



Royal Holloway  
University of London



ROYAL HOLLOWAY, UNIVERSITY OF LONDON

MSC IN INFORMATION SECURITY

[www.rhul.ac.uk](http://www.rhul.ac.uk)

# CONTENTS

<b>INTRODUCTION</b> .....	<b>.2</b>
<b>INFORMATION SECURITY AT ROYAL HOLLOWAY</b> .....	<b>.2</b>
RESEARCH ENVIRONMENT .....	.2
QUEEN'S ANNIVERSARY PRIZE .....	.2
<b>CONTACT AND APPLICATION DETAILS</b> .....	<b>.3</b>
<b>GENERAL INFORMATION ABOUT THE MSC</b> .....	<b>.3</b>
DURATION AND STRUCTURE OF COURSE OF STUDY .....	.3
ENTRY REQUIREMENTS .....	.3
OVERVIEW OF PROGRAMME .....	.4
EXAMINATIONS .....	.5
DEGREE CLASSIFICATION .....	.5
CURRICULUM DEVELOPMENT .....	.6
STUDENT SUPPORT .....	.6
DAVID LINDSAY PRIZE .....	.7
<b>DETAILS OF MODULES</b> .....	<b>.7</b>
IC1 SECURITY MANAGEMENT .....	.7
IC2 AN INTRODUCTION TO CRYPTOGRAPHY AND SECURITY MECHANISMS .....	.8
IC3 NETWORK SECURITY .....	.10
IC4 COMPUTER SECURITY (OPERATING SYSTEMS) .....	.11
OPT5 SECURE ELECTRONIC COMMERCE AND OTHER APPLICATIONS .....	.12
OPT7 STANDARDS AND EVALUATION CRITERIA .....	.13
OPT8 ADVANCED CRYPTOGRAPHY .....	.14
OPT9 DATABASE SECURITY .....	.14
OPT10 COMPUTER CRIME .....	.15
MSC PROJECT .....	.16
<b>THE INFORMATION SECURITY GROUP</b> .....	<b>.18</b>
ACADEMIC STAFF .....	.18
VISITING PROFESSORS AND SENIOR VISITING FELLOWS .....	.22
CONSULTANTS TO THE GROUP .....	.24

## INTRODUCTION

This booklet describes the MSc in Information Security. This is an interdisciplinary course taught by the Information Security Group, and security experts from industry.

The electronic handling of information is one of the defining technologies of our age. Enormous volumes of information are routinely stored and transmitted worldwide – indeed, most aspects of our daily lives would come to a halt should the information infrastructure fail. However, with the benefits deriving from the ability to automatically manage so much information, come major threats to businesses, governments and individuals. These threats include possible fraud through information manipulation, deliberate damage to stored and transmitted information, and blackmail associated with the threat of damage. The field of Information Security, namely the study of countermeasures to these real and serious threats, has grown up very rapidly in recent years. The subject embraces a range of technologies such as cryptography, computer security, and fraud detection, and also includes the study of how security can best be managed.

This advanced MSc degree is designed to introduce the technical, legal and commercial aspects of Information Security. Students of the degree come from a variety of backgrounds, and part-time students are particularly encouraged. The degree is intended as a foundation for a professional career, as well as for postgraduate research, in Information Security. Graduates of the degree are expected to find employment in both industry and commerce as security experts, and the need for such experts is likely to be very high for the foreseeable future.

## INFORMATION SECURITY AT ROYAL HOLLOWAY

### RESEARCH ENVIRONMENT

The Information Security Group offers an active research environment with 13 established academic posts and a large number of research students, making it one of the largest academic security groups in the world. The Group regularly hosts international visitors and has close links to leading companies in the area of Information Security.

A dedicated network of workstations enables MSc students to perform security specific investigations. These 24-hour lab facilities are available exclusively for the MSc students. In addition, students may also use the Computer Centre's facilities. This provides access to a number of PC labs. Students have free access to the Internet including web browsers, file transfer, and electronic mail.

### QUEEN'S ANNIVERSARY PRIZE

The Queen's Anniversary Prizes for Higher and Further Education recognise and reward the outstanding contribution that universities and colleges in the United Kingdom make to the intellectual, economic, cultural and social life of the nation. The Prizes are awarded within the national honours system.

The 1998 Prizewinners were presented with their Gold Prize and illuminated Certificate by Her Majesty The Queen and HRH The Duke of Edinburgh on the morning of 11 February 1999 at a ceremony at Buckingham Palace. The same evening, the Prizewinners were honoured in a celebration

at the Guildhall in the City of London attended by leaders in government and education, industry and commerce from this country and around the world.

One of the 1998 prizes was awarded to Royal Holloway, University of London, in recognition of the work of the Information Security Group. The Prize Citation is as follows:

*“This pioneering Group provides a unique national resource for the training of information security specialists and the development of highly secure communications and computer systems. It offers world-leading independent expertise in a field of national importance where trust and integrity are paramount.”*

## CONTACT AND APPLICATION DETAILS

### CONTACT AND APPLICATION DETAILS

For general information about the MSc please contact:

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

Tel: +44 (0) 1784 443093  
Fax: +44 (0) 1784 430766  
E-mail ISG–Secretary@rhul.ac.uk  
Web Site: <http://www.isg.rhul.ac.uk>

For an on-line version of the application form, please go to:

<http://www.rhul.ac.uk/Studying/Graduate-School/application.pdf>

For more specific queries about the Information Security Group please contact:

Pauline Stoner  
Information Security Group Administrator  
Tel: +44 (0) 1784 443101  
Fax: +44 (0) 1784 430766  
E-mail P.Stoner@rhul.ac.uk

## GENERAL INFORMATION ABOUT THE MSc

### DURATION AND STRUCTURE OF COURSE OF STUDY

#### Course duration

*Full-time* – one full academic year (50 weeks).

*Part-time* – two full academic years (100 weeks).

*Project Submission* – September (week 50 of the academic year).

