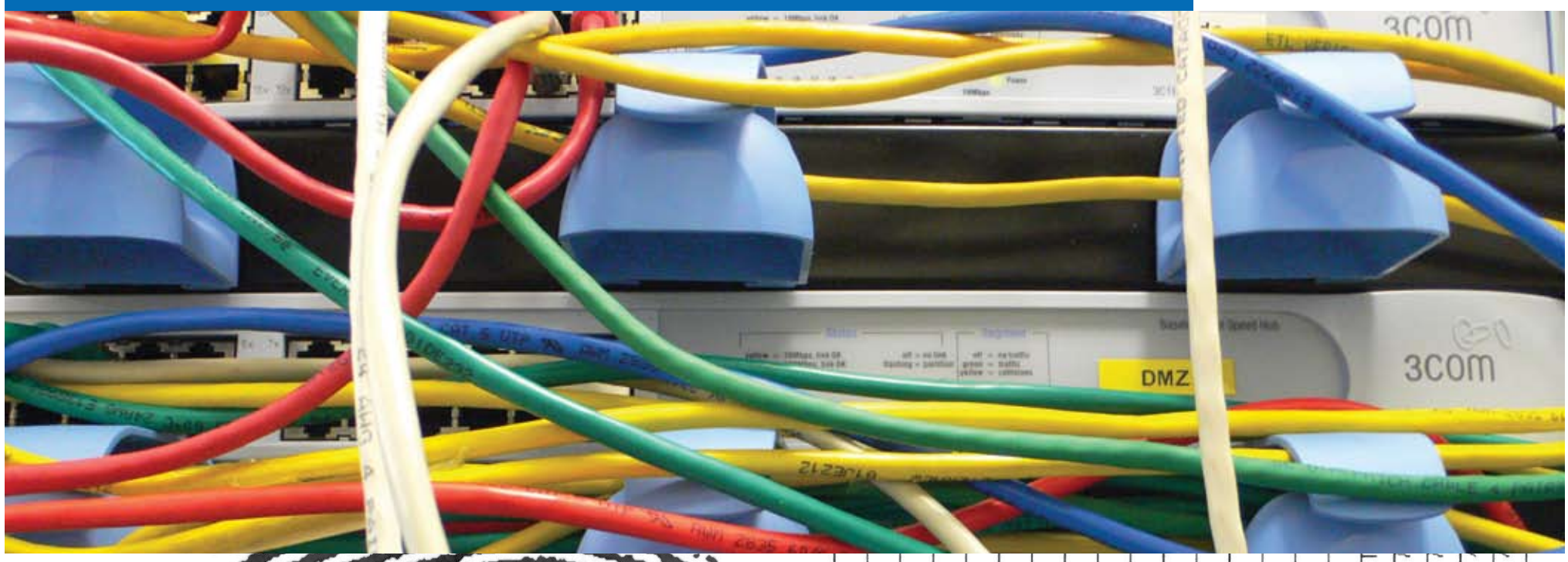
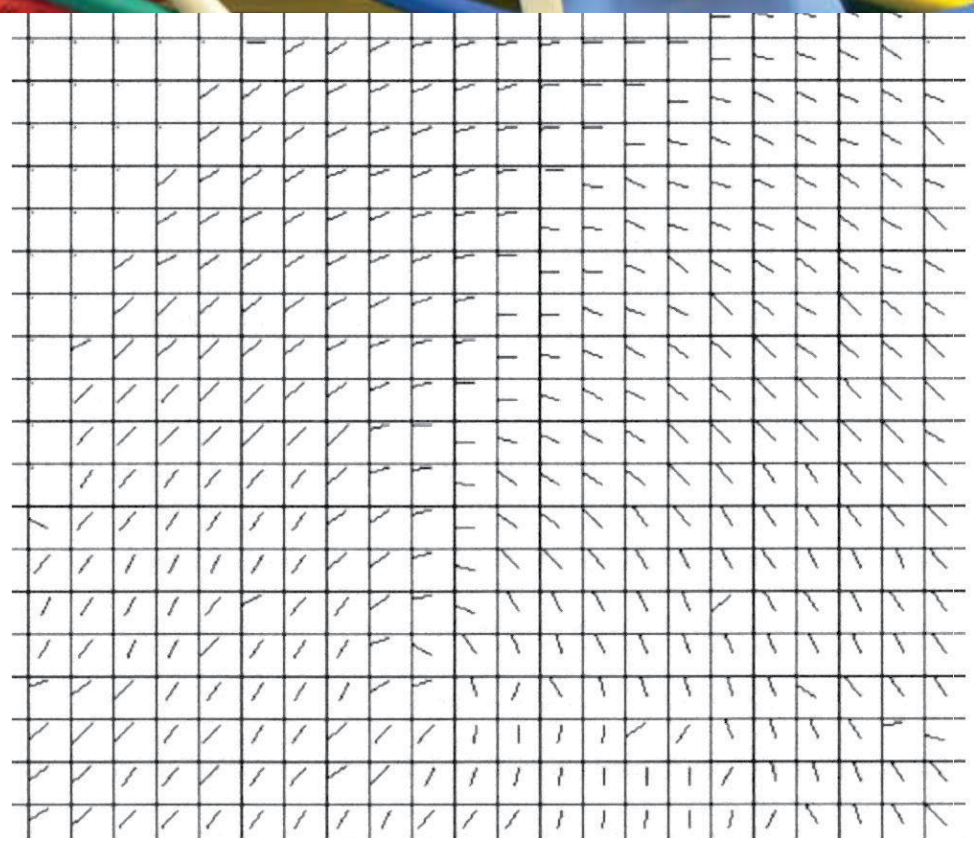
Information Security Group

Review 07/08





Royal Holloway
University of London

CONTENTS

Three words about the MSc

Compulsive, addictive, fun

Ken Jacobie
MSc Student 2007/08

LETTER FROM THE ISG DIRECTOR

This is the second annual review newsletter produced by the Information Security Group at Royal Holloway, University of London. In it, we provide a round-up of some of our recent activities and hope that it gives a flavour of what has been going on over the past year.

This year is a very exciting one for the ISG because on the 21st – 23rd July 2008 we are holding a special conference to welcome back to Royal Holloway many of the alumni who have graduated from the MSc in Information Security. This MSc programme was one of the first such programmes in the world and has seen over 1000 graduates since its launch in 1992. Alumni from the programme have gone on to great, varied and interesting careers throughout the world and it brings us great pleasure that many will be returning to Royal Holloway for this event. For more details, see page 6.

Just for fun, we asked members of this year's cohort of MSc Information Security students to provide us with three words that they associate with their experience of studying at Royal Holloway (either on campus or online). Throughout this newsletter you will see some of the responses. These give a rather interesting snapshot of what studying for an MSc is really like.

We hope that you enjoy the newsletter and are inspired to get involved with our activities. If you would like more information about any of the articles featured here or any of the ISG activities, then please do not hesitate to get in touch.

Professor Peter Wild

Three words about the MSc

Interesting, rollercoaster, challenging

Sylvain Martinez
MSc Student 2007/08

TEACHING INFORMATION SECURITY TO UNDERGRADUATES

The Information Security Group has recently established a new undergraduate degree with the Computer Science Department. This programme, a BSc Computer Science (Information Security), puts a new and highly relevant twist on a traditional Computer Science degree, reflecting the ever-growing importance of security in IT.

This innovative programme covers the best ways of protecting businesses, governments and individuals from threats to their information and information processing resources. Students will study cryptography, security of software and architectures for trusted computer systems under the supervision of a leading researcher in information security, alongside the fundamentals of computer science including Java programming, databases and networks.

Courses in Information Security have become a common component of Computer Science degree programmes, and this new joint degree is a further indication of the growing importance of security in computing. Software engineers need to understand the pitfalls of writing flawed code, system designers need to consider security when designing and integrating systems and users need to be aware of security risks. It is thus vital that security awareness and understanding is provided to all Computer Science graduates.

Of course, the fact that security is now a "mainstream" topic may raise concerns about the value of specialist qualifications in security. However, in our view, there is plenty of room for both mainstream and specialist offerings. Everyone working in IT needs to be aware of, and have a basic understanding of, security issues but this does not mean that the general education provided to a graduate will equip every graduate to be a security specialist. We foresee mainstream and specialist education developing in parallel; indeed, the rapidly growing provision of security education at both undergraduate and postgraduate level suggests this view is shared by the educational world as a whole. We in the ISG are committed to continuing to develop the widest possible range of educational opportunities in the security field and we welcome your views on both existing and possible novel degree programmes.

