 days
Wireless Security	2 days
System Security	2 days
Key Management and PKI	2 days
Applied Cryptography	2 days
Security Testing	2 days
Foundations of Digital Forensics	2 days
Advanced Digital Forensics	2 days
Human Centred Security	2 days

CASE STUDY: SHORT COURSE TRAINING IN LISBON

By Keith Martin

> Prof. Keith Martin is Director of the ISG.

An exciting recent development has been the establishment of a specific set of information security short courses which are run through Rumos, an educational training company based in Lisbon. Most of the students attending the short courses in Lisbon are also intending to complete the Diploma in Information Security.

The organisation and publicity of the courses has been managed by Carlos Figueira of Rumos. "Rumos is continuously looking for the best partnerships for training our Portuguese community of IT professionals. We already have partnerships with Microsoft and Cisco for security issues and with Security Certified Program for courseware, but we felt that there was still a lack of an academic approach to these subjects, so we started a worldwide hunt for the best postgraduate programs. This is how we discovered and became very interested in the modular postgraduate Certificate and Diploma from QCC and the ISG at Royal Holloway, University of London. The idea was to make possible the transfer of knowledge to Portuguese IT professionals from the members of a highly regarded research group, giving them the opportunity to have the same quality of educational experience in Portugal as they would have at Royal Holloway. We thus found the ideal flexibility that we required by partnering with QCC.
We are running two rounds of the courses per year in Lisbon with the same structure, syllabus, and documentation as the courses when they run in the UK. The Royal Holloway brand is now getting bigger amongst the Portuguese IT industry. Rumos is leading an extraordinary and distinctive offering on information security and Portuguese IT professionals now have an excellent opportunity to obtain the most advanced knowledge in these subjects."

John Austen, who represents both Royal Holloway and QCC, oversees the programme and is delighted with the new partnership. "In delivering the Certificate and Diploma in Information Security we have sought partners in other countries who can provide the necessary facilities and who are professional and enthusiastic for educational programmes.
In the autumn of 2009 we made contact with Rumos and started the first edition of these courses in February 2010. Rumos has a history of first class training provision and has purpose-built facilities in the centre of Lisbon. It was through the efforts of the staff at Rumos that the number of students attending the first edition exceeded expectations and was successful. In addition, it was clear that the educational standard of the students was high and that many of them had already completed other professional IT courses through Rumos. The second edition of the Certificate and Diploma was completed in February 2011 and again the standard of students and the facilities provided by Rumos were of the highest order. A third edition is planned in late Spring 2011, together with a number of other conference events. We look forward to continuing this educational partnership with such an excellent training provider."

Travelling to Lisbon to deliver a short course might sound like a pleasant couple of days, but it is certainly hard work and there is no time for sightseeing! There have also been several travel complications. I suffered severe delays during my first visit thanks to it coinciding with a NATO summit, which included the interesting experience of having my tiny TAP commuter aircraft taxiing down the Lisbon runway behind Air Force One. On another recent visit, Carlos Cid had to piece together an imaginative return route via Porto, Gatwick, and various delays on Southwest train platforms, after Heathrow closed during the winter snows. As compensation, the Rumos students are extremely engaging and the small restaurant next to Rumos serves exquisite fish lunches!

The partnership between QCC, the ISG and Rumos has been a highly successful one and we look forward to it continuing.

Rumos
Formação Profissional

DISTANCE LEARNING SUMMER SCHOOL
By Briony Williams

> Briony Williams is a final-year distance learning student on the MSc Information Security.

Every year, the ISG runs a weekend dedicated to students on the distance learning version of the MSc Information Security. I attended the most recent one, in September 2010, together with a small but select group of fellow students from a wide range of backgrounds and locations.

The weekend began with a visit to the Science Museum in London on the Friday afternoon, followed by a very convivial meal at a local restaurant, where we got to know one another in an informal setting.

The formal sessions began on Saturday morning, with a few words of welcome from Programme Director Colin Walter. Prof. Fred Piper then gave a lecture entitled "Information Security: What's it all about?" (one wonders why he was asking - after all, if Fred doesn't know the answer to that, then who does?) He made the very telling point that businesses exist to make money: they don't exist to be secure. He finished by considering the European Convention on Human Rights, which includes (in Article 8) the right to respect for a private and family life, and pointed out the exception made for reasons of "national security", posing the question: who decides? Provocatively, he suggested this could be interpreted as meaning that the Government can do whatever they want. There is clearly food for thought here.

In the remainder of the session Mairead Keaney (Tier-3 Pty Ltd) discussed SIEM (Security Information Event Management), which collates information from different log files from separate areas, and presents it graphically in one place. Ian McKinnon (Atos Consulting) spoke on "Broken cryptography - where the rubber meets the road". This was a close look at problems in the implementation of cryptography in the real world, especially in the domain of traffic speed cameras. Ian pointed out that simply using cryptography is not enough: it is vital to understand what the cryptography can and cannot achieve.

The first talk after lunch was by Williams Rann (BT Global Services), rather fearsomely entitled "Status Quo is not an Option". This discussed risks from the perspective of the Board, which primarily wants predictable results, whereas shareholders care more about relative risk/return performance. Jay George (NTS UK Ltd) reviewed "The role of visualisation systems in security operations". He pointed out that visualisation is about insight, not about making pictures. Since we don't always know what we're trying to find, data visualisation can throw up some surprising observations. Finally Stephen Wolthusen (ISG) gave a quick introduction to digital forensics, which was very illuminating, and discussed the place of the new digital forensics module within the MSc course. As a recruiting drive for potential students, it was most effective.

After a welcome caffeine infusion, Peter Wild (ISG) gave some useful advice to those about to embark on their MSc project. The talks continued with Sudarshan Ratnavelu (Smartlinx Networking) on "Social Engineering: Picking the low-hanging fruit". In this context, the low-hanging fruit comprised: helpdesk staff, receptionists, security guards, Chief Officers, admin assistants, staff, and..... you! The reason why social engineering is successful is because of certain human factors: cultural factors such as politeness, respect for authority, the desire to help someone in need; and also psychological factors such as fear, trust, and subconscious routines. Finally, Shadi Al-Abdul Razak (Roehampton University) gave an introduction to ISG Alumni, which has a number of chapters in several countries. Shadi encouraged all past and present MSc students to get involved – see www.isg-alumni.org for the London chapter. On Saturday evening, we all convened at a Reception followed by a dinner in Founders Building. Congratulations are due to Daniel Miller for his efficient organisation of the dinner and the whole weekend.

Sunday morning dawned bright and clear, with a first talk by Martin Warren (ISG) on the "Information Crime" module of the MSc. I found it fascinating, and have chosen this module as one of my options. Next was Terri Harwood (RIM) on "Protection and privacy - are they the same?". This was a detailed and highly knowledgeable journey through the morass of applicable laws in various countries. Mairtin O Sullivan (Espion) then discussed risk and monetary return on investment in the context of information security. Finally Mark Hanvey (Adviza Consultants Ltd) presented "Data access: Greed, larceny and murder". Despite the gory title, this was in fact a sober and professional overview of incident management and the role of a rapid response team.

After a break for lunch, Kenny Paterson (ISG) discussed "SSH: A case study of cryptography in theory and practice", which did exactly what it said on the tin. Kenny outlined a flaw in SSH v.2. He pointed out that SSH was meant to be bullet-proof but in fact attacks are simple, although may not have much practical relevance, which came as a relief. Emma Webb Hobson (QinetiQ), spoke on "Digital forensics for the cloud". The final speaker was Stephen Elgar (NHS) on "Studying for the MSc while working for the UK National Health Service". This talk began with some personal reflections from Stephen's own experience (such as: start writing the dissertation early), and set his studies in the context of the NHS.

The weekend drew to a close with some concluding remarks by Colin Walter, followed by yet another gathering for food and drink (coffee-time). At about 4pm, the students began to depart, and another stimulating and enjoyable ISG Distance Learning weekend had successfully completed.

I would recommend attendance at the next Distance Learning weekend for those who are able to do so. Although it is not a formal part of the academic programme, attendance at the weekend can help to lessen the feeling of isolation experienced by many DL students, as well as offering opportunities to meet the lecturers and tutors face-to-face. Some of the talks also offer valuable advice on completing the project, or an overview of specific optional modules, while other talks give a window into broader areas of Information Security. I have attended two of these weekends, and have found them both to be highly worthwhile occasions, which significantly enhance one's experience of the MSc programme as a whole.

ALUMNI REUNION CONFERENCE 2010
By Fred Piper

> Prof. Fred Piper is the founder and former Director of the ISG. He is currently Director of External Relations.

In July 2010 the ISG held the second of our Alumni Reunion Conferences. As for the inaugural event in 2008, the aims were to provide both an opportunity for our alumni to network and meet old friends and to provide a low cost, high-quality conference.

In order to minimise the cost to attendees we required sponsorship and it is a pleasure to thank BT/Check Point, KPMG, PGP, Royal Holloway Enterprise Ltd, Thales, Tier-3 and VISA for supporting the event so generously. Ray Stanton, (Executive Global Head, BT Business Continuity, Security & Governance Capability Unit) was one of the backers of the conference: “BT was delighted to act as sponsor for the Royal Holloway Alumni Conference in both 2008 and 2010 – we have very high regard for the work that Royal Holloway does in the Information Security arena, and we are proud to count a number of ISG alumni working in BT today. The conference gives us a great opportunity to cement our relationship with Royal Holloway members past and present and, more recently, to network with the potential future leaders of our industry”.

The conference was attended by more than 150 alumni. All the presentations, with the exception of the two keynotes, were delivered by the alumni themselves. For the keynotes we were delighted to welcome home Dieter Gollmann, who was a founding member of the ISG and who has maintained close links with both the ISG, as a visiting professor, and a number of ex-students. We were also very fortunate that our recently appointed visiting professor, Paul Dorey, agreed to deliver the other keynote. I attend numerous conferences, both commercial and academic, and am delighted to be able to say that the quality of talks at our alumni conferences compares favourably with any of them. Furthermore, the range of topics covered is amazing. The MSc graduates are the ‘product’ of the ISG and these conferences give us an excellent opportunity to ‘review’ that product. We are very proud of the results and it is our firm intention that this conference will become a regular, biennual event in our calendar.

Fortunately our enthusiasm is matched by the alumni themselves. In addition to the obvious social benefits, for many of them it provides a rare opportunity to present their work. Ian McKinnon (MSc 2006-2007) enjoyed the event, particularly “the excellent variety of information security topics covered, in beautiful surroundings and world class facilities, providing a great opportunity to catch up with my peers”. Ian also recognised the benefits that the conference provided in terms of public speaking: “this type of event is a fantastic opportunity for those who are relatively new to presenting to larger gatherings, as the audience are so supportive”. Paul Prebble (MSc 2004-2005) agrees and stated that he saw multiple benefits in taking part in the conference: “firstly, there is a good mixture of technical, research and management-focussed presentations; secondly, it’s an excellent opportunity to catch up with old friends and to make new ones; thirdly, it’s a wonderful opportunity to network and socialise in the surrounds of Royal Holloway’s beautiful campus”.

The next Alumni Reunion Conference will be from the 25th to the 27th June 2012. We look forward to seeing you there.

ROYAL HOLLOWAY, UNIVERSITY OF LONDON ISG ALUMNI REUNION CONFERENCE

> Programme 2010

MONDAY 5TH JULY 2010

09:00 – 10:00 Registration

> SESSION 1: SECURITY EDUCATION

10:00 – 10:10
Fred PIPER (RHUL): Opening remarks

10:10 – 10:20
Chez CIECHANOWICZ (RHUL): The RHUL Information Security Masters Degree

10:20 – 10.45
Taewan PARK (JS Security): You Can't Teach an Old Dog New Tricks! Really? – The case of Korea

10:45 – 11:10
Zoheir IFTIKHAR (Deloitte): A Quick Introduction to the ISG London Alumni Chapter

Morning coffee 11:10 – 11:40

> SESSION 2: CRYPTOGRAPHIC APPLICATIONS

11:40 – 12:10
Ian MCKINNON (Atos Consulting): Broken Cryptography – where the rubber meets the road

12:10 – 12:35
Dimitrios PATSOS (Adacom S.A./VeriSign Affiliate): National PKI: Open Issues and Lessons Learned

12.35 – 13:00
Frederik MENNES (VASCO Data Security): Trends in Strong Authentication for On-line Banking

Lunch 13:00 – 14:00

> SESSION 3: SOFTWARE SECURITY

14:00 – 14:25
Mark BATTERSBY (Omegapoint): OWASP – Software Security

14:25 – 14.50
Andrew LEE-THORP: The State of Trusted Computing: a Primer, Challenges and Potential Solutions

14:50 – 15:15
Vishal GARG (First Base Technologies): Applications & Software Security

15:15 – 15:45 Afternoon tea

SESSION 4: Security Management (15:45 – 17:00)

15:45 – 16:10
Jim HEARD (Centrica): Security is Dead, Long Live Risk! – Deploying an Integrated Risk Framework within a Leading Multinational Energy Company

16:10 – 16:35
Daniel ACCIOLY ROSA (Accenture Australia): Do we really have that many secrets? When Security gets in the way of doing Business

16:35 – 17:00
Paul PREBBLE (Research In Motion): Whatever Happened to Integrity?

Short break: 17:00 – 17:30

SESSION 5: INVITED SPEAKER

16:35 – 17:00
Professor Dieter GOLLMANN (TU Hamburg-Harburg): Security is Moving to the Application Layer

Evening meal: 19:30 Picture Gallery

TUESDAY 6TH JULY 2010

> SESSION 6: CERTIFICATION AND ASSURANCE

09:30 – 09:55
Paul MARCH (Elethian): PCI 2.0: Better or Just Longer?