#### Course structure – full-time students

Full-time students will take the four core modules in their first term, and two or more optional modules in their second term.

#### Course structure – part-time students

Course modules are timetabled to enable part-time students to attend lectures at most one day per week throughout their course of study. In their first year, part-time students will normally take two of the four core modules in the first term, two optional modules in the second term, and the examinations for these four modules in the third term. In their second year, they will take the other two core modules in the first term, up to two optional modules in the second term, and the examinations for these modules in the third term. Part-time students will normally submit their projects in their second year.

## ENTRY REQUIREMENTS

The normal minimum entrance requirement is a second class undergraduate degree (or equivalent) in a relevant discipline, including, but not restricted to, Computer Science, Electronics, Information Systems, and Mathematics. Mature students with industrial experience may, at the discretion of the Graduate School, be granted exemption from the normal entry requirements. Such students are encouraged to apply. Students requiring comprehensive preparation for the MSc may take a qualifying year at the University of London.

Understanding some of the taught material requires background knowledge of computer networks and operating systems, and also some elementary mathematics. However, the level of mathematical knowledge required will not exceed that expected of graduates in the above-mentioned disciplines. For those students lacking the required background, tutorials will be offered during the first few weeks of the term to cover the necessary material.

## OVERVIEW OF PROGRAMME

The MSc degree is taught in course modules. Each module usually consists of three hours of lectures per week, sometimes with tutorials and practical work. As a general rule these lectures are all held on the same day. The duration of a module is one term, which amounts to eleven weeks of lectures (in the first term there is an additional week for induction purposes). As mentioned above, the modules are timetabled to be convenient for part-time students, so that they can attend classes one day per week. For such students this implies a total of 44 days of lectures spread over two years.

The curriculum for the MSc degree consists of six taught modules and a project. Of the six taught modules, four are mandatory core modules and the other two are optional modules chosen by the student from a list of options. The four core modules will be taught in the first term, and the optional modules will be taught in the second term; examinations for all modules will take place in the third term. The project must be submitted by the Friday of the 50th week of the academic year.

The MSc degree thus has three main elements:

- ♦ a *core* element, made up of the four core course modules;
- ♦ an *options* element, made up of the two optional course modules, and
- ♦ a *project* element.

Each element will be separately assessed, and the assessments will then be combined to yield the final degree result (see below).

The four core modules are as follows:

- ♦ Security management – **IC1**
- ♦ An introduction to cryptography and security mechanisms – **IC2**
- ♦ Network security – **IC3**
- ♦ Computer security – **IC4**

The project and the optional modules give students the opportunity to pursue their own interests in more detail.

Exceptionally, subject to approval by the Sub-Board of Examiners, one optional module may be selected from suitable third year undergraduate courses and from courses of other MSc programmes.

The optional modules may be chosen from the following:

- ♦ Secure electronic commerce and other applications – **OPT5**
- ♦ Standards and evaluation criteria – **OPT7**
- ♦ Advanced cryptography – **OPT8**
- ♦ Database security – **OPT9**
- ♦ Computer crime – **OPT10**
- ♦ Other approved modules

The project is a major individual piece of work. It can be of academic nature and aim at acquiring and demonstrating understanding and the ability to reason about some specific area of information security. Alternatively, the project work may document the ability to deal with a practical aspect of information security.

Modules are continually reviewed and revised to keep them up to date with current thinking and practice. All statements made here are subject to University and College regulations.

### EXAMINATIONS

The assessment scheme for the M.Sc. has three elements: the *core*, the *options*, and the *project*. The degree has nine taught modules and a project. Four of the nine taught modules comprise the core (IC1, IC2, IC3, and IC4) and are compulsory. The core mark *C* contributes 50% of the overall mark. The remaining five modules (OPT5, OPT7, OPT8, OPT9, OPT10, other approved

modules) comprise the options, and a student is examined on two out of these five modules. The options mark *O* contributes 25% of the overall mark. Students also have to produce a project dissertation. The project mark contributes 25% of the overall mark.

The taught part of the degree (core and options) is assessed by three three-hour examination papers. Two of the three examinations assess the core; the other assesses the options. The modules examined by each of these papers are detailed in the table below.

Each of these three-hour papers is divided into sections corresponding to the modules assessed by the paper. The core (*C*) mark is the average mark of the two core papers *X* and *Y*, so  $C=(X+Y)/2$ . The options mark (*O*) is the mark for the options paper *Z*.

Both sections of core papers *X* and *Y* are compulsory. Two sections out of five must be answered on options paper *Z*. Each section is weighted equally. The format of each of these sections is similar.

Part-time students take their examinations over two years. By default, first year part-time students are registered for core paper *X* (Security Management and Cryptography) and options paper *Z* (Information Security Options), and that second year part-time students are registered for core paper *Y*

	TITLE OF PAPER	MODULES ASSESSED/SECTIONS
<i>X (MT 5111)</i>	Security Management and Cryptography	IC1, IC2
<i>Y (MT 5112)</i>	Network and Computer Security	IC3, IC4
<i>Z (MT5113)</i>	Information Security Options	OPT5, OPT7, OPT8, OPT9, OPT10, other approved modules

(Network and Computer Security). This part-time examination schedule may be altered with the agreement of the Course Director, and part-time students should consider carefully in which year they wish to take the options paper.

The project will be examined by requiring each student to submit a written project dissertation at the end of the course in September (week 50 of the academic year). An oral examination may take place at the discretion of the examiners. Part-time students will normally hand in their project at the end of their second year, although the end of the first year is also permissible.

## DEGREE CLASSIFICATION SCHEME

To decide whether or not a student will be awarded the MSc degree, and also to decide whether or not a distinction will be awarded, the assessment results from each of the three course elements (the core, options, and project elements) will be used.

To pass the degree programme the student will normally need to achieve each of the following:

- ♦ an average of at least 50%, where the average is computed over the three elements, and where the core is given weight twice that given to the other two elements (i.e. so that the core element contributes 50% of the overall mark, and the other two elements 25% each);
- ♦ a minimum of 50% for the core element;
- ♦ minimum of 40% for the options and project elements, and a minimum of 50% for at least one of these two elements.