More information is available here:
www.cs.rhul.ac.uk

NEWS IN BRIEF

- **Stephen Wolthusen has been appointed to the prestigious position of Editor-in-Chief of the well-known Elsevier IT security technical journal, Computers and Security. This is the official journal of Technical Committee 11 (computer security) of the International Federation of Information Processing. Stephen also presented a keynote talk on modelling aspects of tactical network security at the IEEE International Conference on Computational Intelligence and Security 2007 in Harbin, China.**
- **Allan Tomlinson has been awarded a research grant of just under £300,000 for a Mobile Virtual Centre of Excellence security research project. Mobile VCE is an industry/academia consortium involving seven universities and around 18 industrial partners. The three-year research project also involves the Universities of Southampton and Strathclyde. It will look at privacy in social networks and aims to provide a secure professional social network.**
- **Keith Martin delivered keynote presentations at the 2007 British Combinatorial Conference at Reading (on mathematical modelling of cryptographic key establishment); the Flemish Academy of Sciences, and the 2007 Cryptography and Network Security Conference in Singapore (both on research on secret sharing).**

PRACTICE MAKES PERFECT: NEW SECURITY LABORATORIES

The ISG has launched two new laboratories to enable students to gain vital hands-on experience of information security techniques within safe environments.

The Virtual Penetration Testing Laboratory opened in 2007 and was jointly developed by Matta Consulting. It consists of 40 clients, which allow 40 students at a time to access the laboratory resources. Within the Virtual Lab, students can connect to an "attack machine" that is connected to a network of servers which have known vulnerabilities. All connections from the Virtual Lab to the outside are prohibited. "The advantages of this setup are security, since we have controlled access to the laboratory via a firewall, and maintenance, as all platforms in the laboratory are rolled back to a known state on a regular basis," comments Allan Tomlinson, who was responsible for overseeing the creation of the Virtual Lab. "This allows students to experiment in a safe environment without having to worry about internal or external damage to machines".

Students have free access at all times of the day, however structured penetration testing activities, supervised by tutors, are also run throughout the year. These have ranged from simple network discovery exercises through to running exploits. Future plans include "war games" and "capture the flag" exercises.

Nick Baskett, Managing Director of Matta Consulting, is very pleased with the results of their involvement: "Matta was excited about working with Royal Holloway to put together essentially the first practical Penetration Testing Lab in the UK. We have been building vulnerable networks for testing purposes for many years and this was an opportunity to deploy the concept in a university. Royal Holloway has been very forward-thinking in its ambition to provide students with a more practical and hands-on approach to learning about security. All the way through the project, the staff at Royal Holloway were great to work with. Their enthusiasm was contagious and Matta thoroughly enjoyed being a part of this ground-breaking project".

In addition to the Virtual Lab, the ISG has also opened a new Security Laboratory, which is a physical space, part of which was once familiar to older friends of the ISG as "Chez's office"! This facility is available to both research staff and students for advanced penetration testing and security research. The Security Lab has no external access whatsoever (wired or wireless).

The new laboratories are all part of a wider push to feature more of a "hands on" experience for information security masters and research students. Even courses with a strong theoretical basis, such as the introductory cryptography module, hold laboratory classes. Keith Martin, who leads this module, was originally sceptical that students would benefit from seeing something being encrypted, however was quickly won over when he saw the results of allowing students access to structured activities based on the freeware CrypTool simulator. "I got a genuine kick from seeing some of the concepts on the course being demonstrated using CrypTool's simple interface," says Keith. "There's no more excuses for students not knowing the effects of error propagation in block cipher modes of operation, when they are so easily demonstrated using CrypTool!"

MANET RESEARCH UPDATE

The ISG is actively engaged in research in the emerging areas of mobile ad hoc networks and sensor networks. Both paradigms assume resource constrained nodes communicating over a shared wireless medium. However, unlike cellular networks, ad hoc and sensor networks do not depend on the availability of a centralised communication infra-structure. This lack of infrastructure, idiosyncrasies in the wireless channel and node mobility, create many challenging problems in the design of security architectures for such environments.

Whilst on the face of it, these characteristics may appear to the detriment of many network designs, these infrastructureless networking paradigms are suitable for many applications, particularly in a military or emergency response setting.

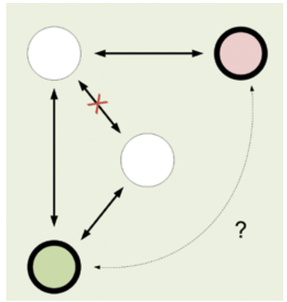
MANETs are attractive in military settings as they may form dynamically in response to some immediate operational requirement. However, with this immediacy comes the problem that pre-established agreements dictating the terms in which nodes will collaborate may not be fully specified.

The ISG is involved in a joint UK Ministry of Defence/United States Department of Defense consortium of transatlantic industry and university partners, the International Technology Alliance (ITA). Part of our research in the ITA is the development and analysis of lightweight and adaptive security architectures and infrastructures that facilitate the formation of (and operations by) secure, flexible "Communities of Interest".

According to Shane Balfe, who is employed as a researcher on this project: "A focus area in this project is dynamic trust establishment among various members of a Community of Interest by taking into account both positive and negative evidence. In addition, we will explore alternatives to traditional public key infrastructures that are inherently more energy and bandwidth efficient and that promise to provide natural support for coalition operations".

Cryptographic key management in sensor networks is the focus of another project group within the ISG. The wide range of potential commer-cial, scientific, humanitarian or military applications of sensor networks means that in practice there is a need for sensor networks with greatly varying properties. Dr Maura Paterson is employed on this three-year EPSRC-funded project: "One area that we have been exploring this year has been the development of efficient ways of assigning cryptographic keys in specific classes of sensor networks. Another strand of research has involved the investigation of effective methods of updating keys in a sensor network environment". This project has involved collabor-ation with researchers from the Technion – Israel Institute of Technology and the University of Waterloo in Canada.

In addition to its involvement in these specific projects, the ISG also has a MANET research group involving academics, research assistants and PhD students, who meet on a weekly basis to discuss significant issues and recent results in the field of ad hoc networks.



Three words about the MSc

Worth the trouble

Gaith Taha
MSc Student 2007/08

STAFF PROFILE: LIZZIE COLES-KEMP

You are the newest member of staff but you have a long association with the ISG, don't you?
I first became involved with the ISG 15 years ago when one of Fred Piper's PhD students contacted me. I was working just down the road from Royal Holloway as a software engineer for a Swedish software house that developed UNIX access control products and the PhD student wanted more details on the authentication protocols. The relationship with the ISG grew from there and I think the access control product (BoKS) featured in one or two early MSc projects.

In 1997, I changed from a technical security focus to a management one when I became Information Security Officer at the British Council. I also decided to study the MSc in Information Security at Royal Holloway at the same time. After the MSc, I opted to continue studying by commencing a PhD in information security management. At the time this wasn't an area of research interest to the ISG so I chose to go to King's College, London.

I suspect that the ISG and I might have drifted apart but for the fact that, in 2000, Keith Martin asked me to do a lecture on VPNs on the then MSc Secure Electronic Commerce. Keith also introduced me to the distance learning MSc programme which was in early development. I spent the next five years producing two children, continuing my part-time PhD, teaching network security, working as a lead assessor to security management standards (ISO 27001 and tScheme) and moonlighting as a distance learning tutor… until I finally joined the ISG as a lecturer in July 2007.

In addition to security management research, my role is to lecture in security and identity management on a Biomedical Informatics BSc at St. George's Hospital, Tooting. This course runs under the South West London Academic Network, of which Royal Holloway is a member.

The thing that makes me laugh the most is that at school I failed my Maths 'O' level four times (in descending order: I started with a D and "progressed" to an X) and although I managed to get my Maths 'O' level 10 years later (with an A), I am still not in the slightest bit a mathematician and yet here I am in a Mathematics Department!

What aspects of information security are you most interested in?
I am interested in how organisations and individuals (both human and non-human) manage security. My particular interest is organic and nomadic organisations and how security management works in these environments. My PhD is about the architecture of information security management systems and how organisational factors change their design. In my research, it is the organic, dynamic organisations that I have found to be the most interesting as the security management design has to be extremely elegant and accurate in order to preserve the dynamic nature of the environment.

I am also interested in how different stakeholders (both human and non-human) measure, assess, express and visualise security. My undergraduate degree was in Scandinavian Studies and Linguistics and I have always had a huge interest in language and communication. I am fascinated by the language used to express information security, and how restrictive it is, and look forward to spending more time exploring the implications of using alternative methods of expressing information security concepts.

My professional and research interests are one and the same. Whether I am auditing, researching, running a company, in the supermarket with my kids, I always do the same thing: I teach. I come from a long line of Methodist lay preachers and teachers – I can remember "teaching" my first class at five years old when I was in my Mum's nursery classroom and doing some kind of teaching with the blackboard! So all my research interests have been honed in the organisations that I have worked with and I am always humbled by the huge interest that all my auditing clients show in my research progress and the enthusiasm they have for engaging with whatever ideas I am currently working on.

Some people suggest that the only way to learn about information security management is actually to manage information security (for a business). What has an academic approach to the subject got to offer practitioners?
I don't really understand this argument. It's true of course that many of us only really understand how something works when we experience it or work directly with it. This is true for many subjects. However academic study in security management offers the chance to step back from the day to day, reflect on the security management patterns and structures and develop some theories as to how you might better manage information security in particular environments. These theories are only theories but they are based on rigorous thought, they have been tested and measured and they offer insight which might be helpful to some.