09:55 – 10:20
Bhavin DESAI (Diamond Security Consultancy): Insights into Common Criteria Certification

10:20 – 10:45
Jeff TUTTON (Intersec Worldwide): Maintaining & Sustaining PCI Compliance (BAU)

10:45 – 11:10
David Kerry DAVIES (KPMG): Cost-Effective 3rd Party Assurance

Morning coffee: 11:00 – 11:10

> SESSION 7: ATTACKS AND PENETRATION TESTING

11:40 – 12:10
Filip SCHEPERS (IBM): Click Here to Get Infected

12:10 – 12:35
Benedict ADDIS (HP Labs): Underground Forums: An Eco-System For E-Crime

12:35 – 13:00
Erik THORMODSRUD (Ernst & Young): Attack & Penetration Testing – a Business Risk Based Approach

Lunch: 13:00 – 14:00

> SESSION 8: STRATEGIC ASPECTS OF SECURITY

14:00 – 14:25
Jane CHAPPELL (Royal Signals, Territorial Army): The Land Information Assurance Group

14:25 – 14:50
Felix BEATTY (FHC): Japan: Information Security Tsumami

14:50 – 15:15
Stephan FREEMAN (London School of Economics & Political Science): Social Networking

Afternoon tea: 15:15 – 15:45

> SESSION 9: SMART CARDS AND RISK MODELS

15:45 – 16:10
Jon HART (RHUL): Website Credential Storage & Two-Factor Web Authentication with a Java SIM

16:10 – 16:35
Kostas MARKANTONAKIS (RHUL): Smart Card Security Revisited

16:35 – 17:00
Neil HARE-BROWN (QCC Information Security): Contextual Risk Models

Short break: 17:00 – 17:30

> SESSION 10: INVITED SPEAKER

17:30 – 18:30
Professor Paul DOREY (CSO Confidential): 20:20 Vision. What you need to know now about information security in the next decade

Evening meal: 19:30 Picture Gallery

WEDNESDAY 7TH JULY 2010

> SESSION 11: PRIVACY AND HUMAN FACTORS

09:45 – 10:10
Aireni OMERRI: When Elephants Fight, the Grass Gets Trampled- the Hindrance of Aid in Developing a National Security Strategy

10:10 – 10:35
Lizzie COLES-KEMP (RHUL): Privacy: Dialogues and Dilemmas

10:35 – 11:00
Karen Lawrence ÖQVIST (Hewlett-Packard): Identity, Reputation & Privacy in the Organisational Context

Morning coffee: 11:00 – 11:30

> SESSION 12: SECURITY IN THE CLOUD

11:30 – 11:55
Piers WILSON (Adviza Consultants): Cloud Computing – Security, Continuity & Assurance

11:55 – 12:20:
Stephen KHAN: (GlaxoSmithKline): Cloud Security – Risk Management Considerations for an Enterprise

12:20-12:45
Emma WEBB HOBSON (QinetiQ): Digital Forensics in the Cloud

12:45 – 13:00
Chez CIECHANOWICZ (RHUL): Closing remarks

Lunch: 13:00 – 14:00

RISK MANAGEMENT FOR INFORMATION SECURITY

By Richard Walton

> Richard Walton is a Visiting Professor at Royal Holloway and a former Director of CESG.

Risk Management (RM) is now established as an important tool of corporate governance in both the private and public sectors. Large companies or Government departments commonly maintain a Risk Register which is regularly updated and presented to the Board. In many cases this is not only a case of following good practice but a regulatory requirement. Generally the risks managed have been concerned with regulatory or legal requirements, losses from natural disasters, health and safety or protection of high value assets. In recent years RM has been extended to cover the information security[1] (IS) domain. This is due to increased exposure and a string of incidents in both the public and private sectors which have shown that risks in this area can neither be avoided nor treated by simple means. However, although there is common agreement on the need for RM in IS, there are divergent ideas as to how to go about it. In this article I shall explain the concepts involved based on my recent experience as a consultant/researcher in the field and based on over 30 years in Governmental IS over a period when the main features of modern IS were evolved from the military/diplomatic discipline of Communications Security.

Many people would like a nice simple formulaic approach to RM – I think of this as a kind of unholy grail which I have spent much of my time resisting. However the appeal of a simple system of tick boxes with numerical scores that are then compared with a threshold and can be operated by unskilled personnel to produce 'the answer', remains strong. There are still those who yearn for such an approach, even though experience has clearly demonstrated that such an approach will never be satisfactory for real risks in the real world. Others have felt that it ought to be possible to lift some extant system (preferably based on some numerical model) used for other categories of risks (e.g. safety or insurance) and apply it with only minor modification to IS – in fact, anything to avoid the pain of what is actually needed: the engagement of hard thinking and analysis by experienced practitioners with a high order of intellectual capabilities. My bottom line is that RM, at least as applied to IS, is a job for expert analysis. Tools in the hands of experts can be useful, even numerical tools! But care must always be taken in applying them and in interpreting results. RM, although rational and scientific, is as much an art as a science and is definitely subjective (perhaps with the occasional island of objectivity).

RM is an aid to decision makers in order to enable them to take rational decisions about their business risks, and to enable such risks to be controlled as far as is possible. RM is all about minimising nasty surprises! In pure and simple terms, RM can be described algorithmically in the eleven steps outlined below. This 'algorithm' can be applied generally for RM and not only in IS, but the emphasis on various components will be influenced by the type of risk being considered.

01. Determine a Risk Appetite – just what risks are acceptable and what risks are not.
02. Scope the system to be addressed - what must be included and, more importantly, what is to be excluded.
03. Produce an Asset Register – with values.
04. List the potential negative Impacts from attacks on or failures of those assets (e.g. costs).
05. Determine the potential Threats (with likelihoods).
06. Determine the Vulnerabilities.
07. Hence compute the Risk of the impact occurring through a threat materialising (e.g. by successfully exploiting a vulnerability or causing collateral damage, whether successful or not).
08. Produce a Risk Register.
09. For each risk decide whether the Risk is Acceptable.
10. If not, look for Countermeasures to mitigate the Risk and iterate through the analysis.
11. Iterate until satisfied that the Risks are adequately addressed, if necessary also producing an Action Plan to implement any changes that have been decided.

However the real world is never pure and rarely simple, so in practice the above algorithm doesn't work very well on its own. Rather, it serves mainly as a guide /checklist for the experts.

I shall now consider the components in turn:

Risk appetite: this is much easier in theory than in practice. Firstly the risk appetite in any particular case is heavily influenced by the details of the risk concerned, which can lead to a rather circular argument and a tendency to fudge the issue. In a sense this is not unreasonable because risks do not exist in isolation, but are a balance between the risks from doing something and the risks from not doing it. Too often the situation can be seen as 'between a rock and a hard place' and the decision will be based on the perception of the least worst option rather than a view that the risk is acceptable in an abstract sense. Thus, in some cases, theoretically unacceptable risks will be taken by a rational decision maker. In any case the matter usually comes down to subjective judgement rather than objective evaluation.

Scope: it is very easy to get this wrong; on the one hand you can soon find yourself including the whole world within the scope of your system by following all possible connections; on the other hand you can draw the boundary too tightly and exclude many important sources of risk. The trick is to strike a pragmatic balance, keep an open mind for exceptional circumstances (with consequent loose boundaries) and be prepared to make adjustments for pragmatic reasons.

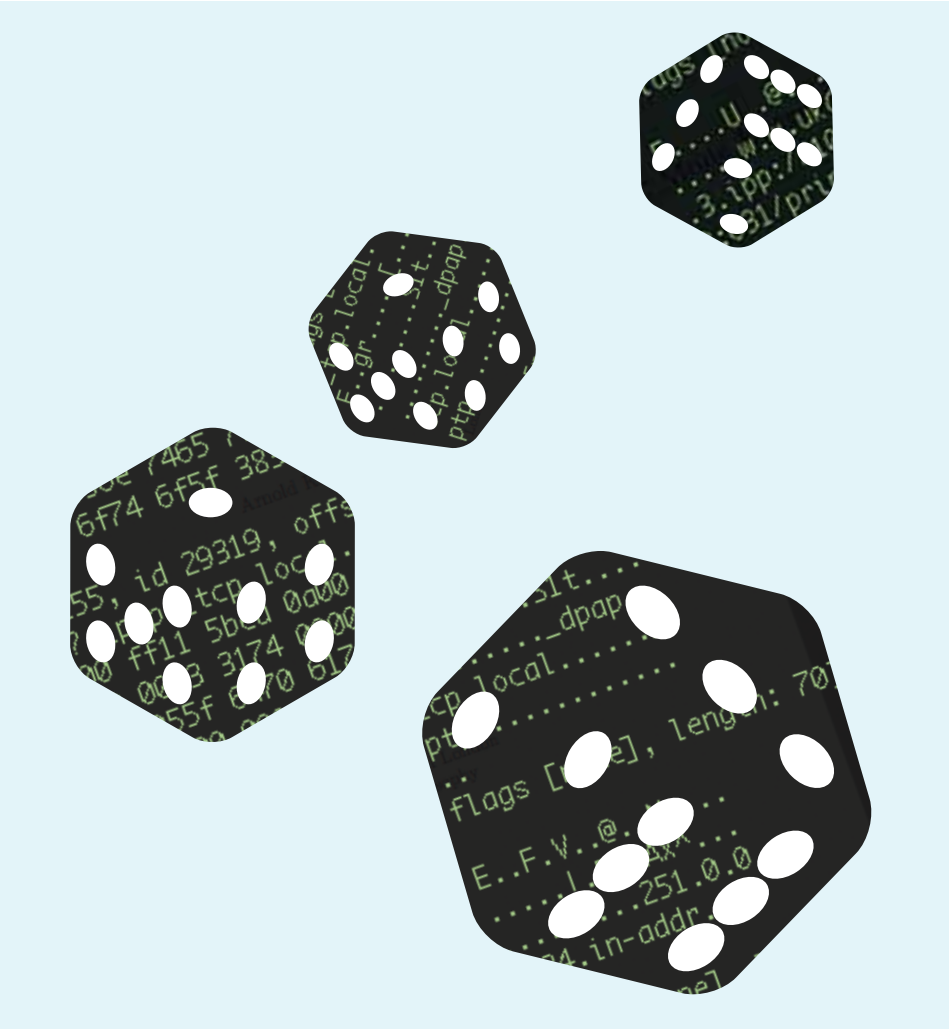
Asset register: it is important to maintain an asset register (in line with the scope) but by itself it is inadequate to serve as a guide to the potential impacts[2,3]. Risks will not only affect assets on your register but may also affect the world outside the scope of either your register or your system. Purists do try to fudge this by various artificial adjuncts to scope or assets but, frankly, these attempts are generally unsatisfactory. For example, in some cases attacks on your system could endanger the lives or property of third parties. The impact on you may be expressible in terms of your assets (reputation, freedom from jail, money for fines); but in reality the impact on the wider world is what is important. Unless we are willing to include far too much in the system scope or asset register, it is necessary to accept that the risks to be managed may need to be expressed in other terms.

Impact: in my view this is the key concept for managing risks, my starting point is to imagine those unwanted consequences that might occur through attacks or failures of the system or assets. This would include both deliberate attacks and natural events (such as fire, flood etc.) and should also include unwanted side effects. For example, a hacker might attempt a denial of service attack on an industrial process. The potential impact should not only include the obvious impact of the hacker succeeding and meeting his goals but also the potential for side effects (such as health and safety failures causing loss of life or injury) that might arise from the hacking attempt even if it fails. I find it helpful at this stage to come up with impact paths that describe the possible things that could go wrong – without yet considering who might bring about the event (or why) or whether there is any chance of success. Expressing the impacts on some kind of qualitative scale can help prioritise the later analysis. This stage is best conducted jointly by a mixed team. The expert really only offers experience here to help guide those with much more relevant domain knowledge of the system and its operations.

Threat: threat analysis really calls for expert input. The goal is to answer the questions: who will do what, with what, to what, and why? Of course, with natural events there isn't a motivated who, and the threat can be more easily determined. Having answered these questions there is usually an attempt to put a probability on each threat. Sometimes this can be done and can be useful (for example in the insurance industry) but more often it is impossible to measure probability sensibly and a vague qualitative scale is more

appropriate. Often it is useful to group potential threat agents into classes to bring together those with similar capability and motivation. It is important to consider all the questions because, when put together with later stages, it can be important to make distinctions since not all attackers are equal. In particular, when considering the effectiveness of countermeasures, the capability (knowledge and resources) and resolution of the attacker will be relevant. An ordinary hacker may have knowledge, but limited resources and only casual interest, and thus be deterred by relatively simple countermeasures, whereas a terrorist might be willing and able to put in considerable resources, be determined to succeed and willing to take significant personal or organisational risks. The level of countermeasures required to prevent or deter the terrorist is likely to be much greater than for the casual hacker, even when the vulnerabilities are the same.

Having come up with a suitable threat list I find it helpful to put this together with the impact list to produce a combined list of threat paths of the form this threat could cause this impact with this combined likelihood (this last being highly subjective and on a qualitative scale). There is a danger here of finding paths that essentially say there is almost zero chance of this threat (or set of threats) producing an effectively infinite impact (think explosions of nuclear power stations). This cannot be analysed quantitatively (0 times infinity can be anything you want).



Vulnerability: so far the threat paths do not take into account whether or not they are actually possible (but remember some threat agent may out of ignorance attempt the impossible and cause an impact through collateral damage). This stage examines the system or asset vulnerabilities that might enable a threat path to succeed. Again this tends to call for expert knowledge – especially where esoteric technical vulnerabilities are being considered. It is also necessary to exercise some caution because there will be unknown vulnerabilities and sometimes it will be sensible to conclude that an attack will stand a chance of success even though you don't know how.

Having done this (including estimates of probabilities of success or failure leading to particular impacts) it helps to merge this with the threat paths to come up with a first cut at genuine risk paths. This can be no more than a first cut because there will inevitably be mitigating (or exacerbating) factors – for example arising from specific system properties, environmental circumstances or existing defensive measures.