To be awarded a distinction in the degree programme the student will normally need to achieve each of the following:

- ♦ an average of at least 70%, where the average is computed over the three elements, and where the core is given weight twice that given to the other two elements (i.e. so that the core element contributes 50% of the overall mark, and the other two elements 25% each);
- ♦ a minimum of 70% for the core element;
- ♦ a minimum of 60% for the options and project elements, and a minimum of 70% for at least one of these two elements.

A student who fails the degree may, in the following year, re-take any element for which an element mark of less than 50% was obtained.

## CURRICULUM DEVELOPMENT

The basic structure of the MSc was widely discussed with more than thirty institutions; these included Government Departments, large IT companies, and many financial organisations. This exercise has ensured that the overall structure of the MSc remains stable.

To ensure that the course is completely up to date, most of the modules involve significant input from recognised security experts from industry. Furthermore, all of the academic staff have links with external organisations that are involved with information security and secure electronic commerce, including many of the largest such organisations in the country.

The main Steering Committee for this course consists of all the members of the Information Security Group at Royal Holloway. Curriculum development is further enhanced

by input from Henry Beker (Visiting Professor at Royal Holloway, University of London), Yvo Desmedt (Professor of Computer Science at Florida State University and Visiting Professor of Information Security at Royal Holloway, University of London), Dieter Gollmann (Microsoft Research, Cambridge (UK) and Visiting Professor at Royal Holloway, University of London) and Michael Walker (Head of Communications Security and Advanced Development Group, Vodafone Ltd and the Vodafone Professor for Telecommunications at Royal Holloway, University of London). Although this latter group has no formal powers their opinions are highly regarded and all their suggestions are therefore taken very seriously and acted upon.

A curriculum committee meets regularly to consider input from the above areas and also from student feedback activities.

## STUDENT SUPPORT

Students are encouraged to discuss any problems arising in their studies with any member of the Information Security Group. Most members of staff can be contacted in their offices during the working day, although if there are problems in contacting individuals then arrangements for meetings may also be made via email or through the ISG secretary.

During the first term, additional tutorials will be arranged to cover necessary background material, depending on the needs of the individual students. Examples of tutorials that might be arranged include a basic introduction to computer networks and operating systems, and elementary mathematics (as necessary to understand the cryptographic concepts).

Tutorials will also be arranged for each of the modules to allow all students to interact with the lecturers in small groups. Typically, each week there will be one day devoted to a particular module, and the module lecturer will conduct a series of tutorials during that day with small groups of students. If required, additional lunchtime provision will also be made for part-time students.

Most modules will include non-assessed coursework, which students are encouraged to complete and submit to the module lecturer for review. Feedback on coursework will be provided to students.

As further student support, many modules have dedicated web-sites where information such as book lists and teaching material is made available. Furthermore, a mailing list of all students on the course can be used for further interaction and information exchange.

## DAVID LINDSAY PRIZE

The British Computer Society Computer Security Specialist Group awards the David Lindsay Prize for the project report that best addresses innovative applications of Information Security. All MSc and BSc projects in the area of Information Security are eligible for the prize. The final decision is made by the British Computer Society Computer Security Specialist Group.

## DETAILS OF MODULES

There follow detailed descriptions of the modules making up the MSc.

## ICI SECURITY MANAGEMENT

First term, core module.

### Aims

This module will emphasise the need for good security management. Its aims are to identify the problems associated with security management and to show how various (major) organisations solve those problems.

### Objectives

On completion of the module, the student will appreciate the complexities of security management, and have seen how some companies attempt to solve these problems.

### Outline of syllabus

There will be 11 sessions lasting about 3 hours. Most sessions will consist of 2 parts:

#### (a)

a lecture lasting from one to one and a half hours given by an outside industrialist and

#### (b)

a discussion lasting from one to one and a half hours on the topics discussed in the lecture led by the academic staff member responsible for the module.

Examples of recently covered topics are:

*Why Security?*

Henry Beker (Visiting Professor)

*Security Architectures as a Strategic Planning Tool*

Gerry Cole (CSS Ltd)

*BS7799 – Information Security as Business Benefit*

Mike Usher (Prudential)

*The Role of Audit in Security Management*

Chris Potter (Pricewaterhouse Coopers)

*Risk Analysis and CRAMM*

Ian Glover & Steve Daniels

(Insight Consulting)

*Business Continuity Planning – A Safety Net for Business*

David Spinks (AEA Technology)

*Building a World Class Info. Sec. Management Framework for the Next Millennium Company Infrastructure*

David Lacey (Consignia)

*The Regulatory Environment*

Chris Amery (Independent)

*IT Security Management in the Real World*

Mark Waghorne (Predictive)

*Security Management – Trying to Put Theory into Action!*

Charles Brookson (DTI)

It is anticipated that future programmes will be similar.

### Method of examination

Written examination

### Module leaders

F.C.Piper, S.Murphy

### Recommended Text

Editors: Krause and Tipton, Handbook of Information Security Management, CRC Press, 2001

### Other References

Scott Barman, Writing Information Security Policies, New Riders, 2002.

Seymour Bosworth and M.E. Kabay (Eds), Computer Security Handbook, Fourth Edition, Wiley, 2002.

Harry B. DeMaio, B2B and Beyond, Wiley, 2001.

Gurpreet Dhillon, Managing Information Systems Security, MacMillan, 1997.

Donn B. Parker, *Fighting Computer Crime*, Wiley, 1998.

## IC2 (SC2) AN INTRODUCTION TO CRYPTOGRAPHY AND SECURITY MECHANISMS

First term, core module.

### Aims

The approach of this module is non-technical. The main objective is to introduce the students to the main types of cryptographic mechanism, to the security services which they can provide, and to their management, including key management. The mathematical content of this module is minimal. Tutorial support for the elementary mathematics needed for this module will be provided if required.