When I started my PhD in 2000, I was struck by how little academic literature had been written about security management. When I was a security manager at the British Council I can remember being frustrated by security management methodologies that sometimes worked and sometimes didn't for seemingly no good reason – risk assessment was the biggest culprit. I started my PhD because I was so annoyed with not being able to find out from others what motivated risk assessment methodology selection and the organisational factors that impacted how a risk assessment methodology was deployed.

Eight years later, I am just completing my write-up. Whilst there are a few academic writers in this area (for example, Dhillon, Backhouse, Sasse, Schneier), there is still very little security management academic literature – so I have spent eight years on raiding parties into 1970s' management science literature, literature on environ-mental governance and literature on organisational theory. What strikes me is that the insights I have made by reading this literature have equally been interesting, and sometimes helpful, to the organisations with whom I work.

In short, my view is that academic study doesn't offer management solutions but it does help to offer some explanation and, at times, promote a deeper understanding.

Why have you personally chosen to work in an academic environment?
Partly because I wanted the freedom to research more topics related to security management and partly because I wanted to make it possible for others to research security management. It was difficult for me to find a PhD supervisor who would take on a security management topic. Eight years later, it isn't much easier. So my hope is that in some small way I can contribute to security management research by providing a few research opportunities for others. I also believe in what I do and I hope that some of the material I produce will help others in their work.

One of the most rewarding aspects about designing organisational processes is that when you get them right it not only makes a process more efficient, it also makes other peoples' lives easier and less stressful. Above all, I think it's fun to learn and I think it's fun to help other people learn.

What has your experience been of teaching information security students online (on the distance learning programme)?
I'm not sure it's really teaching; it's more tutoring and facilitating. The students are taught by reading the course material but the interaction comes with the tutoring to guide the students through the material. The tutoring takes place using seminars and online discussion forums. I enjoy online tutoring because the communication is so direct between the student and the tutor. As a tutor, you are evaluated on how well you deliver and how consistently you deliver. This evaluation takes place one to one, each time you communicate. I think there is nothing "distant" about distance learning. It's a very direct, intense teaching dialogue. It's a marvellous play area where you can experiment dynamically with new ideas and add new tweaks to a course.

The danger is, however, that experimen-tation can create a situation where the students and tutors are slightly overloaded. I came across this problem myself on the first year that I provided online support for the campus Security Management module. I have worked hard with Peter Wild to build a more elegant online support model in this module and, in my view, what we produced is a really neat example of a balanced use technology to support a lecture course.

Can you tell us more about how you have run teaching activities online that are based on practical scenarios?
As I said before, most of us learn best by doing. So, in the distance learning module that I run (Secure Electronic Commerce and Other Applications), I set up a number of online seminars that take scenarios and get the students to explore the material through those scenarios using role play, eye witness accounts, online diaries and so on.
For example, we run a seminar on the Buncefield Oil Depot fire exploring particular uses of the TETRA radio application in this context. It is a demanding way to learn but it does help many students get inside the online material and provides a lens through which to view the academic concepts and make them less abstract.

Describe your ideal day in the office...
To be honest, any day when I am not completely stressed out trying to meet deadlines. When I worked for a Swedish software house as a software engineer, I ended up running the UK subsidiary. By the time I was 30, I had been inside quite a few blue chip board rooms and run some fairly large, high-profile software deployment projects. So I know about pressure and about deadlines. I also know about working in projects with very little margin for error. But anyone who thinks academia is a soft option should think again in my opinion. The pressure I am under as an academic is much more extreme than anything I have experienced in industry.
I am not really sure why, although I suspect it is partly to do with working in a reasonably new research area and being the new kid on the block. It's just as well that I love my subject, like my colleagues and am clear about the benefits of being here!

Pictured: The 18th HP Day was held at the Windsor Building, Royal Holloway

HP DAY: The 18th Annual HP Day: 17th December 2007

The 18th annual HP Day event took place in the new Windsor Auditorium at Royal Holloway on 17th December 2007, attended by over 100 guests from the industrial and academic information security communities. The generous sponsorship of HP has brought many extremely distinguished speakers from around the world to this event over the years, and 2007 was no exception.

First up was Yan Noblot from Atos Origin UK, who is IT Security Manager for the Olympic Games and Major Events. Yan presented a fascinating insight into the challenges of providing a secure communications infrastructure for the Olympic Games. Atos Origin is the official Information Technology Partner for the Olympic Games. They have provided the information technology infrastructure for all recent games and will still be in the hot seat for London 2012.

For many of the audience, this was probably the first time that they had considered the enormous complexities of providing information security in an environment where most employees are temporary (many unpaid volunteers) yet where the smallest failures in IT infrastructure have the potential to be noticed by the entire world. One surprising issue was the importance of securing printers, since all games results only become official once the supervising Olympic recorder signs a hard copy of the results of an event. Years and years of preparation are needed for what is, essentially, only a running environment which lasts for two weeks. Just as for the athletes themselves, there are no second chances for the IT security architects.

Susan Landau, Distinguished Engineer at Sun Microsystems Lab, brought attendees up to date with some of the recent legislation in the United States concerning communication interception and data privacy in her presentation, "Keep calm and carry on". Susan brought an interesting personal perspective to the wider debate on the use of wiretapping, as she is co-author of the well-known book, *Privacy on the Line: The Politics of Wiretapping and Encryption*. She raised several concerns about both the necessity and validity of wiretapping in an increasingly internationally networked world.

Chris Potter, PricewaterhouseCoopers, presented his own personal take on the impact of the Sarbanes-Oxley (SOX) legislation. Speaking as an auditor, Chris claimed that SOX had many benefits, not the least being improved appreciation of information security at senior management levels and better communication links between auditors and senior management. His comments provoked healthy debate among certain members of the audience, many of whom had experiences of SOX from the "other side" of the process.

During the catering breaks, attendees were able to browse a series of posters prepared by HP and ISG researchers, showcasing some of the recent work from both groups.

Event co-ordinator Professor Kenny Paterson summed up the day: "The HP colloquium has always been a great opportunity for networking, meeting old friends and making new ones, and of course to hear some leading lights in the field giving their views. This year's 18th colloquium was no exception and we are very grateful to HP for their continued sponsorship of the event".

Martin Sadler from HP Labs is already looking forward to the 2008 event: "This year will be the 19th year that HP Labs has sponsored the HP Day at Royal Holloway. We believe it to be a key event that aims to be both educational and informative, whilst providing a forum to discuss and exchange ideas with other security professionals in both business and research across Europe".

A WELCOME TO ALUMNI STUDENTS

Graduates from Royal Holloway's security masters programmes from every year since the ISG's launch in 1992 are invited back to Royal Holloway this summer to take part in an Alumni Conference on July 21st – 23rd 2008.

The aims of this event are to have a high-quality information security conference; to rekindle fond memories of time spent at Royal Holloway; to have a great networking and social event, and to be able to share knowledge and the latest news with past graduates.

Whitfield Diffie, Visiting Professor at the ISG and one of the pioneers of public-key cryptography, will be delivering the keynote address at the conference. Other invited speakers are to be confirmed. The rest of the conference programme will include short papers and personal updates by ISG graduates.

If you are a past graduate of the ISG masters programmes and wish to attend this event, then please register at the Alumni Conference website (see below). Even if you do not wish to attend, it will help if alumni complete the application form so that the ISG can update your contact details. Please note that there are limits on the number of possible attendees and that places will be given on a 'first come, first served' basis. To avoid disappointment, we recommend registering as soon as possible.

Attendees will need to pay their own travel and accommodation costs and there is a £25 fee for attending to cover organisational expenses. Those wishing to stay on campus should indicate this on their application as there is limited accommodation available.

We will be delighted to welcome back as many alumni as possible and look forward to this lively summer event.

More details: www.isg.rhul.ac.uk/alumniconference

Three words about the MSc

Security, security, security

Rostom Zouaghi
MSc Student 2007/08

PART-TIME PhD RESEARCH: JUGGLING WORK, STUDY AND PLAY

Studying for a PhD part-time is certainly not an easy option but it can be a challenging and rewarding one. To get an idea of how to survive the experience, we speak to **Bob Bowden**, who holds down a full-time job at BT while conducting his PhD research. Bob is a graduate of Royal Holloway's distance learning MSc in Information Security.

Tell us a little bit about the PhD topic that are you researching
My research is focusing on denial of service attacks, more specifically DDoS attacks and how they can be mitigated against. Certainly coming into this from my MSc (my dissertation was on the same subject), I felt that there are a lot of good solutions to the DoS and DDoS problems, all with their own advantages. Unfortunately, they each have their pitfalls as well, and so none are the panacea to the DDoS problem. By continuing my research in this area, I am trying to find out what the underlying problems are that researchers are trying to address and then looking at what may be done to offer a more rounded solution to the problem.