When all this has been completed, you have an effective **Risk Register**. It is now possible to consider each Risk on the register and decide whether to **accept** it or seek further treatment. Treatment can consist of some or all of:

a) adopting further technical or physical countermeasures to address a vulnerability, deterring a threat or improving the ability to respond and limit damage;
b) introducing extra procedures, usually for deterrence, improving detection or better response;
c) changing the system to reduce the risk (e.g. don't do some of the riskier activities);
d) managing expectations;
e) taking out insurance.

Usually, the last of these is not appropriate for an Information Security environment because the circumstances that might call for it are generally precisely those that have insurance companies reaching for their pens to write an exclusion clause. Decisions on risk treatment should take into account the effectiveness of the proposed treatment, the costs and affordability as well as the nature of the risk itself.

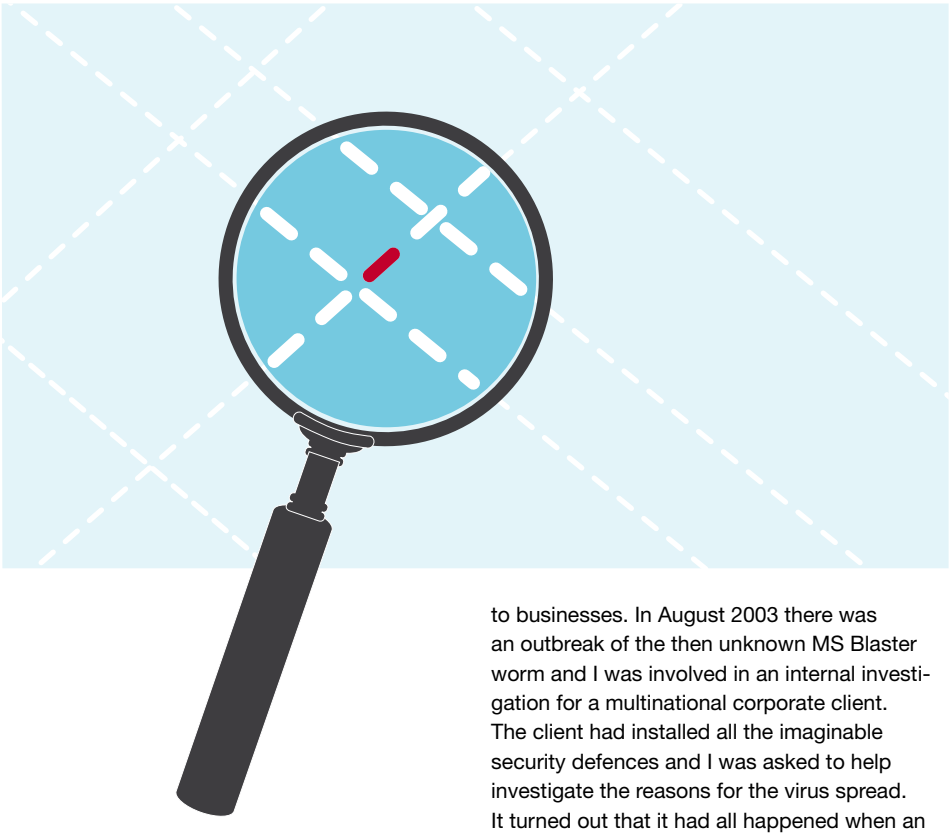
Having completed the above it is necessary to go back (iterate) to take account of any changes you have introduced – whether to the system, its scope, assets, vulnerabilities or countermeasures before signing off on the final risk register and any action plan called for by the analysis.

My conclusion to all this is that RM can be conducted through a framework as above but it requires the involvement of experts, operational personnel, and decision makers. The expertise includes the ability to think deeply and laterally, usually on a case-by-case basis. The process does not lend itself to automatic questionnaires or similar tick-box approaches, although automatic tools in the hands of experts can reduce routine workload. Similarly, numerical models are rarely adequate by themselves but can be useful to help the expert analysis when interpreted properly. Also, it is rare in the real world of IS for risks to be quantifiable in terms of probabilities or expected values.

1. I shall use the term 'information security' consistently throughout this article. Many authorities now prefer the term 'information assurance' (IA) which is more expressive of the concepts as they apply to business (both commercial and governmental). Everything in this article applies equally to IA.

2. In the simpler risk category of insurance of material property the asset and its value is all important and the impact is purely the loss of the monetary value of the property. Generally insurers try to map all their risks into such an impact (by having financial limits of liability) and when the going gets tough they get going.

3. With an exclusion clause. It is also often difficult to determine a monetary value for information assets.



HOW ROYAL HOLLOWAY AND THE MS BLASTER WORM CHANGED MY LIFE

By William Rothwell

> William Rothwell is Director of Abatis (UK) Ltd and a former ISG MSc student.

I am the MD of Abatis (UK) Limited, which is a security company specialising in proactive malware prevention and hacking intrusion protection. This is the story of how the association with Royal Holloway has changed my life. I had been working in the information security field for about ten years before studying the MSc Information Security at Royal Holloway in 1998. The course materials not only had helped me to consolidate my security understanding but I also learned a tremendous amount of new knowledge. I was delighted to graduate with a distinction degree.

Like many graduates, I then pursued my career in the information security sector. I was approached by a Swiss data encryption specialist company before finishing the course and have little doubt that the ISG reputation played a part. I took on the role of their Senior Security Architect. Armed with the knowledge gained from the MSc, I applied what I had learned in my work and the job satisfaction was most rewarding.

After a couple of years I moved on to be a senior security consultant and had opportunities to encounter different security challenges. One predominant issue was the virus threat to businesses. In August 2003 there was an outbreak of the then unknown MS Blaster worm and I was involved in an internal investigation for a multinational corporate client. The client had installed all the imaginable security defences and I was asked to help investigate the reasons for the virus spread. It turned out that it had all happened when an external contractor logged in to the corporate network with his previously infected notebook computer. This same story has undoubtedly repeated itself over and over again, before and after this event.

On the one hand I saw the business disruptions and potential damages caused by the MS Blaster; on the other hand I was surprised that a small piece of virus code could roam a corporate network, defeating detection by multiple layers of anti-virus and security protection tools worth millions of dollars. Driven by the desire to understand the cause of the virus spreading capability, I began the journey to research anti-virus technology and possible defence mechanisms that can address unknown viruses similar to the MS Blaster. It was apparent to me that viruses are plain computer programs created by people who are mischievous or have malicious intent. In other words, a virus is just another piece of computer executable, but one that performs actions as instructed by its creator (the virus writer), rather than to the benefit of the user. I was baffled as to why anti-virus protection, which is a technology that reached a state of relative maturity back in the early 2000s, was not effective in protecting against viruses. I then decided to research the problem domain as a personal endeavour.

I began by recalling an important lesson that I learned during my MSc studies, which I attribute particularly to Prof. Dieter Gollmann and Prof. Fred Piper - that we should understand not only the security symptom/cause but also the layer below. I thus came up with an almost naïve virus prevention approach that I called Hard Disk Firewall (HDF). The HDF concept is simple. From the perspective of a computer, business applications and viruses (malware – malicious software) are the same. They are all application programs and executable instructions; computers do not differentiate between "good" and "bad" applications. From a human's viewpoint, viruses (malware) are programs that we do not want to run on our systems. The solution is therefore obvious. We do not want unknown viruses and "bad" applications to enter into our computer. HDF's approach is to technically enforce the assertion of no unwanted application programs on the computer – it acts like a firewall to the system permanent storage, e.g. hard disk.

The next mental challenge was that while the HDF idea is simple, I was intrigued as to why there are no widely-available solutions that are based on this straightforward approach. Surely, the security industry must have thought of this simple strategy? Apparently they have not; or at least not publicised it for one reason or another. Having developed a prototype, which was validated technically by the Swiss military in the following months, on the back of HDF I founded the company Abatis and filed a patent application in 2005.

The ISG and Royal Holloway Enterprise Centre provided immense support for my commercialisation of the HDF idea, from establishing a presence in the UK market, through to access to investors and the provision of business skills training. Abatis finds itself in a supportive environment and is able to continue R&D with the mission to offer its customers a simple and, more importantly, effective security solution against unknown zero-day malware threats and hacking intrusion protection. HDF has been deployed on business critical systems by a number of household name corporate users with demonstrated successful results. A simple approach has been proven to be effective.

Like most of the ISG alumni, my good memories of the ISG and my MSc student days have stayed with me. From 2005, I offered my time and personal experience from an industrial perspective to assist some MSc students with their research projects. The feedback has been so positive that I am continuing to support the ISG in this way. My aspiration is for other students to contribute to the information security community, and perhaps to repeat a similar story to my own.

I want to close by commenting that the type of career journey that I have travelled is neither an obvious one nor an easy one. Only perseverance has taken me towards my own personal goals, and I am still soldiering on! Although the impact of the MS Blaster worm is fading away, my association with the ISG has not and I hope that it will continue long into the future.

THE ISG AND ECRYPT II
By Carlos Cid

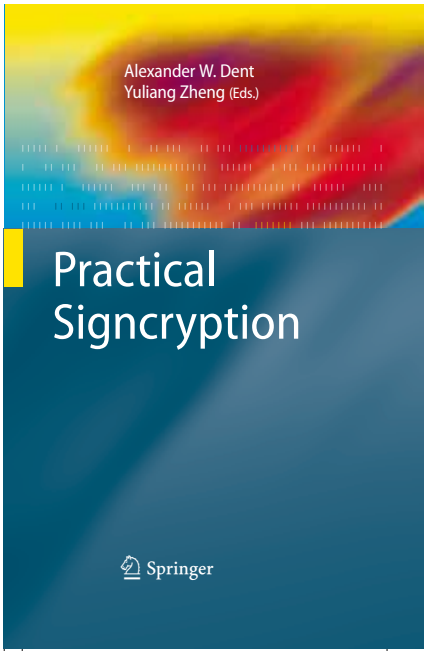
> Dr Carlos Cid is a Reader in the ISG.

Research in cryptology is one of the core activities of the ISG, and we have an extensive network of research collaborators in Europe and across the world. Besides collaboration with individual researchers, participation in research projects is fundamental for our research-active staff: such projects provide staff and students with the opportunity to work with groups having common interests (and complementary set of skills) on challenging research problems.
One of the largest and highest profile projects that the ISG is involved in is ECRYPT II, the European Network of Excellence in Cryptology.

ECRYPT II is a large research project funded under the FP7-IST programme, which officially started in August 2008. ECRYPT II is the successor of ECRYPT, which ran from February 2004 to June 2008. Currently in its third year, ECRYPT II is scheduled to end in mid-2012. ECRYPT II is a "network of excellence", connecting nine academic and two industrial partners (the original ECRYPT project contained 32 partners from 14 countries). The main objective is to ensure a durable integration of European cryptology research in both academia and industry, and to maintain and strengthen the European excellence in the field. Cryptography research in Europe has been traditionally somewhat fragmented, scattered over more than 100 organisations. ECRYPT II aims to provide durable integration of European research in cryptology, by supporting exchange of researchers among partners, facilitating joint publications, and sponsoring summer schools and workshops.

The Information Security Group is one of the ECRYPT II academic partners, and is actively involved in two of the Network's virtual labs: SymLab, which focuses on symmetric key algorithms, and MAYA, focusing on public key algorithms and protocols. 2010 was a particularly busy year: in late June we hosted the ECRYPT II Workshop on Tools for Cryptanalysis, a two-day event with over 60 participants (who were lucky enough to also enjoy an exceptionally sunny week by British standards). Kenny Paterson was an invited speaker at the School on Applied Cryptographic Protocols, held in late September in Mykonos, Greece. Our researchers were also active in ECRYPT II's input to standardization bodies and other dissemination activities, including contribution to one of ECRYPT II's most popular and referenced public reports: ECRYPT II Yearly Report on Algorithms and Key Lengths.

ECRYPT II will soon enter its final year.
In addition to targeted research within ECRYPT II's virtual labs, there are workshops and PhD summer schools scheduled in areas such as cloud computing and lightweight cryptography, as well as further collaboration with NIST on the SHA-3 competition. Over the past seven years ECRYPT has been fundamental in improving the state of the art in practice and theory of cryptology in Europe. Although it is unlikely that there will be an ECRYPT III after 2012, strong links have been created between researchers and institutions working on cryptography across Europe, and these should remain long after the end of the project. For the ISG, the experience has been a very positive one. We are certain that the close interaction with partners across Europe will continue to benefit our researchers and students, and strengthen Royal Holloway's position as a leading academic centre for research on cryptology.



PRACTICAL SIGNCRYPTION

Last year saw the publication of a new book called Practical Signcryption, co-edited and partly written by Alex Dent. The book aims to explain the different construction methods and security guarantees given by signcryption technologies, and their potential uses in practice.

Signcryption arises from the problems associated with combining cryptographic algorithms in a way that preserves the security properties of both algorithms. In particular, signcryption deals with the difficulty of combining confidentiality-preserving public-key encryption and integrity-protecting digital signatures. Practical Signcryption is not just about which methods for conducting signcryption can be realised, but also about the applications for which signcryption might be beneficial. Alex has contributed a chapter on using signcryption for the vitally important process of key establishment. The book also details a number of intriguing proposals for using signcryption to enhance the efficiency of security techniques to protect multicast networks, ATM networks, VoIP and routing for mobile ad-hoc networks.

The chapters of Practical Signcryption have all been contributed by expert signcryption researchers from around the world. Moti Yung (Google and Columbia University), one of the world's leading cryptographers, has described the book as a "handbook on the state of the art of signcryption", and "a fundamental and timely contribution to the cryptographic literature". If you want to learn more about signcryption then there is only one book to read!

I'D LIKE TO STUDY INFORMATION SECURITY – IF I KNEW WHAT IT WAS!