### Objectives

At the end of this module you should be able to:

- ◆ Explain exactly what cryptography can be used for
- ◆ Appreciate the differences between various types of cipher system and in which situations they are most usefully employed
- ◆ Identify the issues that need to be addressed when assessing what types of cryptographic mechanism are necessary to "secure" an application
- ◆ Describe several basic cryptographic mechanisms for providing each of the core security services
- ◆ Identify the limitations of cryptography and how to support it within a full security architecture

Students completing this module should not expect to be able to design algorithms.

### Provisional syllabus

*Cryptographic techniques:* An introductory overview of the aims and types of cryptographic methods. Level of security – cover time and key exhaustion.

*Key management:* Methods of managing keys for symmetric algorithms.

*Stream ciphers:* The one time pad. Pseudo-random key streams – properties and generation.

*Block ciphers:* Confusion and diffusion. Iterated ciphers – substitution/ permutation. The Feistel principle. DES, AES, Modes of operation.

*Public key cryptosystems:* One-way functions and trap-doors. Diffie-Hellman key exchange. RSA. El Gamal cryptosystem.

*MACs:* Using DES. Hash-based MACs.

*Entity Authentication/Identification:* Protocols. Challenge/response.

*Digital signatures:* Digital signature methods – arbiters. Hash functions. SHA-1. DSS. Certificates.

*Public Key infrastructures:* Key management techniques for asymmetric cryptography. X.509 certificates. Directories. Revocation and CRLs. CA interworking.

There will also be a discussion of related legal and national policy issues.

### Method of examination

Written examination

### Module leader

F.C. Piper

### Recommended texts

F. Piper and S. Murphy, *A very short Introduction to Cryptography*, OUP, 2002

S. Levy, *Crypto*, Penguin Books 2000.

S. Singh, *The Code Book*, Fourth Estate 1999.

S. Garfinkel and G. Spafford, *Web Security, Privacy and Commerce*, O'Reilly, 2002.

### Other references

A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

C. Adams and S Lloyd, *Understanding Public-Key Infrastructure*, New Riders, 1999.

D. Kahn, *The Codebreakers*, Scribner, 1967.

H.X. Mel and D. Baker, *Cryptography Decrypted*, Addison-Wesley, 2001.

Richard E. Smith, *Internet Cryptography*, Addison Wesley, 1997.

H.C.A. van Tilborg, *An Introduction to Cryptology*, Kluwer Academic, 1990.

## IC3 NETWORK SECURITY

First term, core module.

### Aims

This module is concerned with the protection of data transferred over commercial information networks, including computer and telecommunications networks. After an initial brief study of current networking concepts, a variety of generic security technologies relevant to networks are studied, including user identification techniques, authentication protocols and

key distribution mechanisms. This leads naturally to consideration of security solutions for a variety of types of practical networks, including LANs, WANs, proprietary computer networks, mobile networks and electronic mail.

### Objectives

At the end of the module students should have gained an understanding of the fundamentals of the provision of security in information networks, as well as an appreciation of some of the problems that arise in devising practical solutions to network security requirements.

### Provisional Syllabus

*Introductory network concepts:* The OSI model and an introduction to computer networks. Example networks and protocols (LANs and IEEE 802, Internet and TCP/IP, ADSL, Cable).

*Introductory network security concepts:* The concepts of security threats, security services and security mechanisms (as in ISO 7498-2). Overview of security for LANs, MANs and WANs.

*Network management security:* SNMP security.

*Identity verification:* Use and storage of conventional passwords. Biometric techniques.

*Authentication and key distribution:* The Kerberos protocol.

*Secure protocols:* IPsec and Virtual Private Networking, SSH, SSL/TLS.

*Network defences:* Firewalls and intrusion detection systems, and the threats they counter.

*Electronic mail security:* Basic e-mail security, Pretty Good Privacy (PGP) and S/MIME.

*Wireless security:* 802.11 and Bluetooth.

*Mobile communications security:* Security in GSM and 3G systems.

### **Method of Examination**

Written examination.

### **Module Leader**

K.Paterson

### **Main references**

W. Stallings, *Network security essentials*, Prentice-Hall (Upper Saddle River, New Jersey), 1999.

W. Stallings, *Cryptography and network security – principles and practice*, Prentice-Hall (Englewood Cliffs, New Jersey), 1998 (2nd edition).

D.E. Comer, *Internetworking with TCP/IP, Vol.1: principles, protocols and architectures*, Prentice-Hall (Upper Saddle River, New Jersey), 2000 (4th edition).

W.R. Cheswick and S.M. Bellovin, *Firewalls and Internet security*, Addison-Wesley (Reading, Mass.), 1994.

## **IC4 COMPUTER SECURITY (OPERATING SYSTEMS)**

First term, core module.

### **Aims**

This course deals with the more technical means of making a computing system secure. This process starts with defining the proper security requirements, which are usually stated as a security policy. Security models formalise those policies and may serve as a reference to check the correctness

of an implementation. The main security features and mechanisms in operating systems will be examined as well as security related issues of computer architecture. Specific well-known operating systems are then studied as case studies. Other areas investigated include the security of middleware, software protection and web security.

### **Objectives**

On completion of this course students should be able to:

- ♦ Demonstrate an understanding of the importance of security models with reference to the security of computer systems.
- ♦ Describe the features and security mechanisms which are generally used to implement security policies.
- ♦ Provide examples of the implementation of such features and mechanisms within particular operating systems.
- ♦ Display a breadth of knowledge of the security vulnerabilities affecting computer systems.
- ♦ Demonstrate an understanding of the main issues relating to Web security in the context of computer systems.

### **Provisional syllabus**

*MSc Lab Security:* An examination of the security features of the computing environment in the MSc Laboratories.

*Concepts and Terminology:* Security: confidentiality, integrity, availability; reliability; security policies; security models.

*Access Control:* Mandatory and discretionary access control, capabilities, access control lists, intermediate controls, lattice models, multilevel security.