Are there potential benefits to your employer of the research work?
There are certainly some benefits. I work for BT, and obviously, as a major ISP, any potential solution to the DDoS problem will be of interest to the business. In addition to this, I actually work within an area of BT where we provide some external consulting to a variety of customers, and so being able to go to those customers and speak authoritatively on the subject of DDoS is also of benefit to the business.

That said, it is important to set the expectations of the business as well. It is unlikely that anyone studying a PhD will find the complete solution to whichever problem they are investigating. However, I will hopefully help to advance the field and, in the process, learn quite a bit about how to research problems and their associated solutions. To my mind, it is these transferable research skills that are of much greater benefit to my employer, since these skills are useful throughout my working life.

How are you finding the work / PhD / rest-of-life balance?
This is certainly the tricky bit. Because of the nature of a PhD, and the lack of immediate deadlines, it can be very easy to give the PhD research the lowest priority. This is especially the case when, like me, you are remote from the university campus. It is basic human nature to prioritise the thing that is right in front of you ahead of those things that appear remote.

However, I like to think that I am becoming more disciplined about this now. I treat the PhD research as another job, even to the point of turning off my work phone when studying for my PhD and coming to an agreement with my partner that study time is time not to be interrupted. Doing this has certainly helped and has meant that I can now realistically set myself a target of completing at least 20 PhD hours a week. As a result, I am starting to feel like I am making real progress.

It took me a while to get into this groove and it is important to find a sustainable balance. After all, a PhD takes at least four years to complete part-time, so whatever regimen that I set myself has to be sustainable for at least that length of time. If it wasn't for the patience and support that my partner offers me, I don't think that this would be anywhere near as easy, or perhaps even possible. She certainly helps an awful lot, even to the point of reviewing my written English.

How does studying at a distance for a PhD vary from studying at a distance for an MSc?
The MSc was certainly a lot easier to be disciplined about. I chose which modules to study for the year, and then things such as the seminar schedule gave me a framework to work within. As long as I had completed the allotted number of units before the seminar began, I was able to proceed at my own pace and stay on track.

My PhD does not have the same deadlines and so I have to manage my time better, especially in light of things that appear much more urgent happening around me. That said, the PhD is in many ways much more interesting, as I tend to set my own study aims and objectives, and I research areas which are of personal interest (after all, investigating a topic you loathe would be almost impossible). This means that I find myself getting quite carried away in the research that I am doing, and suddenly lose days to a particular piece of work!

One thing that is really different is the feeling of isolation. When studying for the MSc, I had access to discussion forums, seminars, a file sharing system, a mailing list and so on. If I ever felt a little bit stuck, lost or demotivated, I always had someone nearby who could reassure me that they were going through the same thing. I find the PhD far more isolating, although of course I have a supervisor who helps to keep me on track and focused.

Do you feel that you are missing out on anything by studying part-time (rather than full-time) for a PhD?
In some respects. By not being on campus, I end up not having much contact (if any) with other people going through the same thing. This can be quite hard. Luckily, a couple of other MSc graduates also decided to go on to do PhDs, so we do occasionally exchange emails and catch up, and this certainly helps to remove this feeling of isolation. Colleagues and friends all ask how it is going from time to time but I have learnt rather quickly that, in general, they would rather not know the detailed answer to that question unless they are having trouble sleeping!

What's surprised you most so far (pleasantly and unpleasantly)?
The most unpleasant surprise was actually borne from a comment that a colleague of mine made. He said that being accepted for a PhD was the intelligence test and undertaking it was more a test of endurance. I took this comment with a pinch of salt at the time, especially as I thought that acceptance couldn't be an intelligence test, or I wouldn't have got through! However, now that I have been doing this for a year, I can see what he means. I certainly underestimated the amount of mental discipline required to continue to research in an isolated environment, especially for someone as disorganised as I am. However, as I get further into it, my organisational skills are improving and it is becoming easier and easier to focus. Keeping in mind the end goal certainly helps.

I was very pleasantly surprised the first time I found out that someone had considered the same ideas that I had, strange as this might sound. I remember that, when I was doing my initial background reading, I came up with a couple of broad ideas on some DDoS mitigations that I would like to look into. On continuing my reading, I found that these ideas had already been looked into by other researchers. In each case, either proposals had been made, or the ideas had been dismissed. I expected that I would feel a little frustrated that someone had "beat me to it" but, instead, I found myself strangely quite satisfied by the knowledge that I was thinking along the same lines as some of the other researchers in this field. This, almost more than anything, made me feel I was moving in the right direction, and certainly gave me the impetus to come up with further ideas.

April 2007

- USA - Bank of America – social security number of employees lost through theft of a laptop
- New Zealand – Inland Revenue – an audit discovered loss of 106 laptops containing customer data
- USA – Dept. of Agriculture – loss of data of 38,000 individuals receiving farm subsidies
- UK – Dept. of Health – data loss of details of hundreds of junior doctors
- USA – New York Special Funds Committee – laptop lost with details of 540,000 individuals

SECURITY STORIES OF THE YEAR

We asked ISG staff for an information security story that had caught their eye in the last 12 months. There was no doubt what the main story was:

JOHN AUSTEN: IS DATA LOSS AN EPIDEMIC?

In November 2007, the Department for Work and Pensions (DWP) disclosed that they had lost computer media containing the details of millions of people who were entitled to child benefit whilst it was in the process of being sent to the National Audit Office. Worse still, those details included personal bank identifiers on claimants.

Despite investigations, at the time of writing this material had not been recovered and nobody knew where it was, or who has access to it. Worse, it was reported that the data was not encrypted. Well, mishaps occur but, in terms of information security, questions arise on precedent and procedure.

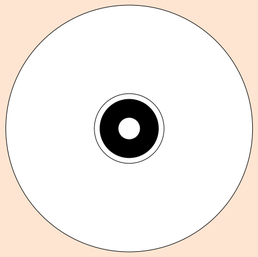
As this was discussed in answer to a parliamentary question, the matter quickly became public knowledge. It became the focus of media attention and left many families with cause for concern regarding the vulnerability of their financial assets. But is this the first time this has happened? Just by looking back six months to April 2007, in reported worldwide incidents, we can see that data loss and disclosure from government departments and large organisations is not something new. Take a look at these:

May 2007

- USA – Louisiana State University – laptop lost with details of 750 students
- USA – Maryland Dept. of Natural Resources – thumb drive lost with details of 1,400 Police and Rangers
- UK – Royal Cornwall Hospital – computer loss with details of 5,000 staff
- USA – Virginia Dept. of the Ageing – hard drive loss, with details of 40,000 people
- UK – Marks & Spencer – laptop loss with details of 26,000 staff on pension plans

November 2007

- UK – HM Revenue & Customs – loss of CD with details of 15,000 pension policy holders

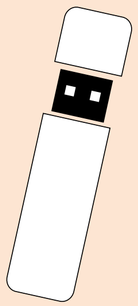


June 2007

- UK – Bank of Scotland – computer disc loss with details of 62,000 customers
- USA – Texas Police – laptop stolen with details of 97,000 employees
- UK – Accountancy firm Moorepay – laptop stolen with details on Prince Charles & his estate
- USA – Bowling Green University – loss of flash drive with details of 18,000 students

October 2007

- UK - HM Revenue & Customs – laptop stolen with financial details of 400 people



July 2007

- USA – Transport Security Administration – loss of hard drive with details of 100,000 employees

... Following the child benefit loss, in January 2008, the Ministry of Defence admitted the theft of a laptop containing details of military personnel. It just never seems to stop…

We do not need to postulate on Descartean Rationalism to understand that despite all the technical advances in information security, it is the basic and fundamental security measures that are being disregarded. Is it a lack of information security policies? Hardly. CESG (the National Technical Authority for Information Assurance) provides guidelines, policies and implements standards across all UK government departments and must be wondering where things are going wrong.

Like so many things it is not the knowing, but the doing, that matters in the end.

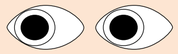
(First published: www.itpro.co.uk/blogs/isg/2008/02/17/is-data-loss-an-epidemic/)

STEPHEN WOLTHUSEN:

Until recently, there has been very limited information on actual information security (cyber) attacks on critical infrastructures, despite consensus that many areas of the critical infrastructure rely more and more heavily on information systems and that many of these systems are not well protected. This all changed when a briefing by T. Donahue (US Central Intelligence Agency) confirmed that there have been successful attacks against electrical utility companies. Details can be found at: www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277.html

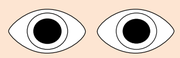
STEVEN GALBRAITH:

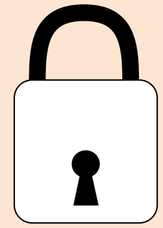
As a mathematical cryptographer, for me the top story of the last 12 months was the complete breaking of SFLASH, a digital signature scheme for resource-constrained devices, by researchers from ENS in France and the Weizmann Institute in Israel. This work was presented at the annual Crypto conference in Santa Barbara. It's a very nice result.



