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. The 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 11.

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 in Information Security 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

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

Sylvain Martinez
MSc. Student 2007/08

Three words about the MSc

Interesting, rollercoaster, challenging
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 students to arrive at any time to access the laboratory resources. Within the laboratory, students can use a so-called "attack machine" that is connected to a network of servers which have known vulnerabilities. All connections within the virtual lab to the outside world are prohibited. "The advantages of this setup are security, since we have controlled access to the laboratory via a firewall, and security, since we have controlled prohibited." The advantages of this setup are security, since we have controlled access to the laboratory via a firewall, and security, since we have controlled prohibited. "The advantages of this setup are security, since we have controlled access to the laboratory via a firewall, and security, since we have controlled prohibited. The advantages of this setup are security, since we have controlled access to the laboratory via a firewall, and security, since we have controlled prohibited.

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

The ISG is involved in a joint UK Ministry of Defence project, the Cyber-Declaration Secure Communities of Practice (well-servers) project, which is a major international project involving university partners, the international community of information security professionals, and many students from the Security Lab who have already produced the first proper national communication protocols and architectures that facilitate the formation of large ad hoc networks. A flexible, "Communities of Interest"

The lab was established in 2007 as the "Lab in a Box" project and it is designed to be portable and easily deployable. The lab consists of a series of modules that can be connected together to create a large network that can be used for various types of exercises and training scenarios. The lab is designed to be scalable, allowing it to be used in a wide range of environments, from small classrooms to large lecture halls.

The lab is currently being used by a number of organizations around the world, including universities, government agencies, and research institutions. It is being used to train security professionals in a variety of skills, including intrusion detection, response, and recovery.

The lab is also being used to demonstrate the effectiveness of various security technologies and techniques. It is being used to test the effectiveness of various intrusion detection systems, and to evaluate the performance of various types of security protocols.

In addition to the lab, the ISG is also working on a number of research projects, including the development of new security architectures and the evaluation of new security technologies. The lab is being used as a testbed for a number of these projects, allowing researchers to experiment with new ideas and technologies in a controlled environment.

The lab is also being used to provide training for a variety of professionals, including security analysts, network administrators, and cybersecurity professionals. The lab is being used to provide training on a wide range of topics, including security protocol design, network security, and intrusion detection.

In addition to the lab, the ISG is also working on a number of research projects, including the development of new security architectures and the evaluation of new security technologies. The lab is being used as a testbed for a number of these projects, allowing researchers to experiment with new ideas and technologies in a controlled environment.

The lab is also being used to provide training for a variety of professionals, including security analysts, network administrators, and cybersecurity professionals. The lab is being used to provide training on a wide range of topics, including security protocol design, network security, and intrusion detection.

The lab is currently being used by a number of organizations around the world, including universities, government agencies, and research institutions. It is being used to train security professionals in a variety of skills, including intrusion detection, response, and recovery.

The lab is also being used to demonstrate the effectiveness of various security technologies and techniques. It is being used to test the effectiveness of various intrusion detection systems, and to evaluate the performance of various types of security protocols.

In addition to the lab, the ISG is also working on a number of research projects, including the development of new security architectures and the evaluation of new security technologies. The lab is being used as a testbed for a number of these projects, allowing researchers to experiment with new ideas and technologies in a controlled environment.

The lab is also being used to provide training for a variety of professionals, including security analysts, network administrators, and cybersecurity professionals. The lab is being used to provide training on a wide range of topics, including security protocol design, network security, and intrusion detection.
Security, security, security

Chris Potter, PricewaterhouseCoopers, presented his own personal take on the impact of the Sarbanes-Oxley (SOX) legislation. Speaking as an auditor, Chris learned 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.

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 information-distinguished speakers from around the world to this event over the years, and 2007 was no exception.

First up was a video from Chris Orm, UK, who is IT Security Manager for the Olympic Games and Major Events. Chris presented a fascinating insight into the challenges of providing a secure communications infrastructure for the Olympic Games. Chris Orm 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 lead for London 2012.

For many of the audience, this was probably the first time that they had considered the enormous challenges of providing information security in an environment where most of us will be working off-site for much of the time. The HP staff who prepared the hard copy of the results of an event.

My PhD does not have the same pressures as an exam. There is no one that can take away your hard work. If you do not do well in an exam, well, it will help if someone can just mark your answers. But if you do not do well in your PhD, well, it will help if someone can just show you creative ideas and help you to achieve better results.

One thing that is really different is the study time you have when you work for a PhD. One of the reasons is that you have more flexibility in your study time. You can have more time to do whatever you want. You can also have more time to do things that you enjoy. You can also have more time to do things that you are passionate about.