*Security Models:* Information flow; Bell-LaPadula model, basic security theorem; integrity models.

*Implementation of Mechanisms:* Security mechanisms in operating systems, memory management, memory protection, logical protection.

*Case Studies:* Linux, RACF, Windows 2000, Smartcards.

*Web Security:* Browser security, server-side includes, cookies, mobile code, malicious code, Java security, software protection.

*Middleware Security:* Distributed security, CORBA security.

### **Method of Examination**

Written examination.

### **Module leaders**

J. Crampton, M.Ganley

### **Main references**

D. Gollmann, *Computer Security*, John Wiley & Sons, to appear 1999.

C.P. Pfleeger, *Security in Computing*, Prentice-Hall, 1997 (second edition).

### **Other references**

S. Garfinkel and G. Spafford: *Practical UNIX and Internet Security*, O'Reilly, 1996.

M. Gasser: *Building a Secure Computer System*, Van Nostrand Reinhold, 1988.

L. Gong: *Inside Java 2 Platform Security*, Addison Wesley, 1999.

S. McClure, J. Scambray and G. Kurtz: *Hacking Exposed*, Osborne McGraw-Hill, 2000 (2nd Ed).

G. McGraw and E.W. Felten: *Securing Java*, Wiley & Sons, 1999.

J.S. Park: *AS/400 Security in a Client/Server Environment*, Wiley & Sons, 1995.

A.D. Rubin, D. Geer and M.J. Ranum: *Web Security Sourcebook*, Wiley & Sons, 1997.

L.D. Stein: *Web Security*, Addison-Wesley, 1998.

## **OPT5 SECURE ELECTRONIC COMMERCE AND OTHER APPLICATIONS**

Second term, optional module.

### **Aims**

This module aims to put the role of security into perspective and demonstrate how it forms part of a security system within an application. The aim is to illustrate, usually by the use of case studies, how a particular situation may make certain aspects of security important and how an entire system might fit together.

### **Objectives**

On completion of the module the students should be able to:

- ♦ recognise the security issues that arise in a variety of applications
- ♦ appreciate how and why particular applications can address various security concerns
- ♦ review how the various security issues in a particular application relate to one another
- ♦ analyse how the security aims are met in a particular application.

### **Provisional syllabus**

The lectures in this module are given by visiting experts in several security application areas who discuss their own specialist topic. There is opportunity for questions and discussion.

Case Studies are likely to include: Protocols for electronic commerce; Banking Applications; Electronic Cash; Baseline protection of IT systems; Electronic Security and Access Controls; Secure mobile communications.

### **Method of examination**

Written examination

### **Module leader**

K. Paterson

## **OPT7 STANDARDS AND EVALUATION CRITERIA**

Second term, optional module.

### **Aims**

Over the last few years, international standards bodies have produced a variety of security-related standards. This module examines some of the most important of these standards in detail. In doing so it illustrates how international standards now cover many aspects of the analysis and design of secure systems. The material covered also puts certain other aspects of the degree course in a more structured setting.

The emerging international standards for general-purpose security mechanisms and services are described in some detail. They are presented within the context of the OSI security architecture. The module also covers existing security evaluation criteria, the current process for evaluating secure

systems, and guidelines for managing IT security.

### **Objectives**

At the end of the module the student should have gained an appreciation of the scope and some of the technical content of existing and emerging security standards. This will have relevance both in the development of security policies, and in the procurement and configuration of systems to meet security policy needs. The topics covered within the module are also of fundamental importance in the specification and development of new security products.

### **Provisional syllabus**

*Network Security Architecture:* The OSI Security Architecture (ISO 7498-2). A very brief look at the ISO security framework standard (ISO/IEC 10181).

*Security mechanism standards:* Encryption algorithms (ISO/IEC 18033 Parts 1-4, NIST FIPS PUB 46-3, AES, and ISO/IEC 9979). Block cipher modes of operation (ISO/IEC 10116). MAC algorithms (ISO/IEC 9797, Parts 1/2). Digital signature techniques (ISO/IEC 9796, Parts 2/3 and ISO/IEC 14888, Parts 1-3). Cryptographic hash-functions (ISO/IEC 10118, Parts 1-4). Non-repudiation mechanisms (ISO/IEC 13888, Parts 1-3). Elliptic curve techniques (ISO/IEC 15946, Parts 1-4).

*Key management:* Key management techniques (ISO/IEC 11770, Parts 1-3). PKI standards (ITU-T X.509, IETF PKIX RFCs). Random bit generation (ISO/IEC 18031). Prime number generation (ISO/IEC 18032).

*Trusted Third Parties:* Guidelines on the use and management of TTPs (ISO/IEC TR 14516). Specification of TTP services to

support the application of digital signatures (ISO/IEC 15945). Time-stamping services (ISO/IEC 18014 Parts 1-3).

*Evaluation Criteria:* TCSEC (Orange Book); TNI (Red Book); ITSEC; Common Criteria (ISO/IEC 15408).

*Management Guidelines:* DTI Code of Practice (BS 7799); other codes of practice; the ISO/IEC Guidelines for the Management of IT Security (ISO/IEC TR 13335, Parts 1-5).

### **Method of examination**

Written examination.

### **Module leader**

C.J. Mitchell.

### **Main references**

W. Ford, *Computer communications security*, Prentice-Hall (Englewood Cliffs, New Jersey), 1994.

W. Stallings, *Cryptography and network security - principles and practice*, Prentice-Hall (Englewood Cliffs, New Jersey), 1998, (2nd edition).

### **Other useful books**

A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997. [Also available electronically at <http://cacr.math.uwaterloo.ca/hac/>]

## **OPT8 ADVANCED CRYPTOGRAPHY**

Second term, optional module.

### **Aims**

This module follows on from the introductory cryptography module (IC2) and provides the basic mathematical background

to cryptography. The emphasis of the module is very much focussed on the most widely used cryptographic processes and algorithms.