CARLOS CID:

It has to be the classic story of TV presenter Jeremy Clarkson losing money after publishing his bank details in his newspaper column. He was trying to make the case that identify fraud was massively over-hyped and did banking security a massive favour by being caught out so publicly. He fully admitted the error of his ways after a reader used his details to create a £500 direct debit to the charity Diabetes UK. Wonderful! See the story at: http://news.bbc.co.uk/2/hi/entertainment/7174760.stm





CHEZ CIECHANOWICZ:

The biggest story for me was undoubtedly the uncovering of Jerome Kerviel's rogue trading activities, which almost brought the French Société Générale bank to its knees. From a security perspective, there were two incompatible roles involved (ie. back office and front office). Although the trader did not hold both roles simultaneously, knowledge gained from the first role was used to circumvent controls when working in the second role. Although it is unrealistic to explicitly forbid employees to move between incompatible roles, internal controls must take such movements into account.

CHRIS MITCHELL:

The big security story of the year was without doubt the revelation that UK government departments appear to be routinely losing millions of sets of personal data. For me, the biggest shock was not that it was lost but the means by which it was lost. Such data seems to be treated as if it is of no value, with large user databases seemingly routinely stored on notebook PCs, written to CDs, and shipped through the post. One case highlighted to me how far UK government is from security best practice. The fact that a government audit department expected to be given millions of personal records is even more shocking than the fact that the data was shipped through the post unencrypted, and much more data than was needed was provided (and lost). I am still shocked when I think about it.

KEITH MARTIN:

For me, one story that really struck home was the fact that Swiss officials were planning to use quantum cryptography technology to secure the channel between the central ballot-counting station in Geneva and a government data centre. I mean, why? What's wrong with the tried and tested key management that is used on a daily basis to secure the world's financial systems? This seems to be a sophisticated publicity stunt designed to raise the profile of a Swiss firm's technology. It is strikingly bold, and somehow also rather concerning that an important application such as electronic voting should be played with in such a way. http://cwflyris.computerworld.com/t/2191514/89321/83014/2/


IMA International Conference in Cryptography and Coding, Cirencester, UK

NEWS IN BRIEF

- **The ISG is supporting a series of exchange visits with the Taiwan Information Security Centre (TWISC), which is a virtual centre of excellence for information security research in Taiwan. In 2006 and 2007, the ISG provided three staff to speak at the TWISC Information Security Summer School in Taipei and, in February 2008, Professor Fred Piper addressed an International Workshop on Information Security hosted by TWISC. In summer 2007, three TWISC PhD researchers spent several months at the ISG conducting research projects under the supervision of ISG staff. Professor Tzong-Chen Wu, Director of TWISC at the National Taiwan University of Science and Technology, has been a driver behind this collaborative relationship: "The ISG is without doubt the best partner for TWISC in the UK due to its breadth and depth in both research and teaching excellence in information security".**

- **Jason Crampton has been appointed to the editorial board of ACM Transactions on Information and System Security.**

- **Fred Piper has joined the advisory board of the International Multilateral Partnership Against Cyber-Terrorism (IMPACT), a global partnership between governments and the private sector whose goal is "to strengthen the global community of nations against the scourge of cyber threats".**

- **Scarlet Schwiderski-Grosche acted as Assessor for the DTI Technology Programme Spring 2007 Competition. Security-related topics were covered in the Technology Priority Area "Networked Enterprise".**

- **Kenny Paterson has joined the editorial board of the Journal of Cryptology and the series advisory board for Springer's Information Security and Cryptography book series. Kenny has also been busy on the lecture circuit, with invited presentations at workshops on pairing-based cryptography at Queensland University of Technology, the University of Melbourne and a symposium in Heeze, Netherlands, and presentations on provable security at Schloss Dagstuhl, Germany, and the Lighthill Institute of Mathematical Sciences, London. Kenny also delivered sessions at two ECRYPT workshops, the Summer School on Emerging Topics in Cryptographic Design and Cryptanalysis, Samos, Greece (on pairing-based cryptography) and the International Workshop on Cryptographic Protocols, Bertinoro, Italy (on identity-based authenticated key exchange protocols).**

- **Carlos Cid has been appointed to the editorial board of the Designs, Codes and Cryptography journal, which publishes research on mathematical aspects of cryptography.**

- **Geraint Price delivered a keynote presentation at the Annual Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS 2007) on the extent to which security services could potentially be provided with no, or weakened, underlying authentication primitives.**

- **Chris Mitchell has been appointed to the editorial board of the International Journal of Information Security (published by Springer). He has also been awarded an Erskine Visiting Fellowship at the University of Canterbury in Christchurch, New Zealand, where he will spend two months.**


IMA International Conference


IMA International Conference


IMA International Conference


IMA International Conference

- **Steven Galbraith was the Programme Chair of the 11th IMA International Conference in Cryptography and Coding, held in Cirencester on December 2007.**

- **The second International Conference on Pairing-based Cryptography (Pairing 2008) will be held at Royal Holloway on September 1st – 3rd, 2008. Steven Galbraith and Kenny Paterson are co-chairs of this event, which is designed to bring together researchers in this extremely active area of cryptographic research (which has, for example, led to elegant schemes for identity-based cryptography). Further details of Pairing 2008 can be found at www.pairing-conference.org**

Recent Completed PhD Theses…

Anand Gajparia
"On user privacy for location-based services"…
Omar Zakaria
"Investigating information security culture challenges in a public sector organisation: a Malaysian case"…
Miss Laiha Mat Kiah
"A key management framework for secure group communication in wireless mobile environments"…
Emmanuel Hooper
"Intelligent Detection and Response Strategies for Network Infrastructure Attacks"…
Michael Tunstall
"Secure cryptographic algorithm implementation on embedded platforms"…
Qiang Tang
"Key establishment protocols and time-released encryption schemes"…
Paulo Pagliusi
"Internet Authentication for Remote Access"…

Three words about the MSc

Enlightening, insightful, great

Stephen Khan
MSc Student 2007/08

Three words about the MSc

Dream come true

Roy Biakpara
MSc Student 2007/08


The Annual Smart Card Centre Open Day, September 2007

SMART CARD CENTRE REVIEW OF THE YEAR
BY KEITH MAYES, DIRECTOR ISG SMART CARD CENTRE

The ISG Smart Card Centre has had another interesting and successful year in 2007, with significant developments on our projects, staffing and teaching activities.

A significant highlight was the publication of a text book *Smart Cards, Tokens, Security and Applications*, co-authored by the SCC staff Keith Mayes and Kostas Markantonakis and published by Springer. This book provides a convenient course text for the elective smart card module on the MSc in Information Security, which has seen an increase in the number of attendees. This module was overhauled in 2007 in order to introduce material on important new topics such as Passports and Identity Cards, overview of Trusted Platforms and the Transport for London Oyster Card system. In an exciting new development, we also intend to develop a distance learning version of this module to further open up the accessibility of this material.

The event highlight of the year was the annual SCC Open Day, which was again very well supported and attended. This year there were 24 exhibitors, representing a 50:50 split between industrial exhibitors and SCC Masters or PhD researchers. One of the most interesting exhibits was an Oyster Card tube station gate brought by Cubic, although the best industry exhibitor prize went to Giesecke & Devrient. The best student exhibitor prize was awarded to Mohammad Shami who has gone on to become a smart card consultant with Consult Hyperion.

The work of another MSc project student Nathan Gatt was publicised in the Sunday Times newspaper (Malta) and has since been submitted to a research conference.

On the personnel front, we were delighted that Will Sirett was awarded his PhD after researching in the SCC and we welcomed Gerhard Hancke as a Research Assistant to work on a new contactless smart card project. Over the summer, we also hosted two Visiting Researchers, Yuan-Hung Lien and Shen Sung-Shio, from the National Taiwan University of Science and Technology, as part of an ongoing co-operation with the Taiwan Information Security Centre (TWISC).

SCC staff also took to the road and lectured at the TWISC summer school in Taipei, as well as in California, Crete and Dresden. The SCC also played a significant organisational role in the WISTP 2007 event on Smart Cards, Mobile and Ubiquitous Computing Systems but has a much more demanding role in 2008, when it is proud to host the prestigious eighth Smart Card Research and Advanced Application Conference (CARDIS 2008) at Royal Holloway: www.scc.rhul.ac.uk/CARDIS/

Another interesting, but tiring, year beckons!

Three words about the MSc

BUZBIIBKQ ZLROPB (CAESAR)

Jose Bartasevicius
MSc Student 2007/08

Three words about the MSc

Well it depends…

C. Orozco-Corona
MSc Student 2007/08

TOWARDS A VISION OF OPEN TRUSTED COMPUTING
BY STEPHANE LO PRESTI

Recent years have seen a steadily growing number of online threats because hackers have progressed from being amateurs simply aiming for glory to professionals seeking large profit. In this context, major players in the computing industry decided in 1999 to create the Trusted Computing Group (TCG), formerly know as TCPA, an industry-wide consortium that now includes more than 150 companies from a wide range of business domains.

Trusted Computing is a new security paradigm based on the open and platform-independent specifications defined by the TCG and provides fundamental security building blocks that are currently needed to enforce and harden security mechanisms.