And I research areas which are of personal interest. You can set your own study aims and objectives, and you can research topics that are of personal interest. You can also choose the papers to read and the books to read. And you can also choose the people to work with.

But you also have to be careful. You have to be careful not to be too relaxed. You have to be careful not to be too relaxed about what you are doing. You have to be careful not to be too relaxed about the time you are spending. You have to be careful not to be too relaxed about the people you are working with. You have to be careful not to be too relaxed about the results you are getting.

Another thing that is really different is the time you have when you work for a PhD. You have more time to do things that you enjoy. You can also have more time to do things that you are passionate about.

One thing that is really different is the study time you have when you work for a PhD. You have more flexibility in your study time. You can have more time to do whatever you want. You can also have more time to do things that you enjoy. You can also have more time to do things that you are passionate about.

One thing that is really different is the study time you have when you work for a PhD. You have more flexibility in your study time. You can have more time to do whatever you want. You can also have more time to do things that you enjoy. You can also have more time to do things that you are passionate about.
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 had access to it. Worse, it was reported that the data was not encrypted. Well, mishaps occur but, in terms of precedent and procedure.

As this was discussed in answer to a parliamentary question, the matter quickly became public knowledge. It became the OF THE YEAR security story that had caught their attention. No doubt what the main story was:

May 2007

• USA – Louisiana State University – laptop lost with details of 790 students
• USA – Maryland Dept. of Natural Resources – laptop lost with details of 1,480 police and rangers
• UK – Royal Cornwall Hospital – computer lost with details of 5,000 staff
• USA – Virginia Dept. of the Aging – hard drive lost, with details of 40,000 people
• UK – Morris & Spence – laptop lost with details of 26,000 staff on pension plans

June 2007

• UK – Bank of Scotland – computer disc lost with details of 22,000 customers
• USA – Boston Police – laptop stolen with details of 57,000 employees
• UK – Association of the Motor Industry – laptop stolen with details of 600,000 registered vehicles
• UK – University of Essex – flash drive lost with details of 18,000 students

October 2007

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

November 2007

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

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 100 laptops containing customer data
• USA – Dept. of Agriculture – loss of data of 30,000 individuals receiving farm subsidies
• UK – Dept. of Health – loss of details of hundreds of junior doctors
• USA – New York Special Funds Committee – laptop lost with details of 540,000 individuals

July 2007

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

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 selling money elver publishing his bank details in his newspaper column. He was trying to make the case that he had identified fraud and then provided ransom money to a criminal by being forced to live in public by afully the elver after a week. He was used to create a £500 direct debit to the charity Diabetes UK. Wonderful. See the story at: http://news.bbc.co.uk/1/hi/entertainment/7134766.stm

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 exciting with the trend toward 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’s strikingly based, and somehow also related concerning that an important application such as electronic voting should be played with in such a way. http://cwflyris.com/2011/05/489/83081405.html

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 (i.e. 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 activity story of the past year which doubt the revelation that UK government departments appear to be routinely losing millions of sets of personal data.

For me, the biggest was not that it was lost but that the thefts were by which it was lost. Such data wasn’t so trivial to be trivial, it’s simply an example of bad practice, sloppy use of technology, and 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.

STEVEN WOLTHUSEN:

Until recently, there has been very little information on actual information security attacks on critical infrastructures, despite consensus that many areas of the critical infrastructure are more and more heavily on information systems and that many of these systems are poorly protected. In July 2007, the 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.

http://www.itpro.co.uk/blogs/isg/2008/02/17/

http://news.bbc.co.uk/2/hi/entertainment/7174760.stm

http://cwflyris.com/2011/05/489/83081405.html

www.washingtonpost.com/wp-dyn/content/
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 Taoying 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 the Journal of Cryptology and the series advisory board for Springer’s Information Security and Cryptography book series. Jason 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 Hessen, Netherlands, and presentations on provable security at Schloss Dagstuhl, Germany, and the Lighthill Institute of Mathematical Sciences, London. Jason also delivered sessions at two EURCRYPT 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- and authority- based key exchange protocols).

• 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.

Recent Completed PhD Theses...

Anand Gargaria
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 Attack Detection"

Michael Turnstall
"Secure cryptographic algorithm implementation on embedded platforms"

Qiang Tang
"Key establishment protocols and time-release encryption schemes"

Paula Pagliusi
"Internet Authentication for Remote Access"

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, staffings and teaching activities.

A significant highlight was the publication of a text book, Smart Cards, Tokens and Security Applications, co-authored by the SCC staff Keith Mayes and Kostas Meletankonis and published by Springer. This book provides a convenient course text for the elective smart card module on the ISG Information Security, which has seen an increase in the number of attendees. This module was introduced 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 Gemweld & Derriment. The best student exhibitor prize was awarded to Mohammad Ehsan who has gone on to become a smart card consultant with Consult Hyperion.