### **Objectives**

On completion of this module, students should be able to understand the role of mathematics in cryptographic systems.

### **Provisional syllabus**

*Block Ciphers:* Design criteria, Testing, DES, AES and other algorithms; Assessment of block ciphers; Linear and differential cryptanalysis.

*Stream Ciphers:* System-theoretic and other approaches, LFSRs, Linear equivalence and other measures of complexity; Combining functions; Nonlinear generators; Correlation attacks.

*Asymmetric Cryptosystems:* Finite fields, Factoring and discrete logarithms, Prime generation and testing, ElGamal, RSA, Digital signatures, DSS, Elliptic curve cryptography.

*Quantum Cryptography and Quantum Computing.*

### **Method of examination**

Written examination

### **Module leaders**

S. Murphy, M. Robshaw

### **Main references**

A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

G.J. Simmons (ed), *Contemporary Cryptology*, IEEE Press, 1992.

D. Stinson, *Cryptography: Theory and Practice*, Capman & Hall/CRC Press, Second edition, 2002.

## OPT9 DATABASE SECURITY

Second term, optional module.

### Aims

This module covers several aspects of database security and the related subject of concurrency control in distributed databases. We will discuss methods for concurrency control and failure recovery in distributed databases and the interaction between those methods and security requirements. We will also examine how access control policies can be adapted to relational and object-oriented databases.

### Objectives

At the end of the module the student should

- ♦ understand how multi-level security can be preserved within a database whilst still permitting the concurrent execution of transactions.
- ♦ understand why confidentiality is so difficult to achieve within a statistical database.
- ♦ understand the implications that security and its administration have in the context of commercial databases such as Informix and Oracle.

### Provisional syllabus

*Introduction:* concurrency, fault tolerance and security.

*Concurrency control and failure recovery:* locking strategy and deadlock detection.

*Transaction theory:* serializability and recoverability.

*Distributed Database:* data replication and commit protocols.

*Database Security:* data confidentiality and data integrity, inference and aggregation, security in object-oriented database systems.

### Method of examination

Written examination

### Module leader

Z. Ciechanowicz

### Main references

P.A. Bernstein, V. Hadzilacos and N. Goodman, *Concurrency Control and Recovery in Database Systems*, Addison-Wesley, 1987.

S. Castano, M. Fugini, G. Martella, P. Samarati, *Database Security*, Addison Wesley, 1994.

C.J. Date, *An Introduction to Database Systems*, Volume 1, Addison-Wesley, 1985.

C.J. Date, *An Introduction to Database Systems*, Volume 2, Addison-Wesley, 1985.

D.E. Denning, *Cryptography and Data Security*, Addison-Wesley, 1983.

## OPT10 COMPUTER CRIME

Second term, optional module.

### Aims

This module complements other modules by examining the subject from the criminal angle and presenting a study of computer crime and the computer criminal. We will discuss its history, causes, development and repression through studies of surveys, types of crime, legal measures, and system and human vulnerabilities. We will also examine the effects of computer crime through the

experiences of victims and law enforcement and look at the motives and attitudes of hackers and other computer criminals.

### **Objectives**

On completion of the module students should be able to:

- ♦ follow trends in computer crime
- ♦ relate computer security methodologies to criminal methods
- ♦ detect criminal activity in a computerised environment
- ♦ apply the criminal and civil law to computer criminality
- ♦ understand how viruses, logic bombs and hacking are used by criminals
- ♦ appreciate the views of business, governments, and the media to instances of computer crime.

### **Provisional syllabus**

*Introduction:* Types of computer crime, history, surveys, statistics, global connections.

*Legal Measures:* Computer Misuse, Data Protection, Criminal Damage, Software Piracy, Forgery, Investigative Powers.

*Case Studies:* Investigations into hacking, PC misuse.

*The Commercial View:* The experience of systems managers.

*The Law Enforcement View:* The experience of investigators.

*The Hacker's View:* The experience of cyber people.

*Viruses:* Types, effects, and investigations.

*Network Crimes:* The Internet and links to other networks.

*The Future:* The expansion of the Internet, pornography and unsuitable material, the corporate view.

### **Method of examination**

Written examination

### **Module leader**

J. Austen

### **Main references**

Dorothy E. Denning (Editor), Peter J. Denning (Preface), *Internet Besieged*, Addison-Wesley, 1998.

### **OTHER OPTIONS**

At the time of going to print, the possibility of an extra option centred around smartcards and their applications is being considered. It is also possible that the SC4 module (Legal and Regulatory Aspects of Electronic Commerce), currently only available to Secure Electronic Commerce MSc students, will also become available to Information Security MSc students.

However, neither of these 2 options is guaranteed.

### **MSC PROJECT**

#### **Aims**

A project is a major individual piece of work. It can be of academic nature and aim at acquiring and demonstrating understanding and the ability to reason about some specific area of information security. Alternatively, the project work may document the ability to deal with a practical aspect of information security.

## Objectives

The student will write a comprehensive dissertation on the topic of the project. On completion of the project students should have demonstrated their ability to:

- ♦ work independently on a security-related project for which they have defined the objectives and rationale,
- ♦ apply knowledge about aspects of information security to a particular problem, which may be of an engineering, analytical or academic nature, and
- ♦ produce a well-structured report, including introduction, motivation, analysis, and appropriate references to existing work.

## Assignment and assessment

Each student will have an academic project supervisor who may give advice on the choice of the project and will monitor its progress. However, it is primarily the responsibility of the student to define and plan the MSc project. Students may do their projects off-site provided they have good Internet connectivity.

It is expected that the topic of the project will be agreed upon at the end of the first term and that students will concentrate on their project after the module examinations in May. Some projects may be supported by industrial partners of the Information Security Group. Projects will be assessed on the basis of the written report, and possibly also on evaluation of computer programs or some oral examination, but no invigilated examination.

The closing date for submission of dissertations is in September (the Friday of

week 50 of the academic year). TWO COPIES of the dissertation must be submitted by 4pm on this date. These should be handed to the ISG Office (Room 230 McCrea Building) and a receipt obtained. Candidates are encouraged to submit upon completion of the dissertation.