Trusted Computing relies on a central component called the Trusted Platform Module (TPM) that is most often implemented as a hardware chipset. The TPM provides cryptographic capabilities (such as RSA encryption, RSA signatures and random number generation), can securely protect secrets and can also reliably report these secrets to outside entities. This component is complemented by various other mechanisms such as measurement, which computes the identity of a program as a hash of its binary (currently SHA-1) and attestation, which exchanges these measurements between communicating entities in a secure and reliable way.

The Open Trusted Computing (OTC) project is a Research and Development project financed by the European Commission through the Sixth Framework Programme. OTC involves 23 partners, including universities such as University of Cambridge, CEA (France), Technische Universitat Dresden (Germany), Ruhr-Universitat Bochum (Germany), Politecnico di Turino (Italy), Katholieke Universiteit Leuven (Belgium) and companies such as HP, IBM, AMD, Infineon and SuSE. Royal Holloway is one of the academic partners and the research work is being led by Chris Mitchell and myself. This project started in November 2005 and will finish in April 2009.

The OTC project focuses on the development of trusted and secure computing systems based on open source software and is using the security building blocks defined by the TCG to create a complete operational system that can be used to provide a higher level of trust and security. Trusted Computing is combined with virtualisation technology, which aims at managing several operating systems executing in parallel (in what is called a virtual machine) and controlling them at the hardware level in order to ensure their correct functioning. This combination of technologies, called trusted virtualisation, is being developed by the OTC project and introduces a finer level of control on monolithic operating systems in a trusted and secure manner.

The OTC project has developed and distributed an initial prototype, including the source code of its main components. This is publicly available from the OTC website: www.opentc.net

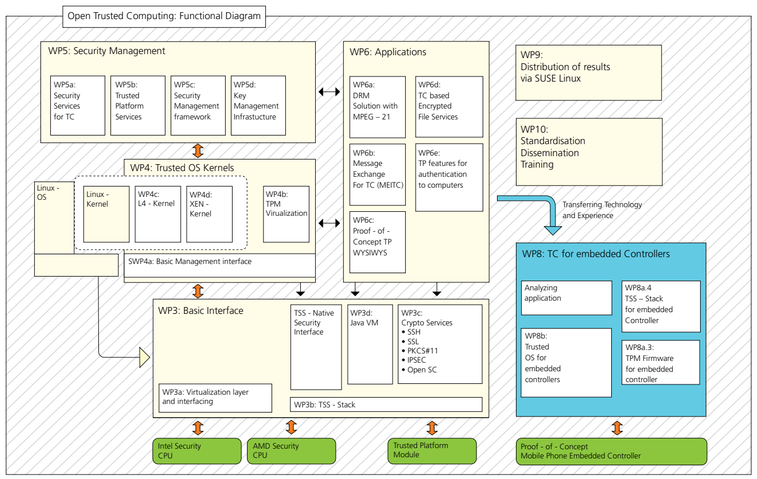
Thanks to the new capabilities of trusted virtualisation, the project first demonstrated protection from an unauthorised client access to an e-commerce server (eg. online banking) in the case where the client platform does not correspond to the software state expected by the server. A mutual attestation protocol ensures that both sides reliably know the state of the other side and, thus, trusted client-server communication is only possible when both client and server execute the trusted virtualisation software in the particular configuration defined for this scenario. Attacks against the client platform by Trojans or viruses are thus ineffective and phishing attacks are prevented thanks to the level of control enabled by trusted virtualisation.

The second OTC prototype is under development and revolves around the scenario of corporate computing at home, where an employee uses a computing system set up by his employer in order to use, in a trustworthy manner, the corporate services in tandem with his private and personal applications. This scenario illustrates the multilevel security that trusted virtualisation can allow, where virtual machines, for example executing the secure VPN corporate client and the private DRM application of the user, run next to each other in isolation and without interference. Such a scenario cannot be implemented on computing platforms that do not contain the Trusted Computing elements, due to the inability to enforce policies in a reliable way.

Royal Holloway also conducts research on how the OTC technologies can be applied to mobile platforms, which have aspects that require the general model to be adapted. This work is in collaboration with the Universities of Bochum and Dresden and the industrial partners Infineon and Comneon. In this work package, scenarios ranging from the hardening of DRM systems to phone identity protection are analysed and mappings to the OTC technologies are being developed.

In parallel to the technical efforts of the project, several partners, including Royal Holloway, are teaching courses that introduce Trusted Computing technology to the security community.

In combination with a significant publication effort, these courses help in fighting the prejudices against the technology that were formed as a response to early criticisms and misunderstandings. Royal Holloway is enjoying its role as a leader in education and research on Trusted Computing technology.



Three words about the MSc

Knowledgeable, useful, competent

Sander Moonen
MSc Student 2007/08

Three words about the MSc

Fantastic, super, informative

Graham Hili
MSc Student 2007/08

BREAKING ENCRYPTION-ONLY IPsec: CRYPTOGRAPHY MEETS NETWORK SECURITY
BY KENNY PATERSON

Introduction
IPsec is a suite of protocols for providing security at the network layer, ie. for providing cryptographic protection directly to IP datagrams. It is widely used in Virtual Private Networking (VPNs) to extend the reach and security of corporate-owned networks across the potentially insecure Internet.

First developed in the mid 1990s, the IPsec specifications have gone through three generations, with the latest set being defined in IETF RFCs 4301-4309 and published in December 2005. IPsec is a mandatory part of IPv6 and seems set to become a critical security component of the next generation of IP networks. IPsec permits a lot of flexibility in how it is deployed and configured, and, as a consequence, the third generation RFCs form a very complex set of documents, running to over 300 pages of detailed technical specifications.

So how secure is IPsec exactly? This is a question that we set out to study in late 2004, and are still thinking about today. It's been a fascinating journey.

In our work, we've focused mostly on "encryption-only" configurations of IPsec. In these configurations, the data to be protected are encrypted but not integrity-protected. Despite there being several high-profile examples where the lack of integrity-protection (or the inappropriate provision of it) has allowed attacks against network protocols, the IPsec standards still allow encryption-only configurations to be used. In fact, for reasons of backwards compatibility, support for encryption-only was mandatory in the second generation of IPsec standards! Already in 1995, Steve Bellovin had sketched attacks which allowed plaintext data to be recovered even though protected using IPsec's encryption protocol, ESP. Moreover, there is plenty of support from theoretical cryptography for always combining encryption with integrity protection to get an appropriate strength of security against active attackers. Some of this research was even cited in the second generation version of ESP, along with warnings about the dangers of encryption-only IPsec and Bellovin's attacks. Still, to quote RFC 4303:

"ESP allows encryption-only … because this may offer considerably better performance and still provide adequate security, eg. when higher layer authentication/integrity protection is offered independently."

Surely then, with all this history and warnings, there's no danger of anyone actually ever configuring IPsec in encryption-only mode? Well, remember that until recently, developers were required by the IPsec RFCs to support encryption-only ESP, so the option should be available to users. Developers rarely pass RFC warnings to users, and users don't usually read RFCs (unless they have a bad case of insomnia). And users might reasonably assume that encryption on its own gives confidentiality. After all, didn't we all learn in class that encryption provides confidentiality for data?

To cap it all, we found that many online tutorials do not highlight the dangers of encryption-only IPsec. Worse than this, we found several tutorials actively encouraging the abandonment of integrity protection. Take this classic example from the IPsec Tunnel Implementation administrator's guide of a well-known vendor:

"If you require data confidentiality only in your IPSec tunnel implementation, you should use ESP without authentication. By leaving off the authentication service, you gain some performance speed but lose the authentication service."

We decided to investigate the (in)security of encryption-only IPsec more closely. To make the case against encryption-only as damning as possible, we set out to find attacks that were as realistic as we could make them: no paper sketches for us, no chosen plaintexts – only the ability to sniff data from an IPsec VPN, inject packets into the network, and watch how the network responds.

Attacking the Linux Kernel Implementation
Our first set of attacks exploited something already well-known to cryptographers, the bit-flipping property of CBC mode encryption. This property, inherited in the IPsec protocol ESP, allowed us to manipulate certain fields in the headers of encrypted IP datagrams so as to force unusual IP datagrams to be produced upon decryption; these unusual packets were eventually received and processed by the IP layer, and resulted in error messages of various types. The error messages are carried by ICMP, the standard protocol for reporting such problems with IP.

But here's the punchline: so as to be as helpful as possible, ICMP reports back the entire header of the offending packet, plus the first few bytes of that packet's payload. But this is now all in plaintext form! By appropriately slicing and dicing the encrypted packets and repeating the process, we were able to recover the entire contents of encrypted packets, given only the ability to sniff, modify, and inject data into the network, and to observe the ICMP responses. Normally, these error messages would be encrypted in the tunnel but by using more tricks, we were able to ensure they were sent outside the tunnel, even straight to the attacker's machine in some variants.