By Paul Dorey

> Paul Dorey is a Visiting Professor at Royal Holloway and currently runs two consultancy firms, following over 25 years of information security management experience at Morgan Grenfell / DeutscheBank, Barclays Bank and BP.

Recently I have been advising some students from a range of universities on the subjects to choose for their dissertations or, in one case, for potential doctorate studies. In nearly every example the students were proposing very wide areas of work themed as 'Information Security'. One proposal was to study 'human factors', another 'risks in mobile devices', a third 'cyber attacks'. These are all vast, or at least major, topics and generally use words that have unclear definitions. Take 'cyber attacks and cybersecurity' for example:

Definitions

Wikipedia[1] makes "Cybersecurity" synonymous with "Computer Security"; which it defines as ***"a branch of computer technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users."***

Interestingly, nobody in a corporate security job seems to call themselves a "Computer Security Manager" and most prefer "Information Security Manager", just as their colleagues are no longer called "Computer Systems Manager" or "Data Processing Manager" but instead adopt "Information Technology Manager" or even "Information Officer" (as in "Chief Information Officer", or CIO). Cynics might call this marketing and playing with words, but I believe that the name change did follow a better understanding that information is what is really being managed and technology is just the supporting tool.

So most people in our field consider that they work in, or study, "Information Security", and we show our alignment at Royal Holloway with our very own "Information Security Group" title. The industry's professional institute,[2] The Institute of Information Security Professionals, also follows this theme.

So does "information security" have a clearer definition? Most sources from over ten years ago would probably define information security as ***"Preservation of the confidentiality, integrity and availability of information"***, sometimes known as the "CIA triad".

Around 2002 Donn Parker expanded this into what is sometimes called the Parkerian Hexad[3] to also include Possession or Control, Authenticity (the veracity of the claim of origin or authorship of the information) and Utility (usefulness). Donn's point is that it is the inherent value of the information and its very purpose that we have to protect.

I also confess to placing a similarly wider definition into the security lexicon: ***"Information security provides the management processes, technology and assurance to allow businesses' management to ensure business transactions can be trusted; ensure IT services are usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and ensure critical confidential information is withheld from those who should not have access to it."*** [4]

You may question whether I should have included "error" and "disaster" in my definition because a security event is surely one where there is deliberate, malicious intent. In my defence, I will argue that security controls and countermeasures often also provide risk mitigation for some errors and disasters. However, true security management indeed has "bad guys" and deliberate attack at its core.

I am less apologetic that my definition does not confine information to just that residing on IT systems and thus covers physical paper and other information media. In terms of business goals this has to make sense. Senior managers furious over the consequences of a data loss incident are unlikely to listen long to a defence that "the systems are fine, it's just the stack of printed paper that went missing".

The Need For Breadth

The proliferation of information systems into our lives (such as social networking) and into the physical world of manufacturing, transport ("fly-by-wire" planes and cars) and industrial systems like refineries or electricity grids, also broadens the problem to give information security almost no boundaries.

And there we have one key message of my commentary. What matters in the delivery of information security is that the information is appropriately secured in all parts of its lifecycle, and looked after "end-to-end" in its communication. To have too narrow a scope – for example defining Information Security just as "protection against viruses" - allows the attacker to find another area of people, process or technology that has not got good security, and to exploit that instead. However, within organizations, different security specialisms may be located in different departments – the best people for physical security and protecting individuals may reside in corporate security, those protecting networks will report to the IT department, and those looking at industrial systems will be more likely to be engineers than IT people. "Convergence", or the better inter-working of these different security functions, has the goal of not having security gaps between teams and is currently a strong theme in the industry.[5]

So good information security is very wide indeed. It must take the broadest possible view of risk and ensure that everything has been considered. However, a superficial view will not work either.

The Need For Depth

A piece of software with a single byte code error, a gap in a fence, or lack of observation by a member of staff, are all sufficient to allow a security breach. It thus takes real depth of understanding and analysis to find and fix these problems. Good security is also designed in from the start. This means that there is a wealth of detailed security subjects for people to specialize in, or study.

We are still a relatively immature discipline but I believe that we have gone beyond the high-level study of the problem. To look at "Information Security in Companies" would be the same as proposing to study "Health in humans"; too broad and unfocused. To those looking at areas of study, I advise an initial broad high-level view to look at the risk landscape, and then pick a particular technology or business process to give clarity of focus on the area of study. There are many new challenges and continual stretch introduced by the pace of new technology adoption, so there are plenty of opportunities out there.

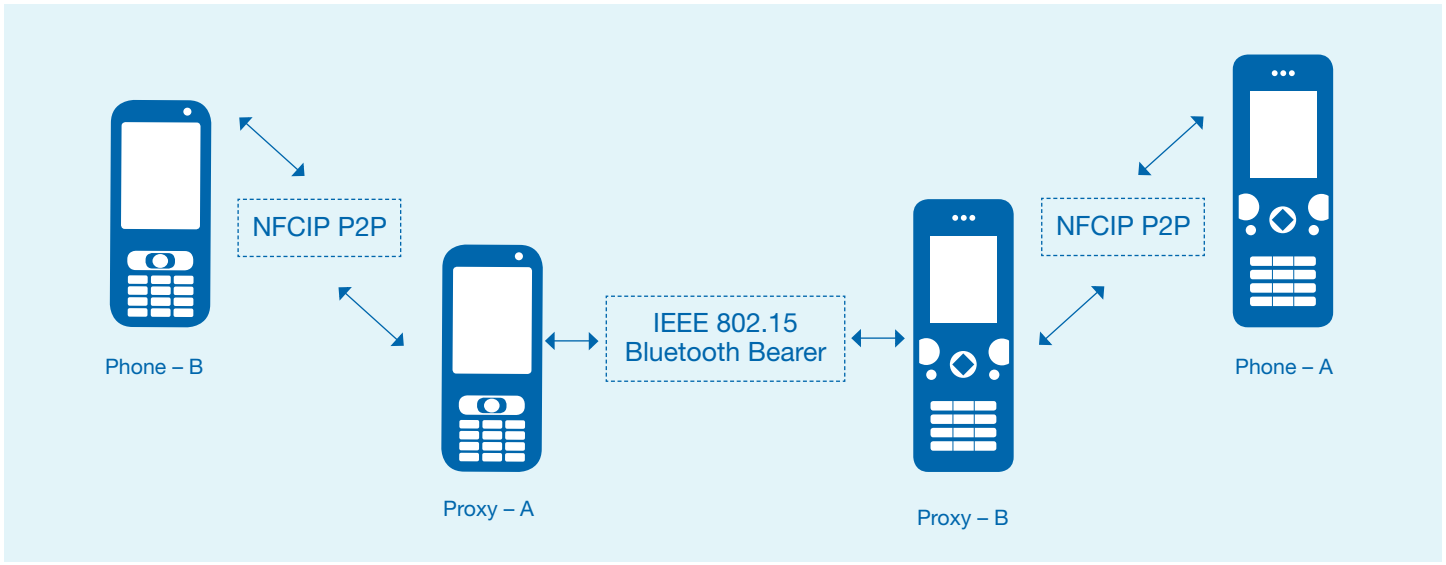
[1] http://en.wikipedia.org/wiki/Cybersecurity on 11/02/11

[2] http://www.instisp.org

[3] Parker, Donn B. (2002). *"Toward a New Framework for Information Security"*. In Bosworth, Seymour; Kabay, M. E.. The Computer Security Handbook (4th ed.). New York, NY: John Wiley & Sons. ISBN 0471412589. http://www.computersecurityhandbook.com

[4] COBIT® Security Baseline: An Information Security Survival Kit, 2nd Edition 2007. The IT Governance Institute.

[5] http://www.aesrm.org/a_case_for_convergence.html



SECURITY OF NFC ENABLED MOBILE PHONES

By Lishoy Francis

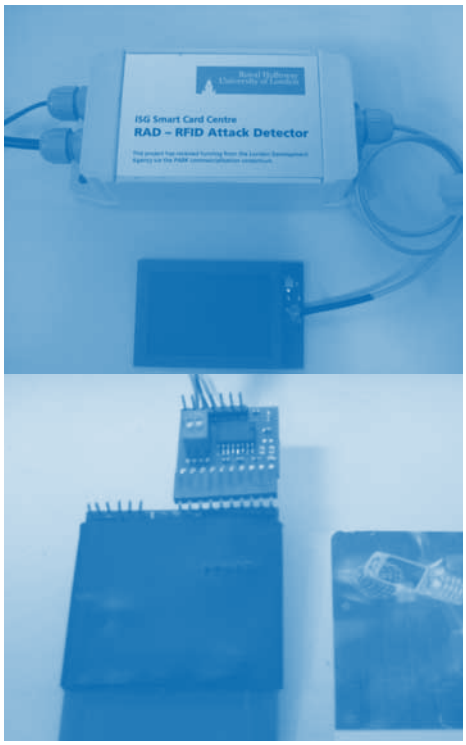
> Lishoy Frances is a PhD student working in the Smart Card Centre.

Following the success in evaluating the platform security of NFC (Near Field Communications) enabled mobile phones by finding security exploits and proposing the required countermeasures, we continued our research to explore the security of NFC transactions. In particular, we were interested in examining the security of NFC Peer-to-Peer (P2P) transactions (as specified in ISO-18092/ ECMA-340 and ISO-21481/ECMA-352), which are being used for sharing data and content between mobile devices, such as digital business cards and social networking details. Recently, NFC P2P has been considered for more sensitive applications such as payments. For example, Apple Inc. in its 2010 patent actively discusses NFC P2P techniques for its payment application. Although the feasibility of relay attack using NFC mobile phones was proposed in the existing literature, a practical relay attack using this platform has not been demonstrated until now.

We found that by using off-the-shelf NFC enabled mobile phones it was possible to create and maintain a proxy channel between legitimate parties and attackers in order to mount a relay attack. We created a P2P transaction in a controlled laboratory environment that would authenticate two mobile phones by exchanging a few bytes of data. We then created and established a Bluetooth (IEEE 802.15) proxy channel between two attack mobile phones. Each of the proxy phones (attackers) then entered into a P2P transaction with legitimate mobile phones (victims). The mobile at one end of the proxy channel relayed all commands to the one at the other end and all responses were then relayed back across the proxy channel (as illustrated in the above Figure).

Our experiments also showed that it is possible to create a proxy channel using any other available bearers such as SMS and mobile Internet. The attack functionality was implemented using only software via publicly available APIs in a standard MIDlet (Mobile Information Device Profile or MIDP application) using JSR 118 API. It was interesting to find that the MIDlet neither required access to secure program memory nor use any code signing, which would give an advantage to the attacker. The attack could be further de-skilled by providing ready-to-install-and-run software that could be misused by any non-technical attacker. We carried on our work to present relay attack countermeasures using device location that is easily available within the mobile environment. These countermeasures could also be applied to detect and inhibit relay attacks on contactless applications using ‘passive’ mode of NFC enabled mobile phones.

Our work appeared in the proceedings of The 6th Workshop on RFID Security (Practical NFC Peer-to-Peer Relay Attack using Mobile Phones, Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis, In Proc. S.B. Ors Yalcin (Ed.): RFIDSec 2010, LNCS 6370, pp. 35–49, 2010. Springer-Verlag Berlin Heidelberg 2010). This work has also resulted in filing a patent application that explores a location and proximity security solution.



RFID Attack Detector (RAD) Pictures

THE ISG SMART CARD CENTRE IN 2010
By Keith Mayes

> Dr Keith Mayes is Director of the Smart Card Centre.

As usual, the most public activity of the ISG Smart Card Centre (SCC) in 2010 was the SCC Open-Day on September 7th. The day was opened with stirring speeches from Vice Principal Adam Tickell and Dean of Science Philip Beesley, who referred to the importance of university engagement with industry in order to guide research and train the work force of the future. Industry was well represented with our exhibitors including Giesecke & Devrient (G&D), Transport for London, ITSO, Comprion, Barnes International, Cubic, The Institution of Information Security Professionals, Infineon, Gemalto, Oberthur, Collis, Burall Infosmart and Multos International. As always the industry participants were matched by exhibits from SCC masters and PhD students and there were also a couple of posters prepared in conjunction with the Geography and Bio-Sciences departments at RHUL. The guest lecture was from Dr. Klaus Vedder of G&D.

Visitors voted for their favourite industry and student exhibits and, yet again, G&D was awarded the Crisp Telecom award in the industry class with Adefurin Odunyemi (Design of a health information system card with an NFC-enabled mobile phone in developing country) winning the student class. A runner-up, Andreas Grunert, was not disappointed for too long as he later went on to win the David Lindsay prize for his project "Efficiency of Zero-Knowledge Proofs of Knowledge Identification Protocols on Smart Cards". There were also a special industry award to the ISG's own Jon Hart for his MSc project in 2009 entitled "SIMwallet: Secure mobile credential storage and enhanced web authentication using a Java SIM".

A regular SCC exhibitor (Xuefei Leng) was absent this year, as he had successfully completed his PhD thesis. Congratulations go to Dr Leng, who is now working back home in China. Attendees of the open day probably don't realise that as soon as the doors close on the exhibition we start preparing for the next one. It is fantastic that six organisations have already offered sponsorship for the event in 2011. The main sponsor is Orange (more about them later), with regular sponsors including Visa, CESG, Barnes International, Comprion and Collis.

The smart card MSc module is now in full swing and the SCC will be supervising around 25 MSc projects this year. The topics are as usual diverse and inspired by industry suggestions and in some cases offers of short internships for students. One of the most active companies in this respect has been Orange and I am delighted that they have agreed to become a full member and sponsor of the SCC over the next three years. I am excited about the prospect of what Orange and the SCC may do together. I am also extremely pleased that Transport for London has agreed to extend its involvement with the SCC for at least another year.