## Timetable for project work

### *First term*

During the first term students should consider the topic area in which they wish to do their project. Students are encouraged to discuss their ideas with prospective supervisors, a list of whom will be provided at the beginning of the module. By the beginning of the last week of term, every student should inform the Chair of the MSc Project Committee in what area they intend to work, and with whom, if this has been agreed with a prospective supervisor.

### *Second term*

A list of assignments of academic supervisors to students will be circulated at the beginning of the term; this list will be based on the preferences provided at the end of the first term. Each student should meet their supervisor to discuss the scope of the project; such meetings should normally continue through the life of the project. Should the student be seeking an industrial placement they should also meet prospective industrial collaborators.

Every student shall provide the Chair of the MSc Project Committee with the working title of their project and an outline of the scope of the project by the beginning of the third term. Both the title and summary should be agreed with the project supervisor before submission to the Project Committee.

### *June to September*

This is the main period during which work should be undertaken on the project, although some students may wish to start their project work earlier in the year. Advice should be sought from project supervisors, and any other appropriate sources, at all stages, and the supervisor should also be kept informed of progress. It is advised that students should show their supervisor a draft of their project dissertation at least two weeks before the submission deadline.

### **Guidance on structure and content of project dissertation**

There is no page limit to the dissertation. Typically, the project dissertation will be a document of about 50 pages. It must be the work of the candidate, and should be a readable and coherent account of the chosen topic. It should provide an outline of the scope of the project and describe the extent to which the objectives of the project are met. It should also describe its relation to any industrial placement with which it may be associated.

It is important that the students show that they have extended their source material by including a critical analysis of their chosen subject area. A student may do this, for example, by elaborating the treatment as found in the sources, by comparing different approaches to solving a problem, or by performing practical experimentation to inform their analysis. The students should also demonstrate that they appreciate how the topics discussed relate to one another and to the rest of the subject area concerned.

### **Project committee**

P. Wild (Chair), Z. Ciechanowicz, K.Martin.

## **THE INFORMATION SECURITY GROUP**

### **Information Security Group Director:**

Professor Fred Piper

### **MSc Course Director :**

Dr Chez Ciechanowicz

The Information Security Group at Royal Holloway is an interdisciplinary research group comprised of computer scientists and mathematicians. The group has 13 established academic posts and a large number of research students, making it one of the largest academic groups working on information security in the world. The group has strong research links with a number of industrial and government institutions. This is evidenced by a number of distinguished Visiting Professors, a regular seminar series with considerable industrial participation and sponsorship, and the annual Hewlett-Packard Security Colloquium at Royal Holloway.

A recent initiative has been the formation of The Smart Card Centre by Giesecke and Devrient, Vodafone, and Royal Holloway.

Further information regarding the group may be found at the web page:

*[www.isg.rhul.ac.uk/](http://www.isg.rhul.ac.uk/)*

### **ACADEMIC STAFF**

#### **Simon Blackburn BSc (Bristol) DPhil (Oxon)**

Simon Blackburn received his BSc in Mathematics from Bristol University in 1989 and his DPhil in Mathematics from Oxford University in 1992. From 1992–1995, he was a Research Assistant in the Department of Mathematics at Royal Holloway, specialising

in Stream Ciphers. From 1995 to 2000 he was an EPSRC Advanced Fellow. He is currently a Reader in Pure Mathematics. His research interests include combinatorics, group theory and cryptography.

**Zbigniew ‘Chez’ Ciechanowicz, BSc PhD (London),**

Chez Ciechanowicz received his BSc (Hons) in Pure Mathematics in 1975 from the University of London, and his PhD degree in Mathematics (also from the University of London) in 1980. He then worked at the National Physical Laboratory for five years specialising firstly in compiler validation, then in cryptography and digital signatures. He ended his stay at the Laboratory holding the rank of Senior Scientific Officer. His next appointment was as a full-time lecturer in the Computer Science Department of Royal Holloway, his main area of interest being cryptography. Between 1999 and 2001 Chez worked as a consultant at Baltimore Technologies (a company that works exclusively in the area of Information Security). His main areas of interest at Baltimore were risk analysis and security management. Chez has performed numerous security reviews for large Government departments and industrial institutions throughout Europe and the States. He was a principal author of Baltimore’s own risk analysis method. He is editor of the Elsevier Information Security Technical Report. For an extended period Chez was on secondment to the Information Security Group as the Baltimore Teaching Fellow. He is also a member of the BCS ISEB Information Security Management Certificate Board. Chez became a permanent member of the group in 2001.

**Jason Crampton BSc (Manchester) MSc PhD (London)**

Jason Crampton was awarded a BSc (Hons) in Mathematics from the University of Manchester in 1986. He worked as a maths teacher for several years and then for a trade union developing software solutions for the collection, recording and reporting of subscription income. He completed a part time MSc in Computer Science in 1996 and a PhD in 2002. His research interests include role-based access control and the application of partial order theory (and Sperner theory in particular) to access control.

**Hilary Ganley BSc MSc (London)**

Hilary Ganley received her BSc in Mathematics (Hons) from Royal Holloway in 1968. She then held various Mathematics teaching posts including Head of Mathematics at the High School of Glasgow. She was awarded the Postgraduate Certificate of Education at Jordanhill College of Education in December 1975. Following a career break, she completed a Diploma in Computing Science at Glasgow University in 1983, after which she worked as a part-time lecturer in the Computing Science Department, in addition to part-time roles as an Open University tutor and lecturer in Business Studies at Glasgow’s Central College of Commerce. For the last ten years she was (full-time) Director of the MSc in Information Technology at Glasgow University, an interdisciplinary taught postgraduate course of 160 students and was appointed as Senior Lecturer in 1999. During sabbatical leave from Glasgow she returned to Royal Holloway to complete the MSc in Information Security (distinction). She has recently accepted a role within the

Information Security Group with a special interest in developing Royal Holloway's contribution in Information Security to the e-University of the University of London.