We implemented these ideas in an attack client and tested it on a small network of machines running the Linux Kernel Implementation of IPsec; our client could recover plaintext in nearly real-time. For detailed technical reasons, the attacks only got better the larger the block size of the encryption algorithm – AES fared worse against our attacks than DES. No amount of upper-layer integrity protection could prevent our attacks: they were done-and-dusted before the upper layer ever saw the data. And even some of IPsec's many allowed ways of combining encryption with integrity protection were still vulnerable to attack.

We were unsure of what real-world impact our attacks might have: on the one hand, we felt that someone, somewhere must be using encryption-only IPsec, but how many installations might be affected? To help us better gauge this, and just in case the consequences really were serious, we decided to opt for responsible disclosure. We worked hand-in-hand with staff at NISCC, now the Centre for the Protection of National Infrastructure (CPNI). With their help, we explained our attacks to the vendor community, giving them time to react before the publication of NISCC's High Severity Vulnerability Advisory [1]. NISCC's advisory was picked up by US-CERT and was covered on Slashdot, The Register, clnet news, and elsewhere. Eventually, our technical paper [2] appeared at Eurocrypt 2006, Europe's leading research conference on cryptography. We also wrote a non-technical account of our work [3], highlighting the breakdown in communication between cryptography theoreticians, IPsec standards writers, implementors and users that we believed it represented. We hoped that this extensive coverage would ensure our message was not lost on those who needed to hear it.

Attacking the RFCs
End of story? Not quite! What we did not anticipate was the reaction from the IPsec experts themselves. The main message we received was that none of this was news (quite true if you knew about Bellovin's paper and had read the RFCs but perhaps not quite so well-known outside the inner circle).

Moreover, our attacks were only attacks against a particular implementation but not attacks against the standards themselves. Indeed, Steve Kent, one of the main writers of the IPsec RFCs, pointed out to us that the Linux implementation omits to carry out certain post-processing policy checks specified in the RFCs which, if properly done, would have prevented our attacks. So it was argued that our attacks worked only against an incomplete implementation of the RFCs. One might respond by asking what is more important: an attack on paper against a specification, or an attack that works in practice against a widely-used implementation?

Inspired by this reaction, we had the idea of trying to find attacks that would work ONLY if an implementor had been strict in following all the advice to implementors given in the latest set of IPsec RFCs.

Our aim was to make the point that it didn't matter whether we found attacks against specification or implementations but rather that encryption-only IPsec was fundamentally weak. To prevent Bellovin's earlier attacks, the RFCs recommended the use of padding checks, to ensure that data had been properly padded to a block boundary before encryption. This gave us our way in. We were able to extend earlier work of Serge Vaudenay to show how padding (and other) checks that should be carried out by an RFC-compliant implementation could be exploited to build a side-channel attack against IPsec. Our side-channel was based on the detection of certain ICMP packets that would be produced by processing of attacker-manipulated packets by IP. So as to pass policy checks, we could not direct these to our attacker's machine – now they went back across the VPN in encrypted form. But they had a characteristic length which meant we could spot them by doing simple traffic analysis on the VPN.

So much for the theory – what would happen in practice? Would any implementation be strict enough in following the RFCs that our on-paper attacks would actually work? This is where the final twist in the tale arises.

Story continues on page 16

Three words about the MSc

Enlightening, strenuous, indispensable

Andy Moore
MSc Student 2007/08

Three words about the MSc

They look young (some of the other students!)

Kerry Davies
MSc Student 2007/08

Peter Wild, Peter Jaco, Tony Greenwood, Vice-Principal David Sweeney

OrbisIP PARTNERS WITH THE ISG

Royal Holloway has signed a partnership agreement with OrbisIP Limited to assist in the commercialisation of Information Security intellectual property developed by the Information Security Group. OrbisIP is focused on the technology transfer and licensing of Information and Homeland Security Intellectual Property (IP) Patents and Products.

Under the agreement, OrbisIP will work closely with the ISG to explore areas of technology development that have commercial application and will also advise them on the technical requirements of OrbisIP customers. The ISG is already working with OrbisIP supporting the evaluation of new Security Technology for inclusion within the OrbisIP Patent and Product Pool.

"We are pleased to be partnering with OrbisIP to develop additional distribution channels for our information security-focused Patents and Products as produced by our Information Security Group," said Tony Greenwood, Director of Research & Enterprise, Royal Holloway.

"OrbisIP offers a new and groundbreaking way of working with producers of security-focused Intellectual Property that will help us to promote our technology, brand name and Information Security consulting skills to a worldwide audience of technology consumers."

"We are delighted to welcome Royal Holloway, University of London as our first University Partner," said Peter Jaco, Chief Executive Officer, OrbisIP. "As one of the largest Information Security academic research groups in the world, the breadth and depth of the Information Security research undertaken within the University's Information Security Group is well recognised. We are looking forward to working with our new partners to help promote their technology to international OrbisIP customers who rely on the development of innovative security technology."

THE ECRYPT EUROPEAN NETWORK OF EXCELLENCE IN CRYPTOLOGY
BY CARLOS CID

Cryptology is the science that studies mathematical techniques related to the security of transmission and storage of digital information. It encompasses both cryptography (the art of designing and use of cryptosystems, ie. secure algorithms and protocols) and cryptanalysis (the art of 'breaking' cryptosystems). Although it has been historically linked to confidentiality, modern cryptology covers a much wider range of issues, such as integrity, authentication and non-repudiation.

Until the 1970s, cryptologic research was almost the exclusive monopoly of government agencies; little was available on cryptographic design and analysis in the public domain. The 1970s saw the birth of cryptology as an academic subject, and it has since attracted the attention of a growing number of mathematicians, computer scientists and engineers. Although unarguably in its infancy as science, cryptology is currently a very active, thriving area of interdisciplinary academic research.

Europe has always had a strong tradition in cryptologic research. Much pioneering work in areas such as block cipher, stream cipher and hash function design and analysis, elliptic curve cryptography and mobile communications security has been carried out by researchers in Europe. For example, the current US standard symmetric algorithm for encryption (AES) is a Belgian design. Although collaboration between different European groups has obviously always existed, it was clear that a concentrated effort to integrate research in this area could bring much benefit to the development of cryptology in Europe.

To intensify the collaboration of European researchers working in the field, the European Network of Excellence for Cryptology (ECRYPT) was launched in February 2004. ECRYPT is a project funded under the European Commission's Sixth Framework Programme, with the main objective of "ensuring a durable integration of European research in both academia and industry and maintaining and strengthening the European excellence in the area of cryptology" (www.ecrypt.eu.org).

ECRYPT has 32 partners, which are able to integrate much of their individual efforts in cryptology within five virtual labs, focusing on the core research areas of symmetric cryptography, asymmetric cryptography, cryptographic protocols, efficient and secure implementation of cryptosystems, and watermarking.

First and foremost, ECRYPT is a network; its main goal is to create links between its partners, by facilitating research and better collaboration between European researchers working in cryptology. This has been achieved by sponsoring workshops and summer schools, exchange visits of researchers and PhD students and developing a joint infrastructure in cryptologic research. Royal Holloway is one of the main partners within ECRYPT. Several researchers from the ISG are heavily involved in a number of ECRYPT activities, from co-ordination of working groups and organisation of events, through to simply establishing and strengthening collaborative work with other researchers.

After more than four years, ECRYPT comes to an end in 2008. ECRYPT has been fundamental in improving the state of the art in practice and theory of cryptology in Europe. Strong links have been created between ISG researchers and their peers across Europe and it is anticipated that these will remain long after the end of the project. In fact, its successor, ECRYPT II, a new research project funded under FP7-IST programme will officially start in July 2008. This is a four-year project, with nine academic and two industrial members. Royal Holloway is once again one of the academic partners; close interaction with partners across Europe should continue to benefit its researchers and students, and ultimately strengthen the position of the ISG as one of the leading academic centres in cryptologic research in Europe.

The 3rd ECRYPT PhD Summer School was held in Crete, Greece, in May 2007

ECRYPT

RECOGNISING OUTSTANDING THESES – SEARCH SECURITY PUBLICATIONS TEAMS UP WITH THE ISG

The ISG has teamed up with popular industrial information security resource Search Security (www.searchsecurity.co.uk) to recognise outstanding MSc project theses with particular applications to business.

A number of outstanding candidates were invited to write short articles on the subject of their thesis. These articles will appear throughout the year on the Search Security website and the corresponding thesis will be published as an ISG Technical Report (downloadable from www.ma.rhul.ac.uk/tech).

According to Dr. Alex Dent, who is co-ordinating the project: "The idea is that students gain recognition for their efforts and that industry gains a valuable resource. We hope that the short articles will be accessible enough for everyone to read, while the complete theses give the interested reader a much broader and more detailed analysis of the subject. It's a great example of how our students can bridge the gap between theory and practice."