PhD/staff research activity has generated around 12 published papers in 2010 (www.scc.rhul.ac.uk/publications.php), covering diverse topics. Some of these papers involved Yuanhung Lien who had been a SCC visiting researcher from NTUST/Taiwan and I am very pleased that Dr Lien recently obtained his PhD in recognition of his work.

In the 2009 newsletter I mentioned that funding was received from "PARK" to develop an RFID Attack Detector prototype (RAD). I am pleased to say that the RAD prototype is fully functional thanks largely to the efforts of Gerhard Hancke, and is currently being shown to interested parties, with the hope to continue its development/exploitation.

What else does 2011 hold in store? Well I shall be helping Kostas Markantonakis to write/edit a new text book on "Secure Smart Embedded Devices: Platforms & Applications" and we will also both be doing our best to attract new PhD students and funding. Please contact us if you feel that there are areas that we could explore together.

2011 STEVENSON SCIENCE LECTURE: LT GEN SIR EDMUND BURTON

By Keith Martin

> Prof. Keith Martin is Director of the ISG.

The ISG was honoured that Lieutenant General Sir Edmund Burton accepted an invitation to present the annual Stevenson Science Lecture at Royal Holloway on February 23rd, 2011. Sir Edmund, who supports the Cabinet Office in implementing the UK Government Information Assurance Strategy, addressed the audience on the subject of Scientific Community - Fulfilling an Effective Role in Shaping an Uncertain Environment.

Sir Edmund began his presentation by challenging the audience to consider how society can best be made aware of the critical role that knowledge plays in the lives of both citizens and businesses. He felt that there was plenty of evidence to suggest that society was taking far too long to acknowledge this. He gave several thought-provoking examples that provided evidence for a lack of understanding of this issue, including the numerous massive security breaches in the UK that have occurred since 2004 and the fact that the Government "inspired and funded a nationwide programme of CCTV cameras and Automatic Number Plate Readers without a concept of use or formal business case". He stated that he wished to "set out the case for an urgent, invigorating discussion between and across academic communities in order to inspire new thinking and research into the social, political, economic, legal, ethical and technological implications of the information revolution" and to emphasise the role of academia in addressing these issues.

Sir Edmund went on to observe that major IT initiatives will continue to fail if the intersection areas concerning people, processes and technology are not understood. He felt that currently they are not understood well and questioned whether they are being addressed at the right level in our current education system. He felt that "the education of the current and future generations of enlightened leaders" is a key role for the academic community. With this in mind he acknowledged the contribution of the ISG in establishing information security as an academic discipline and praised the training of 2000 MSc Information Security alumni around the world.

While Sir Edmund's message was framed around information security, much of his message had wider relevance to the communication of scientific ideas amongst society in general. He concluded his talk by considering how science can play a leading role in our society. Sir Edmund made several suggestions based on his considerable personal experience. These included the importance of networks because "innovation frequently occurs at business and cultural boundaries, when good people meet". He stressed the value of interdisciplinary links and the importance of good communications between academia, industry and government. He also commented on the importance of continuous modification and updating of educational programmes to match the pace of developments in the IT sector and the need to inspire and link with the wider community, including schools, charities and regulatory bodies.

This was a powerful message and one that resonates strongly with the spirit in which the ISG has been set up and managed over the last 20 years. Sir Edmund was quick to recognise this and suggested that academic groups around the world could benefit enormously from the experience of the ISG. He closed by emphasising this point: "It seems to me that Royal Holloway and the ISG, under the leadership of Prof. Fred Piper and his colleagues within and beyond the College, have demonstrated what can be achieved".

Prof. Mike Walker proposed a vote of thanks. He stated that Sir Edmund's insightful picture matched his own experience in the telecommunications business where "innovation was all about cross-disciplinary work". Mike called for more engagement between technologists and board members, and for more co-operation between science and industry, and acknowledged the pioneering role of the ISG in this latter regard.

"DOG BITES MAN"— WHY STUXNET WASN'T NEWS

By Thomas Richard McEvoy

> Thomas Richard McEvoy is a part-time PhD student and Risk Practice Manager at HP Enterprise Security.

Reporters ringing my PhD supervisor, Dr Stephen Wolthusen, in late 2010 regarding the Stuxnet Trojan were somewhat disappointed by the reaction that they received. Not only was Stephen not interested in the question of attribution, but he was less than excited about the malware's capabilities.

Yet this was a piece of malware which was targeting SCADA systems, apparently for the first time, and possibly attacking factories in Iran – although it should be said that the attack was somewhat scatter-gun and also affected factories in Norway and Germany.

Such ennui is easily explained. Not only is this not the first time such attacks have been carried out, but for at least a decade researchers, including myself, have carried out work which describes and predicts the capabilities and behaviour of such malware on SCADA (supervisory control and data acquisition) systems, which form part of the critical national infrastructure. Moreover, the technical details of Stuxnet reveal a pedestrian, and indeed somewhat clumsy, approach to the code development, with nearly all of the techniques employed being derived from previous examples of such malware. Perhaps the only exception was the Stuxnet WinCC module, where the technique derived relied simply on having carefully `read the manual".

SCADA systems are used on industrial and transport systems and comprise of a set of master consoles manned by human operators with various commun-ication links to control units, which may be geographically distributed. The control units directly operate valves and switches in accordance with preset parameters based on desired physical behaviour (for example, temperature) while the operators can acquire information (perhaps for quality assurance purposes) and alter parameters in accordance with business and production requirements. Examples that we have used in research are a beer pasteurizer, a chemical plant and a hydro-electric power system.

In computing terms, SCADA systems are large distributed, segmented networks with a mixture of hard and soft real-time processing and communications requirements. In the past, such networks have been built from proprietary components and were isolated from other networks, but today they are built using commercial off-the-shelf hardware and software and are normally connected to the Internet to permit real-time decision-making on production outcomes and product distribution.

In the past, attacks on SCADA systems required physical access. However, the rapid introduction of modern, generic hardware and software and external network communications has exposed such networks to remote malicious attack. This security exposure is worsened by both the failure of process control engineers to understand security requirements, which results in them not applying them, and the failure of IT specialists to understand production priorities, which results in inappropriate security solutions being suggested. As an example of the latter problem, modern antivirus and encryption techniques have the potential to place an unacceptable burden on performance in some SCADA systems.

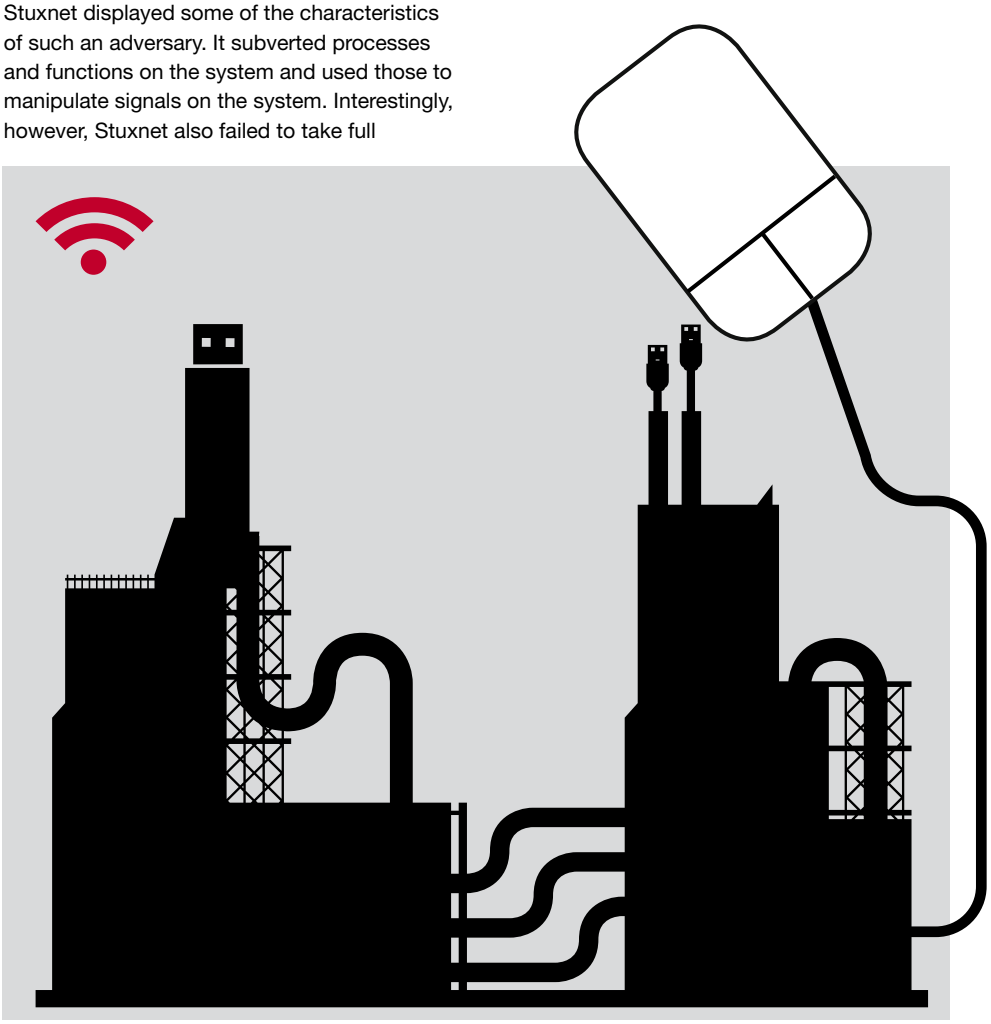
My own research work has outlined an adversary capability model for SCADA environments. This model sets out how attackers subvert processes on a system. These processes carry out various operations, based on the attacker's understanding, but need to be updated to deal with new situations. There is a lag between updates which sometimes allows detection. For example, Stuxnet used USBs both to spread itself and to pass on updates, as well as remote network channels. Clearly, the creator(s) felt that they could tolerate considerable delays in updates but, according to my model, this maximized detection opportunities and may, in some cases, have contributed to its detection. Stuxnet displayed some of the characteristics of such an adversary. It subverted processes and functions on the system and used those to manipulate signals on the system. Interestingly, however, Stuxnet also failed to take full advantage of the situation. It could have been made considerably more sophisticated. For example, Stuxnet failed to use covert channels for communication. It could also have carried out internal denial of service attacks which, on a chemical plant, could have had very serious (not to say explosive) consequences. In other words, the way is paved for much worse versions of the same kind of malware. However, I believe that we have already predicted many of these characteristics and methods and so can be prepared in defensive terms.

I want to better understand the vulnerabilities of SCADA systems and to help protect these systems in the future. I am modelling attacks and working on detection methods which continue to function even when an intruder has taken over some of the processes and communication channels on the system. The end goal of such research is not just to detect an attacker but to be able to intervene in an attack and wrest back control of the system from the attacker.

Further reading:

Thomas Richard McEvoy and Stephen Wolthusen, ***A Formal Adversary Capability Model for SCADA Environments***, CRITIS 2010

Ronald L Krutz, ***Security SCADA Systems***, Wiley 2006



TWO TALES OF A SUMMER INTERNSHIP AT IBM NEW YORK

By Elizabeth Quaglia

> Elizabeth Quaglia is a final-year PhD student, currently writing up her thesis.

EVALUATING WIRELESS SECURITY

In a world that is increasingly reliant on digital technologies, security is a major concern and the driving principle behind protocol design. The recent years have seen the rise and rapid growth of wireless technology, which uses waves (instead of wires) to carry signals over the communication path. Compared to a wired network, wireless networks are subject to additional security threats such as the deliberate transmission of signals that disrupt communication, also known as jamming. This means that the specific nature of the network may lead to considerably reduced efficiency. Suppose that we choose a secure key exchange protocol and directly plug it in a wireless communication channel. This will preserve its security properties, but could worsen its performance so severely that the protocol may become impractical. Therefore, it appears necessary to revisit traditional protocols in light of new potential attacks. For this purpose, a powerful toolbox into the quantitative evaluation of wireless security protocols has been developed. Not only does this provide us with a way to accurately select the most efficient solution, it also gives some insight for the design of new protocols, more specifically tailored to the wireless environment.

This work is the result of a fruitful collaboration between Royal Holloway, IBM Watson and the University of Massachusetts, and was largely carried out during my internship at IBM Watson last summer. It involved combining several areas of expertise, from cryptography to linear systems theory, in order to obtain the desired performance enhancements that are crucial to the wireless setting. In particular, we analysed key-exchange protocols and proposed more efficient solutions, achieved by blending carefully crafted techniques. The toolbox can be further developed and applied to more complex protocols, such as public key management or secure routing protocols for ad hoc networks.

While working on this project, I experienced how relevant dialogue and collaboration between research communities are to real-life applications. Scientific progress is indeed based on technical skills but also on the ability to reach out to other fields. My exposure to different research environments, such as Royal Holloway and IBM Watson, has been invaluable in my personal development as a researcher. As a PhD student, I highly recommend proactively engaging in various areas of research, since this may lead to advances in not only one field, but many.