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

On the personal front, we were delighted that Bill Sirett was awarded his PhD after researching in the SCC and we welcomed Sarvath Francis as a Research Assistant to work on a new contactless smart card project. Over the summer, we also hosted two Visiting Researchers, Yuan-Hung Lian and Shen Sump-Shih, from the National Taiwan University of Science and Technology, as part of an ongoing cooperation with the Taiwanese 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, Centre 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 Applications Conference (CARDIS 2008) at Royal Holloway:

www.scc.tcd.ie/aS-CARDIS

Another interesting, but tiring, year beckons.

Three words about the MSc...

Jose Bartasevicius
MSc Student 2007/08

Three words about the MSc...

C. Ozcro-Corona
MSc Student 2007/08

Three words about the MSc...

Stephen Khan
MSc Student 2007/08

Three words about the MSc...

Charles Macauley
MSc Student 2007/08

Three words about the MSc...

Roy Blakpara
MSc Student 2007/08

Three words about the MSc...

Qiang Tang
MSc Student 2007/08

Three words about the MSc...

Mr. Steve Chong
MSc Student 2007/08

Three words about the MSc...

Min Yeo
MSc Student 2007/08

Three words about the MSc...

Sharon Xiao
MSc Student 2007/08

Three words about the MSc...

Paula Pagliusi
MSc Student 2007/08

Three words about the MSc...

Qiyu Zhang
MSc Student 2007/08

Three words about the MSc...

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 3rd - 5th, 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

SMART CARD CENTRE REVIEW OF THE YEAR

By Keith Mayes, DIRECTOR ISG SMART CARD CENTRE

Three words about the MSc...

Buzbirb Zlrob
(CAESAR)

Three words about the MSc...

Well it depends...

Three words about the MSc...

Enlightening, insightful, great

EMPIRE
We are on a historic journey. The Open Trusted Computing (OTC) project is a Research and Development initiative sponsored by the European Commission through the Sixth Framework Programme, OTC involves 23 partners, including universities such as University of Cambridge, CEA (France), Technische Universität Dresden (Germany), Ruhr-Universität Bochum (Germany), Katholieke Universiteit Leuven (Belgium) and companies such as HP, IBM, AMD, Infineon and SMG. 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 2003 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 a combination of technology that allows a machine to control them at the hardware level in order to ensure their correct functioning. This combination of technologies, called trusted virtualisation, at the heart of the OTC project and introduces a finer level of control on the way applications run in a trusted and secure manner.

The OTC project has developed and distributed an initial prototype, including the source code of its main components, which can be downloaded from the OTC website (www.otc.net).

Thanks to the new capabilities of trusted virtualisation, the project first demonstrated protection from an unauthorised client accessing to an enterprise server (e.g. 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; thus, trusted-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 receives around the scenarios of corporate computing at home, where an employee uses a computing system at home that is employed in order to use, in a trustworthy manner, the corporate services in tandem with his private and personal applications. This prototype establishes a user-centric approach as a response to early criticisms and misunderstandings. Royal Holloway is playing its role in a leader in education and research on trusted Computing technology.

In parallel to the technical efforts of the project, several partners, including Royal Holloway, are teaching courses that introduce Trusted Virtualisation technology to the security community. In combination with a significant industrial and academic effort, three courses help in fighting the prejudices against the technology that were foreseen in early years. In particular, the experience of using a virtual machine as a trusted context to run critical applications gives a clear view on the benefits of a trusted virtualisation technology.

So how secure is OpenSC exactly? Is it a scary evil that we set out to study in late 2004, and are still thinking about it 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 these being several high-profile examples where the lack of integrity-protection (or an inappropriate provision of it) has allowed attackers 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 [standard! Already in 1995, Sean Brooks was aware of the fact that allowed attackers 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. Nowadays, there is plenty of support from experimental cryptographic techniques for always choosing encryption-only security to get an appropriate strength of security for a given scenario. Some of this research was even cited in the worm that targeted a large number of systems, along with warnings about the dangers of encryption-only, and Bell Labs’ attacks. Still, to quote RFC 4303

ESP allows encryption-only... because this may offer considerably better performance compared to a more adequate security, esp. when higher layer authentication protocols give only the ability to sniff, modify, and replay the message. ESP does ensure that both sides reliably know the state of the other side; thus, trusted-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.

In parallel to the technical efforts of the project, several partners, including Royal Holloway, are teaching courses that introduce Trusted Virtualisation technology to the security community. In combination with a significant industrial and academic effort, three courses help in fighting the prejudices against the technology that were foreseen in early years. In particular, the experience of using a virtual machine as a trusted context to run critical applications gives a clear view on the benefits of a trusted virtualisation technology.