This year's collection of award winners spans a huge range of information security topics, from information security training techniques to intrusion detection systems based on the human body. The complete list of award winners is:

Forensics of BitTorrent
by Jamie Acorn and supervised by John Austen

Review and Analysis of Current and Future European e-ID Schemes
by Siddhartha Arora and supervised by Michael Ganley

Detecting Pandemic and Endemic Incidents through Network Telescopes: Security Analysis
by Fotis Gagadis and supervised by Stephen Wolthusen

Information Security Training & Awareness
by Monique Hogervorst and supervised by Keith Martin

Securing Financially Sensitive Environments with OpenBSD
by Nicholas C. P. Humphrey and supervised by Peter Wild

Copy Protection of Computer Games
by Richard Hyams and supervised by Peter Wild

Cheating and Virtual Crime in Massively Multiplayer Online Games
by Rahul Joshi and supervised by Andreas Fuchsberger

Metamorphic Virus: Analysis and Detection
by Evgenios Konstantinou and supervised by Stephen Wolthusen

Tigger team – a novel methodology to manage business risk
by Ian McKinnon and supervised by Keith Martin

Proposed Model for Outsourcing PKI
by Christopher McLaughlin and supervised by Geraint Price

Intrusion Detection and Prevention: Immunologically Inspired Approaches
by Devid Pipa and supervised by Alex Dent

Computer Security: A Machine Learning Approach
by Sandeep V. Sabnani and supervised by Andreas Fuchsberger

Network Covert Channels: Review of Current State and Analysis of Viability of the use of X.509 Certificates for Covert Communications
by Carlos Scott and supervised by Chez Ciechanowicz

For more details, visit:
www.ma.rhul.ac.uk/tech

Three words about the MSc

Exciting, inspiring, professional

Bruno Kovacs
MSc Student 2007/08

Three words about the MSc

Hard, lonely, rewarding

Stephen Thornber
MSc Student 2007/08
(Distance Learning)

Chez Ciechanowicz and Fiona Higgins accept the Best Information Security Team (government) Award at the RSA Conference Europe

ISG RECEIVES INDUSTRIAL AWARD

The Information Security Group was awarded the industry prize of the Best Information Security Team (government) at the SC Professional Awards. The ceremony held at the RSA Conference Europe in London on 22nd – 24th October 2007 saw five categories awarded throughout the information security sector.

The honours reward the truly outstanding members of the profession and recognise excellence in the fields of data security and risk management.

Director of the ISG, Professor Peter Wild, was proud to have received the award: "It reflects the way that academia and industry can work in harmony together and endorses the relevance of our MSc in Information Security. As a team we try to foster close collaboration with our contacts in the commercial sector. We trust that we are meeting the needs of business by producing high quality graduates in information security," he said.

Professor of Information Security, Kenny Paterson, added that it is excellent to receive recognition from within the industry:

"The whole ISG team is committed to working hand-in-hand with industry to set the highest levels of quality in research and education in Information Security. This external validation helps to confirm that we are continuing to do that."

With an estimated 2 billion security incidents to date, information security is thought to be key in securing success in any organisation. The 8th Annual RSA Conference Europe highlighted how critical it is to stay ahead of information security threats and be kept informed about the latest solutions, products and trends.

Three words about the MSc

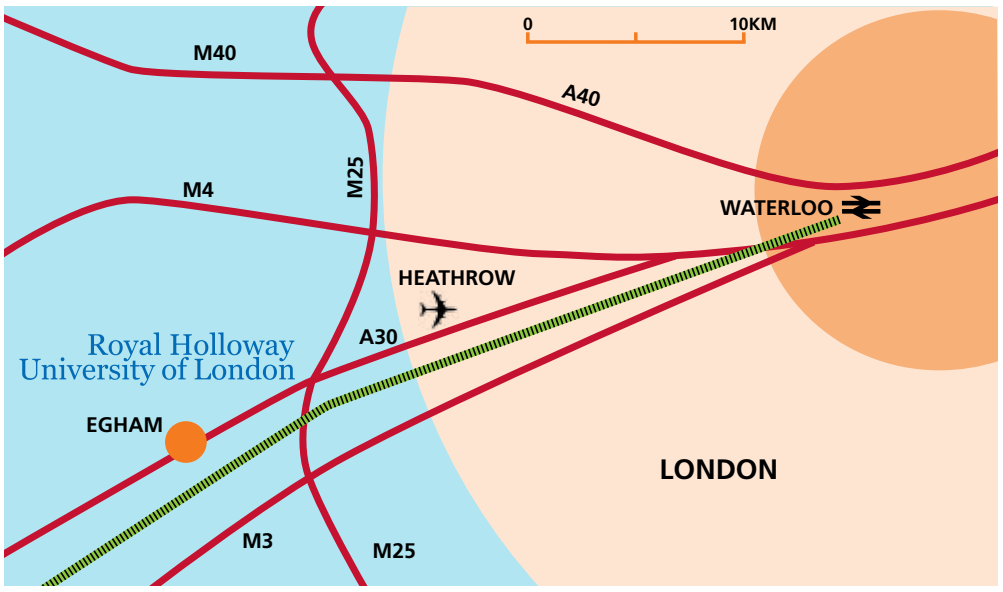
A wonderful experience

Paulo Cardoso
MSc Student 2007/08
(Distance Learning)

Three words about the MSc

Tricky, thought-provoking, stimulating

Christian Bonnici
MSc Student 2007/08



CONTACT INFORMATION:

For general information about the Information Security Group and the MSc and diploma programmes offered by the ISG, please contact:

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

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

For an overview of the application process, please visit: www.rhul.ac.uk/graduate-school

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

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

HOW TO GET TO ROYAL HOLLOWAY:

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

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

Three words about the MSc

Thorough, challenging, knowledge

Babak Sokout
MSc Student 2007/08
(Distance Learning)

CONT FROM PAGE 13

We looked at many open-source implementations of IPsec to see what they did. Linux did no padding checks at all, rendering it vulnerable to Bellovin's 10-year-old attacks (the code contains the classic comment: "/* ... check padding bits here. Silly. :-) */"). Others (Openswan, strongSwan, FreeS/WAN) checked the padding carefully but then did nothing if the padding was wrongly formatted. Strange, but not inconsistent with the RFCs which don't actually mandate a packet drop in this case! Only one implementation, OpenSolaris, appeared to be strict enough to allow our attacks to work, since it allowed the user to configure strict padding checks as an option. But when we selected this option and ran our attack, we found that IPsec stopped working. After much head scratching, we discovered that there was a bug in the OpenSolaris implementation of the padding check that broke IPsec. By this time, we were in direct communication with Dan McDonald at Sun Microsystems, one of the chief architects of IPsec in Solaris. With Dan's help, we got the bug fixed in Release 55 of OpenSolaris ... after which our attacks worked perfectly! The full technical details of our second set of attacks can be found in [4].

Concluding Remarks
Our analysis required a mixture of mathematical cryptanalysis, socket-level programming, line-by-line analysis of IPsec RFCs and implementation code, and a good grasp of basic IP networking – hardly the domain of traditional academic research in cryptography.

Our efforts revealed some interesting insights (at least for us) into the interactions between cryptography and network security. Of note were the complexity of the RFCs; the extent to which security guidance in RFCs is ignored or misunderstood by implementers; a modicum of disregard for the vulnerable position of the security-unaware end-user on the part of standards writers, and a clear tension between security and the need to maintain backwards compatibility which surprised us in a standard dedicated to security. We also identified challenges for the cryptography research community: what can we do better to ensure that existing theory is translated smoothly into practice? What can we do to extend theory so as to immunise cryptography against poor implementation practices?

Unfortunately, our work came too late to influence the text of the third generation of IPsec RFCs, and the IETF working group on IPsec has now been wound up. At best, we hope that our work, and the coverage it garnered, will help raise awareness of the dangers of using encryption without appropriate integrity protection. At the very least, we got onto Wikipedia [5] and NISCC's Christmas card list [6]!

[1] NISCC Vulnerability Advisory IPSEC — 004033, 9th May 2005. http://www.cpni.gov.uk/docs/re-20050509-00385pdf?lang=en

[2] K.G. Paterson and A.K.L. Yau, Cryptography in Theory in Practice: The Case of Encryption in IPsec, In S. Vaudenay (ed.), Eurocrypt 2006, Lecture Notes in Computer Science Vol. 4004, pp. 12-29, Springer-Verlag, 2006. Full version at http://eprint.iacr org/2005/416

[3] K.G. Paterson and A.K.L. Yau, Lost in Translation: Theory and Practice in Cryptography, IEEE Security & Privacy, vol. 4, no. 3, May/June 2006, pp. 69-72

[4] J.P. Degabriele and K.G. Paterson, Attacking the IPsec Standards in Encryption-only Configurations. In IEEE Symposium on Privacy and Security, pp. 335-349, IEEE Computer Society, 2007. Full version at http://eprint.iacr.org/2007/125

[5] http://en.wikipedia.org/wiki/ipsec

[6] Private communication from NISCC, Christmas 2005

This newsletter has been printed on Cyclus Offset 100% recycled paper.
Design: Allyson Waller / Editing: Keith Martin / Jo Moulds