SEARCHING FOR A STUDIO IN NEW YORK

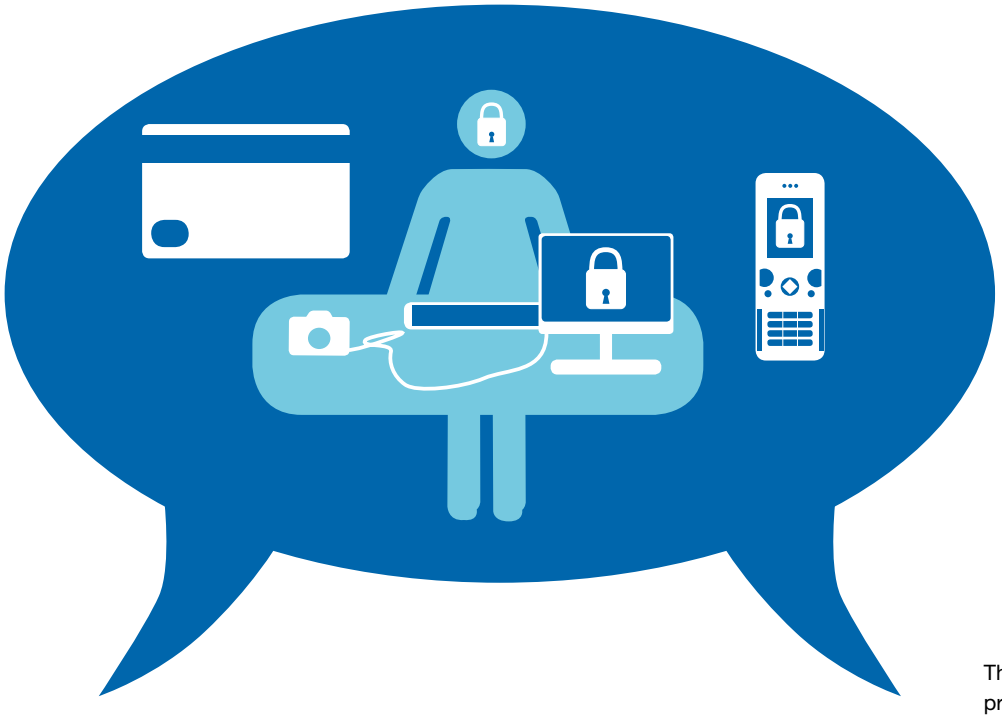
I arrived in New York City on a hot summer afternoon, and everything looked just as I had imagined. The wide and elegant hall of Grand Central Station, the hectic yellow traffic jam of 5th Avenue and the lively and colourful streets, filled with queuing people, in line for a succulent hot dog, a rushed cab or for a ritual picture in front of the Empire State building. In the first few days I only focused on finding a studio to rent and so I kept my eyes busy looking at street signs and getting in the correct side of the metro entrance. It took me a while to realise how little sky you can actually see from Manhattan.

The house-hunt turned out to be far more adventurous than I had anticipated. My meticulously planned viewings started in an area which looked respectable, but as I was getting closer to the precise address I gradually developed a feeling of sadness and abandonment, in perfect harmony with the surroundings. As she was coming out from the building I was about to view, a girl said to me "It is full of cockroaches, do not rent here". I believed her. My next appointment was with a woman, who showed me a cute studio on the East Side. In the city where a minute is just 59 seconds too slow, I had found the studio I wanted, made my way to the agency, signed the contract and paid the monstrous deposit in less than 24 hours.

Or at least I thought I did. My card did not work, probably since it was such a large amount from abroad, and then it was blocked, leaving me in a complete state of panic. Alone, I spent my first weekend in New York not using transport and not eating, caused by irrational concerns about wasting the little cash I had. An unnatural feeling of having been scammed also started growing inside me, most likely fuelled by comments and criticisms made by various encounters I had, like the policeman telling me "You found your studio on Craigslist? Don't you know a woman was killed because of Craigslist two months ago?"

A healthy reality check with my family back home got me through these first moments, and my card was functioning again by Monday, which allowed me to calmly settle in soon after. I then started to deal with all the other aspects of moving to a foreign country, such as getting a social security number, opening a bank account and setting up utility bills. And of course, I had to start my internship. After a few bureaucratic headaches, including a rather worrying tentative non-confirmation letter, a mistake by Homeland Security, everything eventually fell into place just about two weeks before I had to leave!

But I will not complain. After all, I was living in New York for three months...



CITIZENS, ACADEMIA AND INDUSTRY – FORGING NEW PARTNERSHIPS AND CO-CREATING ALTERNATIVE FUTURES

By Lizzie Coles-Kemp

> Dr Lizzie Coles-Kemp is a Lecturer in the ISG.

Increasingly, academic research projects are required to demonstrate social impact. The role of dissemination within a research project is on the front-line when it comes to demonstrating social impact. In social research projects, in particular, dissemination is undergoing transformation as traditional techniques become augmented with public engagement activities.

The Visualisation and Other Methods of Expression (VOME) research project uses dissemination in a number of very different ways. The project's primary goal is to develop interaction tools to help service users make better sense of their on-line privacy protection options. The technology design component is led by a research team within the ISG. The technology design draws on the social research conducted in other parts of VOME together with user experience research to develop designs for interaction tools that are more empathetic with the ways users think and engage with on-line privacy, as well as respond to the design's functional requirements.

At each stage in the project, VOME has run dissemination events that include "grass roots" (ground-up and citizen-centric) debate on current privacy and consent issues. We work with speakers who can situate the debate in current political and social topics. In order to obtain this, at each event we include as many representatives as possible from the different communities that VOME has been working with. The objectives of this type of activity are knowledge transfer, exploration of technology issues in current contexts and the stimulation of debate between different stakeholder groups. We measure social impact directly in terms of stakeholder reach and follow-on dissemination activities. We measure social impact indirectly in terms of impact on our technology design, opportunities for further engagement with stakeholder communities and influence on the future agendas of the stakeholder groups represented.

In December we ran one such event at the British Museum. The workshop was entitled "Delivering public services on-line: How does it change the status quo?" and explored the implications of digitizing public service delivery. The vision of a digitally enabled and digitally confident citizen is one that has endured government change within the UK. The changing social and political context and the shifting expectations of both the citizen and the government mean that whilst there is still a need for privacy and identity management tools, the nature of those needs shift and the degree of ambiguity related to privacy concerns increases. Designing technology in such a fast moving landscape is challenging. VOME sits right in the middle of this fluid landscape.

The event started with an overview of VOME progress and then moved to a range of voices on the workshop topic. The keynote speakers focused on very different aspects of on-line public service delivery. Ollie Bray, National Adviser for Emerging Technologies in Learning and Technology Futures at Learning and Teaching Scotland (LTS), delivered a talk on understanding the new learning landscape. Kieron O'Hara, Senior Research Fellow in Electronics and Computer Science at the University of Southampton, delivered a talk on the government's transparency agenda and the relationship with privacy. Practitioners representing the different communities that VOME has worked with were both in the audience and part of the reflective voices that were used to comment on the content of each talk and to contextualize it in the situations in which VOME has been working. These talks and some of the feedback on them can be found on our website. The talks and the reflections stimulated small group discussions that enabled the audience to delve deeper into the topics raised, explore VOME work in context, and provide feedback on our work to date.

This type of dissemination activity is very powerful for social technology design because it promotes a dialogue between the different stakeholders involved and enables the designers to better understand the interests of each stakeholder group, as well as the types of interaction that each would like to have. Being able to situate the evaluation of our research outputs in the context in which our work was carried out enables the workshop participants to obtain a better sense of how we envision our work to be used, as well as give them a context through which to give us feedback.

www.vome.org.uk

VOME is funded by the Technology Strategy Board, EPSRC and ESRC.

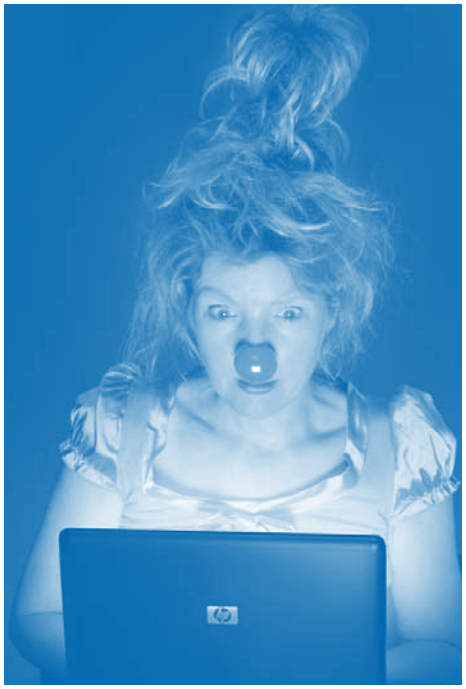
SERIOUSLY CLOWNING AROUND
By Lizzie Coles-Kemp

> Dr Lizzie Coles-Kemp is a Lecturer in the ISG.

2010 was a year of many firsts for the ISG, including our first steps into performance art! The ISG took part in the UK's Festival of Social Science by putting on a play of the first year results of the on-line privacy project, Visualisation and Other Methods of Expression (VOME). The event was run by VOME's technology team, who are resident in the ISG, and was entitled "Exploring privacy: your privacy and the internet". It took place on March 13th, in Winter Gardens, Sunderland, and was played to members of the general public.

Choosing to make a play of scientific results might seem like a strange choice of activity for a technology research team. However, using art to stimulate scientific debate and draw out different dimensions of complex issues, such as on-line privacy, is increasingly gaining credibility as a tool that can usefully situate science within its social context. The situated nature of privacy makes it an extremely difficult topic to engage on with many audiences. Creating a story, and situating privacy within that story, enabled VOME to reach a wider audience with their results and to stimulate further discussion on the work to date.

Each year the Economic and Social Research Council (ESRC) runs a nationwide Festival of Social Science to feature events from some of the country's leading social scientists. The festival celebrates the very best of British social science research and how it influences our social, economic and political lives – both now and in the future.



Developing a play based on field research is no small challenge! In order to help us, we teamed up with physical theatre company Bimbilibausa. We gave our first year results to the three performance artists who form Bimbilibausa and talked through the scenarios that might enable us to tell the story of our work. Both VOME and Bimbilibausa wanted a play that encouraged audience participation and which asked the audience to work through the different privacy scenarios with the performance artists.

The play was set in an office environment and examines the relationship between the three characters Margareth, John and "the Boss". Using theatre, the play was able to encourage the audience to explore privacy and identity issues in physical and virtual spaces simultaneously, just as these issues manifest themselves for all of us in our everyday lives. The audience participated by using an e-voting tool to vote on the privacy practices that the play's lead character, Margareth, should have followed.

After the event, Frances Freya Sturt, who plays Margareth, reflected on the main challenges of putting on such a play. "Firstly, we wanted to make sure that we were representing the research by VOME and the behaviour of on-line use. With any piece of theatre it needs to be dramatically watchable, the writing needs to be strong. We also wanted to engage the audience and therefore use questioning. The audience's answers had a direct influence on the direction of the play. The involvement of audience participation means there is more risk taking and the work is more unpredictable. This makes it more challenging for the actor/writer, whilst at the same time makes it alive and exciting – the performer needs to listen well and improvise. The final challenge was that we wanted to make sure that we were not manipulating outcomes and that we left these open for the audience to decide. "

So is there a role for performance art in information security research? Working with various forms of art is part of the toolkit that we are using as researchers to explore the "invisible" and intangible aspects to privacy. It is an approach that we use to understand how privacy looks and feels from the perspective of being human, as opposed to how it looks to a computer. As a performance artist, Frances thinks that "Performance art can help define the grey areas that are harder to explore using conventional research methods - it can help engage people and promotes lateral thinking." The story VOME is looking at is a human one, so using tools that explore what it is to be human helps us to further understand that story.

In 2011 VOME is further developing its engagement with artistic communities in order to develop its final outputs. A range of arts is being used to stimulate the final design of its technologies and the project hopes to be able to exhibit its work as art, as well as communicate it as science, at the end of the project.

You can hear more from Frances and watch the play at www.vome.org.uk

STAFF PROFILE: DUSKO PAVLOVIC

> Prof. Dusko Pavlovic, formerly of the Kestrel Institute, joined the ISG in January 2011.

Q: Tell us a little bit about what you were doing prior to joining the ISG.

A: I worked at the Kestrel Institute in Palo Alto, California. Kestrel is the place where they introduced the "correct-by-construction" idea. The founder of Kestrel, Cordell Green, defined the concepts of theorem prover and program derivation in his thesis in the late 1960s. So the Kestrel idea is that you write down formal specifications of what your software system should do, and refine them until you completely pin down all functions, at which point you can generate code. I went there because I didn't want to spend my life just talking about computers, but wanted to generate something, and it was a very exciting time. I got a project to do the "correct-by-construction" thing for security protocols. But you cannot simply refine security protocols, of course, since something that could have lots of values before may end up with fewer values, and less security, after you refine it. So it was a challenging task. It was especially challenging to compose protocols knowing that they will preserve each other's invariants. There are now some publications about that. When the tool was done, you could incrementally build not only protocols, but also attacks, and it broke, for example, a protocol that was just standardized after seven years of the internet drafts, even formally verified... But it was a very big development project, a bit too much for me, especially towards the end.

Q: What attracted you to apply for a job with the ISG?

A: I spent a long time at Kestrel, longer than anywhere else in my life. I didn't think that I would start missing academia, but my students disappeared into Google and I started missing academia. I made long visits to Oxford, where I hold a Visiting Professorship. I now work in information security, and ISG was just about the first "information security school" in the world, wasn't it? Information security as a branch, in fact a separate tree, is well established in industry, but it only recently started growing its own roots in academia. So the ISG may have been some 15 years ahead of its time. How could I not apply? Very happy to be here.

Q: You have a diverse range of research interests – what drives you to constantly explore new areas of research?

A: I don't have an answer in the form of a master plan. But I have of course noticed the phenomenon: that my publications span from graph colouring, through higher order polymorphism and garbage collectors, to distance bounding protocols and trust, with the odd excursions into symbolic computation and games. Not to mention the quantum stuff. It immediately raises the flag that the breadth must go at the cost of the depth, and also at the cost of your career, since science and publishing are done within tightly knit communities, which don't always like outliers.

But I think that it is a big picture behind everything that I have been working on. It goes as follows. The one big thing that happened during my life is computers. The question that computers always ask you is: How do you replace cleverness by method and write down this program? Why is it that I cannot write an inductive procedure to optimally colour a map when there is the 4-colour theorem? How do I build a really big software system that does not get exponentially buggier as it grows? And so on.