In parallel to the technical efforts of the project, several partners, including Royal Holloway, are teaching courses that introduce Trusted Virtualisation technology to the security community. In combination with a significant industrial and academic effort, three courses help in fighting the prejudices against the technology that were foreseen in early years. In particular, the experience of using a virtual machine as a trusted context to run critical applications gives a clear view on the benefits of a trusted virtualisation technology.
Cryptography is the science that studies mathematical techniques related to the security of transmission and storage of digital information and encompasses both cryptography (the art of designing and using cryptographic systems, i.e., secure algorithms and protocols) and cryptanalysis (the art of breaking ciphers). Although it has been historically linked to cryptography, modern cryptology covers a much wider range of issues, including algorithm design, authentication, and non-repudiation.

Until the 1970s, cryptology research was almost exclusively the 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 unequally 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 cryptography 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 always been important, it was clear that a coordinated effort to integrate research in this area could bring mutual benefit to the development of cryptography in Europe.

To intensify the collaboration of European researchers working in the field, the European Network for 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 academic 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 cryptographic systems, and postquantum cryptography. (the art of designing and using cryptographic systems, i.e., secure algorithms and protocols) and cryptanalysis (the art of breaking ciphers). Although it has been historically linked to cryptography, modern cryptology covers a much wider range of issues, including algorithm design, authentication, and non-repudiation.

Dr. and Mrs. By Carlos CID

EXCELLENCE IN THE ECRYPT PROGRAM

THE ECRYPT NETWORK OF EXCELLENCE IN CRYPTOLOGY

Recognising Outstanding Theses – Search Security Publications Teams Up with The ISG

The ISG has teamed up with popular e-mail information security resource SearchSecurity.co.uk to organise outstanding MSc project theses with particular application to business.

A number of outstanding candidates were invited to write short articles on the subject of their theses. 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.cs.rhul.ac.uk).

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 a 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 and trends.

The complete list of award winners is:

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

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

Cheating and Virtual Crime in Massively Multiplayer Online Games by Ahsa Joshi and supervised by Andreas Fuhsberger

Metropolitan Virus: Analysis and Detection by Evgenios Kostantinos and supervised by Stephen Wolthusen

Ticker team – a novel methodology to manage business risk by Ryan McCormack 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 David Paps and supervised by Alex Dent

Computer Security: A Machine Learning Approach by Sandeep S. Sabnani and supervised by Andreas Fuhsberger

Network Covert Channels: Review of Current State and Analysis of Viability of the use of X.509 Certificates for Cryptographic Protocols by Andreas Fuchsberger and supervised by Chriz Chattawut

Extraction and Analysis of a Public Key Infrastructures (PKI) Security Threat by Nicholas C. P. Humphrey and supervised by Stephen Wolthusen

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

Cheating and Virtual Crime in Massively Multiplayer Online Games by Ahsa Joshi and supervised by Andreas Fuhsberger

Metropolitan Virus: Analysis and Detection by Evgenios Kostantinos and supervised by Stephen Wolthusen

Ticker team – a novel methodology to manage business risk by Ryan McCormack 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 David Paps and supervised by Alex Dent

Computer Security: A Machine Learning Approach by Sandeep S. Sabnani and supervised by Andreas Fuhsberger

Network Covert Channels: Review of Current State and Analysis of Viability of the use of X.509 Certificates for Cryptographic Protocols by Andreas Fuchsberger and supervised by Chriz Chattawut

Extraction and Analysis of a Public Key Infrastructures (PKI) Security Threat by Nicholas C. P. Humphrey and supervised by Stephen Wolthusen

ISG Receives INDUSTRIAL AWARD

The Information Security Group was awarded the industrial 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 receive 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.

ISG Partners With The ISG

Royal Holloway has signed a partnership agreement with OrbisIP Ltd 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 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.

They look young (some of the other students!)

Andy Moore
MSc Student 2007/08

Bruno Kovacs
MSc Student 2008/09

Stephen Thormber
Distance Learning

ISG Receives INDUSTRIAL AWARD

The Information Security Group was awarded the industrial 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 receive 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.
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. -1 */”). 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 implementations 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]!

http://www.cpni.gov.uk/docs/re-20050509-00385pdf?lang=en


[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 Meulls

MSc Student 2007/08
Three words about the MSc
A wonderful experience
Paulo Cardoso
Information Security Group Secretary
p.stoner@rhul.ac.uk
+44 (0)1784 430766
Eggham, Surrey, UK TW20 0EX
Royal Holloway, University of London
Information Security Group and the
three words about the MSc
Three words about the MSc
Three words about the MSc
Three words about the MSc
Three words about the MSc
Thorough, challenging, knowledge
Babak Sokout
MSc Student 2007/08
(Distance Learning)