But the thing is, if you honestly listen to the question that the computer asks, you end up in the other corner of the room, without noticing. Twenty years ago, the computer was in the box in front of you, or in the room next door, printing some numbers. Nowadays Netflix predicts which movies you will like, even though you have never heard of them; and Google tells you the answers to your questions before you ask them. Well, twenty years ago I thought about the computer on my desk; and nowadays I am thinking about this new computer, and about Alice and Bob talking through it. I believe that I have been exploring the same mountain all these years; but the mountain moved.

Q: You have experience of working in the U.S. and the U.K. – do you see any differences in the information security culture between the two?

A: Ah, while most developing countries have many similarities, each aging empire is aging in its own way! I am not sure that I yet have a good insight into the UK, I only lived here sporadically since the 1990s. But my impression is that the basic difference arises from the fact that in the US, the government is mainly preoccupied with the emerging cold war in cyberspace, while industry has been given an open field for gathering and analyzing data about the citizens and the market, achieving some remarkable results, be it good or scary. On the other hand, in the UK the government has somehow developed the idea that gathering and analyzing data about the citizens would make it more efficient, and heavily invested in this, so industry focused on selling the data and security services to the government, without much incentive to deliver or innovate. The common players in both scenes, such as the credit card operators, some data aggregators, and some financial structures, have the potential to develop into a serious information security threat with technology advances and a lack of regulation.

Q: What challenges have you set yourself for the next few years?

A: I now understand several things about information security that I would like to "write down". I need to learn how to communicate them very clearly. It is a tall order, though, since the area is a conceptual mess.

Q: What does it feel like to be occupying the legendary Peter Wild's office?

A: First thought: honoured. I don't know Peter that well, but I have had the chance to interact with the other founders of ISG. Quite a torch for all of us to try to keep aflame.

DIGITAL FORENSICS IN VEHICULAR TRACKING AND SURVEILLANCE

By Saif Al-Kuwari and Stephen Wolthusen

> Saif Al-Kuwari is a PhD student with interests in computer forensics and cybercrime investigations.

> Dr Stephen Wolthusen is a Reader in the ISG.

In many legal proceedings, establishing the whereabouts and actions, particularly movement, of individuals is crucial in establishing guilt or innocence. This not only applies in intelligence and counter-terrorism operations and serious criminal matters, but is also potentially of interest in civil matters such as injunctions and divorce cases. The information may be sought under real-time constraints (e.g. in pursuit of a suspect), or forensically. However, in the latter case one can typically distinguish situations where some preparation, such as sensor placement, can occur beforehand, from situations where one is reduced to relying on opportunistic data availability.

Recent years have already seen a dramatic proliferation in the availability of geolocation information, largely (but not only) driven by inexpensive satellite geo-positioning components becoming embedded in smart phones, digital cameras, and a multitude of other devices. In other cases indirect terrestrial radio-frequency based methods are used to similar effect.

This has raised a number of privacy-related issues. For example, social networking applications have been making use of this information to provide location-based services (e.g. Foursquare, Facebook Places and Google Latitude), leading to an entire category of “Geosocial Networking” mechanisms providing location-based services. However, such information is also revealed inadvertently. Even individuals who do not share their location information, or may not even be active users of such services, can be identified by the geo-location information embedded in photographs by third parties and the use of advanced face-recognition systems.

In support of both forensic and particularly surveillance applications by law enforcement, we have been investigating novel ways of linking individual geo-position reports with a number of other data sources in order to establish a more complete view of the whereabouts and movements of observation targets in novel ways, including from radio-frequency emissions such as Bluetooth or IEEE 802.11 (WiFi) signals.

This allows the formation of a more accurate picture of observation target movements and, together with the use of explicit mobility models, the prediction of likely behaviour of a target, as well as constraints on movements. In forensic applications this serves to enhance the confidence with which a movement can be reconstructed. In real-time surveillance situations such mobility models may also serve to pre-position scarce assets for surveillance in order to ensure that an observation target is not lost or can learn about the surveillance.

While even moderately concerned individuals will be aware of some of the perils of location-based services, another category of surveillance and forensic analysis data may be less familiar, but potentially even more intrusive. Many modern vehicles, particularly those used by executives, typically come with a geo-positioning system, but also with a large number of additional sensors which can aid in tracking and surveillance. A high-profile example is the OnStar assistance programme, which was used primarily by General Motors in North America and China, initiated in 1995 and launched in 1997. This was the subject of a court case in the U.S. 9th Circuit Court of Appeals, which resulted in the U.S. Federal Bureau of Investigation being barred in 2003 from using the built-in mobile telephony service for surveillance. Such restrictions do not, however, apply in all jurisdictions – and neither intelligence agencies nor criminals are bound by them.

The combination of a hands-free telephone system, Internet connectivity and geo-location system which can both be externally activated or monitored is not new. However, this is also only a subset of currently available sensors and, more importantly, the fact that surveillance is externally activated and conducted means that it can be observed by a target, potentially provoking evasive actions or modification of target behaviour.

Our recent research shows that this restriction on observers is no longer a severe impediment. Modern vehicular systems not only come with significant amounts of non-volatile storage (to be used for on-board navigation and entertainment systems), but also a plethora of internal and external sensors. These include microphones placed throughout the vehicle’s interior, as well as motion detectors, and in some cases cameras for detecting driver behaviour such as drowsiness. External sensors may include several high-quality cameras operating in either visible light or infrared spectrum. Reversing cameras are rapidly becoming standard equipment on higher-end vehicles, and have recently become available with surrounding cameras in order to assist parking in tight spots. This, together with further sensors such as radar or ultrasonic parking distance sensors, as well as the ``black box” data recording components that are mandated in some jurisdictions, provides a rich suite of active and passive sensors that can be accessed from other vehicular electronics. This permits modern vehicles to be turned into semi-autonomous surveillance systems.

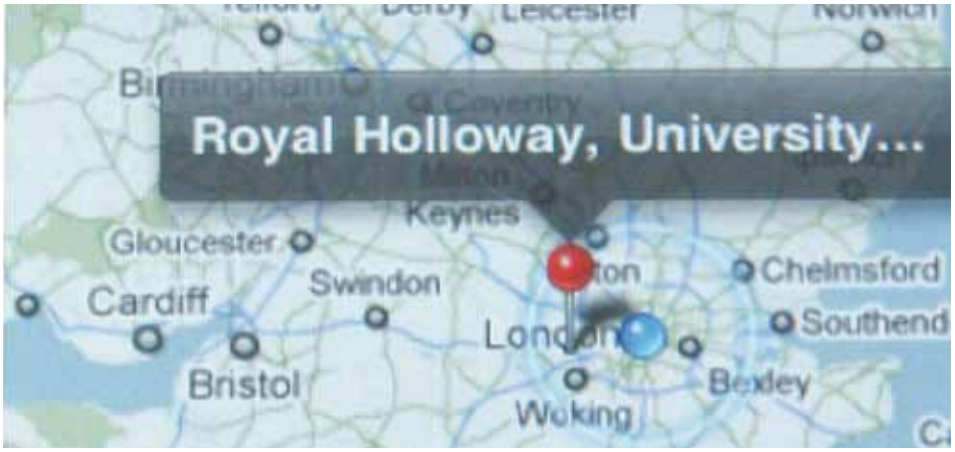
Based on these findings, it is rather advisable to stop regarding vehicles as private, secluded spaces and to consider them as being highly vulnerable to surveillance and forensic analysis.

Further reading:

Al-Kuwari, S., and Wolthusen, S. ***On the Feasibility of Carrying out Live Real-Time Forensics For Modern Intelligent Vehicles***. Proceedings of the 3rd International ICST Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics 2010), Shanghai, China, Nov. 2010,

Al-Kuwari, S., and Wolthusen, S. ***Algorithms for Advanced Clandestine Tracking in Short-Range Ad Hoc Networks.*** Proceedings of the Second International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (Mobisc 2010), Catania, Italy, May 2010, vol. 47 (part 3) of IFIP Advances in Information and Communication Technology, Springer-Verlag, pp. 67-79.

Al-Kuwari, S., and Wolthusen, S. ***Probabilistic Vehicular Trace Reconstruction Based on RF-Visual Data Fusion.*** Proceedings of the 11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS’10), Linz, Austria, May 2010, , vol. 6109 of Lecture Notes in Computer Science, Springer-Verlag, pp. 16-27.



SNOW (ALMOST) STOPS PLAY AT THE 2010 HP COLLOQUIUM
By Kenny Paterson

> Prof. Kenny Paterson is an EPSRC Leadership Fellow in the ISG.

The 21st Hewlett-Packard Symposium on Information Security was held at a snow-bound Royal Holloway campus on 20th December 2010. Despite the atrocious weather, a healthy audience of ISG "friends and family" gathered to hear the three invited presentations, to view posters produced by the ISG's students and postdoctoral researchers, and to engage in networking in a relaxed setting.

The day kicked off with a topical and thought-provoking presentation by Prof. Brian Collins, Chief Scientific Adviser at the UK government Department of Business, Innovation and Skills and at the Department for Transport. In his talk, Brian ranged far and wide, drawing on his experiences as a physicist and as a policy influencer, to reflect on the topic of "Information, Security and Anthropology". His presentation provoked a lively debate that continued well into the lunch break.

Brian's talk was followed by a presentation from Prof. Bart Preneel (K.U. Leuven in Belgium), who had struggled manfully through the weather conditions to reach Royal Holloway at about 2am that morning. In his talk, Bart gave an overview of the challenges to privacy engendered by modern technologies, as well as thoughts on how new technologies might be developed to preserve privacy in the face of this onslaught. Given the deteriorating travel conditions, Bart left us immediately after his talk, with reports eventually reaching us of a monumental return journey involving trains, ferries and a PhD-student-provided taxi service. Bart certainly wins the prize for perseverance in the face of overwhelming odds!

The day then continued with a presentation to Pauline Stoner, on the occasion of her retirement. The presentation of a silver watch and a cheque for Pauline's holiday fund was made by Marcus Alldrick from Lloyds on behalf of all of Pauline's friends in the information security industry. Pauline was suitably embarrassed and has been working hard to suppress all photographs of the event; there was not a dry eye in the house...

The final talk of the day was delivered by Prof. John L. Manferdelli, Distinguished Engineer at Microsoft Research, on the topic of "A Framework for Trusted Computing in Clouds". John introduced the audience to the massive scale and computational power of cloud computing services, before discussing the many security issues – new and old – that arise in these outsourced computing environments. John then went on to sketch how trusted computing technologies might be harnessed to address many of these issues.

We would like to thank everyone who contributed to making the day a success, especially the speakers who could so easily have turned back at the start of their journeys. We are already planning next year's event, on the assumption that the Gulf Stream will still be in operation in December 2011.

LIVE AND LET DRIVE: THE WHITE HAT RALLY

Keith Mayes from the ISG and his trusty co-driver Glen McDermott took part in the James Bond themed 'White Hat Rally' as the 'Live and Let Drive' team.

The charity car rally organised by Information Security professionals, some from the ISG alumni, was raising money for ChildLine, a confidential 24 hour helpline provided by the NSPCC for children and young people in distress or danger which relies on charitable donations in order to continue operating.

The rally started in Laon, France, and over three days worked its way down through Switzerland and finally to Venice in Italy, following some of the routes seen in 'On Her Majesty's Secret Service' and 'Goldfinger'.

Keith said: "The first day was tough as we had to cover 500 miles through France in torrential rain. Our car steamed up so badly that we had to have the sun roof open and put up with the rain dripping on us. Going through Switzerland in fancy dress was quite fun and got interesting when we took a detour up a mountain pass. We followed a steep winding road with hairpin bends and suddenly found ourselves in a snow storm only to then descend the mountain into glorious sunshine. We managed to reach the finish line near Venice without problems, although a few ageing vehicles expired en route and one crashed out, luckily without injuries."

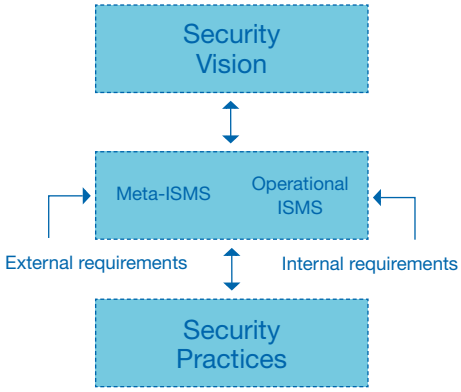
Around 20 teams took part in the rally, with each vehicle fitting into one of three categories, Veteran (25 years and older), Fancy Dress (any car dressed up) or Banger (costing less than £500 and getting scrapped at the end) . The event has raised more than £35,000 for the charity.

THE INTERNAL BARRIERS TO PERFECT SECURITY MANAGEMENT

By Alex Dent

> Dr Alex Dent is a Lecturer in the ISG.

Security evangelists have been preaching the importance of security management for the last fifteen years. The truth is that organisations have always had some form of information security management, even if it's just a vague premise that the organisation wouldn't give unauthorised personnel the opportunity to access critical information. The evolution of security management over the last fifteen years has mostly concentrated on the development of formal information security management systems – i.e. an explicit, written management system which controls the way in which information can be processed by an organisation. There are many articles that discuss the development of security management standards and the experiences of organisations who are implementing them. This article will focus on a slightly different topic: we will examine the underlying mechanisms that encourage or resist the changes which are necessary to fully adopt a useful formal information security management system.



Since any term connected with information security management has at least seven different definitions, we begin by clarifying the meaning of some of the terms that we will be using throughout this article. We assume that an organisation always has a conception of its security aims – we term this the organisation's security vision. An information security management system (ISMS) is the part of the organisation that is responsible for translating the security vision into secure procedures and practices. This article will only be concerned with formal, written information security management systems.

Consider a hypothetical organisation that wishes to use a formal ISMS to manage its use of information within some scope of its operation. Research has shown that the overwhelming majority of formal ISMSs have been put in place to comply with some kind of externally defined notion of security – either in the form of externally imposed regulation (such as SOX or PCI DSS) or voluntary self-regulation (such as ISO/IEC 27001). This external requirement may target the organisation's core business functions, as is the case when an organisation voluntarily chooses to undergo ISO/IEC 27001 certification in order to improve their brand image, or may target the organisation's supporting business functions, as is the case when an organisation implements a formal ISMS in an attempt to satisfy SOX regulation.

Research by Dr Lizzie Coles-Kemp, a colleague of mine in the Information Security Group, has shown that we may view a formal ISMS as having two distinct components:

- The meta-ISMS is the set of security management functions that deal with security requirements that are imposed on the scope of the ISMS from outside of that scope. These management functions seek to ensure that information processing is performed in a way that is consistent with the regulation imposed on the organisation. Typically, these requirements are assessed by a security expert who does not engage in the day-to-day running of the organisational unit which is being assessed and who passes their results down to the scope through policy documents. It can therefore be thought of as an external view of security.
- The operational ISMS is the set of security management functions that deal with security requirements that arise from within the scope of the ISMS. These management functions seek to effectively and efficiently deal with security problems that have arisen in practice, either as the result of observed operational weaknesses or regulatory controls that have been imposed by the meta-ISMS. Typically, these requirements are assessed by a security expert who is actively involved in the day-to-day activity of the organisational unit and can therefore be thought of as an internal view of security.

Given this view of the management system, it is easy to see that the majority of formal ISMSs are developed by the meta-ISMS. This view is broadly supported by the ideas of von Solms, who separates the functionality of an ISMS into those parts which are responsible for security and those parts which are responsible for regulation and compliance. Lizzie's research also demonstrates that formal ISMSs tend to move through six well-defined stages as they mature; however, the focus of this article will not be on the characteristics of these six stages, but on the way in which a formal ISMS moves through these six stages (See diagram on the left).

One fascinating fact that underpins the majority of organisational management research is that organisations are not so different from individuals. Organisations have personalities, memory, and abilities just like individuals. These organisational traits are not simply the result of the personalities of the staff, but are aspects of the organisation itself and exist beyond any one member of staff. They are ingrained in the documentation and processes of the organisation, taught to new members of staff through socialisation, and implicit in hiring procedures which ensure that an organisation only hires new employees with "the right kind of attitude". And organisation personality is very difficult to change – this fact is implicitly proven when any new employee (even a new CEO) attempts to make changes to deeply-rooted policies, only to find a significant backlash against their attempts to "change the way we do things around here".

I don't mean to suggest that organisational personality is necessarily a bad thing: it inspires a sense of belonging and security. Organisational personality is only problematic when it prevents an organisation from adopting improved working practices or adapting to new situations.

The development of secure information processing practices is an example of organisational learning.

The development of secure information processing practices within an organisation can be viewed as an example of organisational learning: the organisation has to learn to value information security and learn the skills required to implement secure practices. The ISMS is the vehicle by which this organisational learning occurs, despite the fact that the ISMS is not a "finished" entity either. The ISMS is also continually learning the best way to manage the security practices within its scope of control. This gives us an academic framework by which we can consider information security management within an organisation.

My own research has concentrated on the approach to organisational learning put forward by Argyris and Schön. Their work is based on the idea that learning occurs whenever an entity (individual, organisational unit or complete organisation) predicts the outcome of a situation and observes the actual result. This can only occur if the entity has a mental model of the scenario which they are able to "play forward" to predict the expected outcome. Every prediction/observation results in learning regardless of whether the observed outcomes agrees with the prediction (in which case the learning reinforces the existing model) or disagrees with the prediction (in which case the learning changes the existing model in some way).

This leads to two broad classes of learning:

- Single-loop learning occurs when an observed outcome disagrees slightly with the prediction and the entity "learns" by making some small tweaks to their mental model in order to optimize it. The entity believes that their mental model is broadly correct, but needs to be "fine-tuned" in order to give better results in the future.
- Double-loop learning occurs when an observed outcome disagrees wildly with the prediction, and the entity has to completely discard their mental model and form a new idea of cause and effect for these situations. Double-loop learning takes much more time and mental effort than single-loop learning.

Neither type of learning is inherently "better" than the other. Double-loop learning provides much more insight into the different scenarios, but takes more resources. It can be argued that the role of management is to minimise the need for double-loop learning so that entities can concentrate on their business functions:

> ***"Single and double-loop learning are required by all organisations. One might say that one of the features of organisations as social technology is to decompose double-loop issues into single-loop issues ..."*** -- Chris Argyris (1999)

It is easy to see examples of single-loop and double-loop learning in information security. We can see the effects of single-loop learning in situations where a receptionist, after making a decision to allow an unusual character entry to a secure building, vows to be more stringent in checking identification documents in future. We can see the effects of double-loop learning in situations where a network manager sees an increase in information loss and realises that perimeter network defences are insufficient to prevent malicious activity that originates from within the network.

Excessive amounts of double-loop learning will reduce the effectiveness of an organisation. An organisation simply cannot provide a useful function if the majority of its employees are spending all their time attempting to use every learning opportunity to re-write their mental map of reality! Thus, organisations unconsciously develop a series of organisational defences which are designed to prevent excessive amounts of double-loop learning. Unfortunately, these organisational defences often manifest themselves as actions which resist learning and change. It is against these organisational defences that the ISMS has to fight when attempting to impose useful new security practices within an organisation.

After observing a large number of different business situations, Argyris and Schön concluded that all entities (individuals, organisational units or complete organisations) are governed by the same set of motivating factors, which they called Model I Action Logic. These motivating factors state that an entity will always:

- strive to be in unilateral control,
- act to maximise winning and minimise losing,
- minimise expression of negative feelings (especially when this could cause embarrassment),
- be rational (in the sense of setting personal goals and measuring success against these goals).

These motivating factors cannot be the most efficient possible for an organisation. Consider a situation where a task has to be completed jointly by two departments. According to the Model I Action Logics, both departments will strive to be in unilateral control. However, since this is impossible, it is likely that one department will take control over the majority of the task (having "won" the battle for unilateral control) while the other department retreats from the task in silence (minimising their losses and their expression of negative feelings towards the other department). Since the task required joint control in order to be effectively completed, it is likely that the task will not be successfully resolved, thus seemingly justifying the decision of the second department to withdraw from the process. Meanwhile, the first department is likely to begin to silently blame the second department for their lack of involvement (minimising their loss and expression of negative feeling). The use of Model I Action Logics has caused the task to be poorly implemented and caused a breakdown in trust between departments which need to work together.

Model I Action Logics lead to a series of unproductive organisational defences.

Model I Action Logics lead to a predictable series of unproductive organisational defences. The most prevalent and destructive of these are easing in, mixed messages, and bypass behaviour:

- Easing In occurs in a confrontation between two entities, when one entity attempts to reduce the amount of embarrassment that another entity will feel by falsely amplifying success of certain irrelevant aspects of a project, before discussing the overall failure of that project. In projects that have truly achieved a mixture of success and failure, easing in is often considered very sound management practice, as it ensures that all parties acknowledge the success of a project before considering how the project might be improved. However, this strategy only works if there are aspects of the project which are truly praiseworthy. False praise is easily detected and only serves to make individuals feel more embarrassed about their performance, which leads to a worsening of relations between both entities.
- Mixed Messages occur when an entity gives contradictory instructions or makes statements that are not consistent with their actions. For example, an entity might claim to be handing over all managerial aspects of a project to another entity, while asking for daily reports and weekly meetings on the project. Mixed messages leave entities without a clear vision of their own capacities, responsibilities and liabilities.
- Bypass Behaviour occurs when an entity deliberately avoids a procedure or policy (bypasses the procedure) and refuses to acknowledge any procedures that might force them to undertake it (makes the bypass behaviour undiscussable). This leaves the organisation with two choices: they can ignore the bypass behaviour and make other arrangements or they can force the entity to implement the procedure and cause great embarrassment to all parties involved.

We believe that these kinds of organisational defences are common when implementing formal information security management systems, since we believe that this requires significant double-loop learning on the part of the entire organisation. Indeed, returning to the idea that a formal ISMS moves through

ORGANISATIONAL DEFENCES IN INFORMATION SECURITY

We can easily imagine situations in which organisational defences can inhibit the development of good information security practices across the organisation. We know that the majority of formal ISMSs are initially implemented by the meta-ISMS; however, a number of the security functions are better handled by the operational-ISMS (such as security training). Hence, there comes a point where the meta-ISMS must relinquish control of certain security functions to the operational-ISMS. This attacks the Model I Action Logics of both the meta-ISMS (which must give up unilateral control over the formal ISMS) and the operational-ISMS (which, by taking on extra security responsibilities, opens itself up to opportunities to "lose").

Therefore organisational defences could manifest themselves on either side of the operational divide. The meta-ISMS may attempt to convince the operational-ISMS to take responsibility by suggesting that their previous security work with the organisation's external auditors has been excellent and explaining that they appear to be the most appropriate entity to take over new security responsibilities (Easing In). The meta-ISMS might insist that operational-ISMS take full control of the new security functions, as long as they check operations with the meta-ISMS for compliance purposes (Mixed Messages). The operational-ISMS might claim that they would like to take over the new security responsibilities even though they have limited resources and thus may not be able to spend too much time dealing with them (Mixed Messages). The transfer of security responsibilities now occurs in a scenario in which neither party is sure of their responsibilities and liabilities.

If the new security functionalities prove too difficult and/or onerous to be implemented correctly by the operational-ISMS then the procedures may be ignored. In such situations, it is unlikely that the operational-ISMS would want to discuss their failings (Bypass Behaviour). We now have a situation in which the security function is not implemented correctly, cannot be easily corrected, and may threaten the organisation's practical security and compliance portfolio. Organisational defences have managed to destroy a working security function and threaten regulatory compliance.

six distinct stages, we would expect to encounter organisational defences many times as the ISMS matures and evolves (from both the information security team and the rest of the organisation). Moreover, we would expect that evidence of these organisational defences would be apparent in the minutes and policy documents of the organisation.

What can be done to lower organisational defences? The question is not an easy one.

So what can be done to lower these organisational defences? The question is not an easy one to solve. These defences aren't limited to a distrust of new information security policies and procedures, but demonstrate the genuine difficulty in forcing entities to undertake double-loop learning. They do not bow to evidence or persistence, but need to be conquered at a personal level. Argyris has often claimed that double-loop learning skills can be learnt, but that to achieve the ability to consistently overcome one's own organisational defences is about as hard as learning to play a consistently good tennis game.

Argyris and Schön propose training employees to reject Model I Action Logics in favour of Model II Action Logics (which are purely evidence-based and force an organisation to implement any idea for which an employee can present sufficiently compelling evidence). Moving to an evidence-based system is meant to eliminate any embarrassment and prevent any entity taking unilateral control of a project.

However, the approach is designed to be used in situations where all employees have the same level of education and it's unclear whether this approach is useful for information security professionals. By demanding evidence to back-up any proposal, the information security team still remains in unilateral control of all information security decisions simply by virtue of the fact that other employees are unlikely to have the expertise to gather significant evidence. The security team may also experience a level of embarrassment if an "untrained" employee puts forward an idea which is better than the security teams' own proposals.

We believe that further research is required to determine the most effective way to encourage organisations to learn to handle information security and we intend to provide some of that research.

Further reading:

E. Coles-Kemp.
The Anatomy of an Information Security Management System. PhD Thesis, 2008.

S. von Solms.
Information Security Governance – Compliance Management vs. Operational Management. Computers & Security, 24(6), pp. 408-412, 2006.

C. Argyris and D. Schön.
Organisational Learning: A Theory of Action Perspective. 1978.

CYBER SECURITY CHALLENGE
By Allan Tomlinson

> Dr Allan Tomlinson is a Lecturer in the ISG.

The UK Cyber Security Challenge, launched in 2010, is a series of national competitions designed to encourage talented professionals into joining the UK IT security industry. Royal Holloway was a founding member of the Cyber Security Challenge consortium back in 2009, and contributed to its efforts throughout 2010. I served on the competitions committee who devised the competitions and set the assessment criteria.

This work came to its fruition in March 2011 at the first Cyber Security National Awards ceremony held at the At-Bristol Science Centre. There are three competitions: a security treasure hunt; network defence challenge; and a digital forensics challenge. At the awards ceremony the ISG were delighted to present prizes to Alistair Senior, Tony Shannon, Channon Powell and Richard Hodgson, the winners of the defence security challenge. The four winners will be given an opportunity to attend their choice of week-long block mode masters courses in order to enhance their knowledge of specific areas of information security.

Prior to the awards ceremony there was a “masterclass” for the winners of each competition and a final challenge to select an overall winner. The overall winner of the 2011 challenge was postman Dan Summers from Wakefield and the runner up was Stuart Rennie, a 17-year-old college student from Cambridgeshire. The Keynote speaker at the main awards ceremony was the Rt. Hon Baroness Pauline Neville-Jones, the minister for cyber security.

The ISG plans to continue its support for the Cyber Security Challenge. Keith Martin, Director of the ISG, explained why we are backing the Challenge: “Information security has long ceased to be a concern only of select IT professionals and is now something that wider society needs to be critically aware of. Royal Holloway has worked hard over the last 20 years to increase this awareness through our information security education programmes. The Cyber Security Challenge is both an imaginative and extremely exciting way of taking this message to an even broader community”.

ISG NEWSLETTER 10/11 CONTRIBUTORS

PICTURE CREDITS
Page 08: by Bhavin Desai.
Page 05 (top) / **24** (top):
by Tristan Findley, Alopex Productions:
http://www.alopexproductions.co.uk.
Page 13: by Garrett Coakley
http://www.flickr.com/photos/garrettc/
Page 17: Viet Pham (bottom)
Page 19: by Elizabeth Quaglia.

CONTACT INFORMATION:

For further information about the Information Security Group, please contact:

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

T: +44 (0)1784 443101
F: +44 (0)1784 430766
E: isg@rhul.ac.uk
W: www.isg.rhul.ac.uk