**Konstantinos Markantonakis BSc (Lancaster) MSc PhD (London)**

Konstantinos received his BSc (Hons) in Computer Science from Lancaster University in 1995, his MSc in Information Security in 1996 and his PhD in 2000 both from Royal Holloway, University of London. His main areas of interest are smart card security and smart card applications along with security protocol design. Since completing his PhD, he has worked as an independent consultant in a number of information security and smart card related projects. He has worked as a Multi-application smart card Manager in Visa International EU, responsible for multi-application smart card technology for southern Europe. More recently, he was working as a Senior Consultant in Steer Davies Gleave (a transport consultancy company) responsible for advising transport operators and financial institutions on the use of smart card technology. He is also a member of the IFIP Working Group 8.8 on Smart Cards. He is currently a member of the Information Security Group, as a Lecturer in the Smart card Centre. He continues to act as a consultant on a variety of topics around smart card security, smart card migration program planning/project management for financial institutions and transport operators.

**Keith Martin, BSc (Glasgow), PhD (London) C Math FIMA**

Keith Martin joined the Information Security Group as a lecturer in January 2000. He received his BSc (Hons) in Mathematics

from the University of Glasgow in 1988 and a PhD from Royal Holloway in 1991. Between 1992 and 1996 he held a Research Fellowship in the Department of Pure Mathematics at the University of Adelaide, investigating mathematical modeling of cryptographic key distribution problems. In 1996 he joined the COSIC research group of the Katholieke Universiteit Leuven in Belgium where he was primarily involved in an EU ACTS project concerning security for third generation mobile communications. He has also held visiting positions at the University of Wollongong, University of Adelaide and lectured at numerous international institutions. Keith's current research interests include cryptography, mobile security and electronic payment systems. He has served on a number of recent conference program committees and conducts regular refereeing work for international journals. He has provided security consultancy and training for commercial organisations in Australia, Belgium and the U.K.

Keith is also interested in e-learning, and is co-developer of the Information Security Group's contribution to The University of London's Virtual Campus Project.

**Keith Mayes BSc PhD (Bath) CEng MIEE**

Keith received his BSc (Hons) in Electronic Engineering in 1983 from the University of Bath, and his PhD degree in Digital Image Processing (also from the University of Bath) in 1987. During his first degree he was employed by Pye TVT (Philips) which designed and produced TV broadcast and studio equipment. His PhD was sponsored by Honeywell Aerospace and Defence and on completion he accepted their offer of a job. In 1988 he started work for Racal

Research Limited (RRL), at a time when Racal owned its core defence business, Chubb and a small company called Vodafone. During 7 years at RRL he worked on a wide range of research and advanced development products and was accepted as a Chartered Engineer. In 1995 he joined Racal Messenger to continue work on a Vehicle Licence plate recognition system (Talon) and an early packet radio system (Widanet/Paknet). In 1996 Keith joined Vodafone as a Senior Manager working within the Communication Security and Advanced Development group, under Professor Michael Walker. Early work concerned advanced radio relaying systems and involved participation in international standardisation. Later he led the Maths & Modelling team and eventually took charge of the 20 strong Fraud & Security group. During this time he was training in intellectual property and licensing, culminating in membership of the Licensing Executives Society and the added responsibility for patent issues in Vodafone UK. Keith is named inventor on many patent applications. In 2000, following some work on m-commerce and an increasing interest in Smart Cards he joined the Vodafone International organisation as the Vodafone Global SIM Card Manager, responsible for SIM card harmonisation and strategy for the Vodafone Group. In 2002, Keith left Vodafone to set up his own Telecoms Consulting Company (Crisp Telecom) and in November 2002 he also started as the Director of the Smart Card Centre at Royal Holloway.

**Professor Chris Mitchell BSc PhD (London) CEng CMath FBCS FIEE FIMA**  
Chris Mitchell received his BSc (1975) and PhD (1979) degrees in Mathematics from

Westfield College, London University. Prior to his appointment in 1990 as Professor of Computer Science at Royal Holloway, University of London, he was a Project Manager in the Networks and Communications Laboratory of Hewlett-Packard Laboratories in Bristol, which he joined in 1985. Between 1979 and 1985 he was at Racal-Comsec Ltd. (Salisbury, UK), latterly as Chief Mathematician. He has played an active role in a number of international collaborative projects, including the Mobile VCE Core 2 programme, three current EU 5th Framework projects (SHAMAN on mobile security; FingerCard and USB\_Crypt dealing with novel security tokens), and two recent EU ACTS projects on security for third generation mobile telecommunications systems (USECA and ASPeCT). He is currently convenor of Technical Panel 2 of BSI IST/33, dealing with security mechanisms and providing input to ISO/IEC JTC1/SC27 on which he has served as a UK Expert since 1992. He has edited six international security standards and published well over 100 research papers. He is academic editor of Computer and Communications Security Abstracts, and a member of the Editorial Advisory Board for the journals of the London Mathematical Society. He continues to act as a consultant on a variety of topics in information security.

**Sean Murphy BA (Oxon) PhD (Bath)**

Sean Murphy received a BA in Mathematics from Oxford University in 1985 and a PhD in Statistics from the University of Bath in 1988. He has been at Royal Holloway since 1988 and is currently a Reader in the Information Security Group. His research interests centre on cryptology, especially

encryption algorithms. He published some of the early papers on differential cryptanalysis, and has written papers on a variety of cryptographic algorithms such as DES, FEAL, IDEA, SAFER, Twofish and Rijndael.

**Siaw-Lynn Ng BSc (Adelaide) PhD (London)**

Siaw-Lynn Ng was awarded a BSc (Hons) degree in Mathematics from the University of Adelaide in 1995, and a PhD in Mathematics from Royal Holloway, University of London in 1998. She was a post-doctoral research assistant at Royal Holloway from 1998 to 2001. Her research interests includes combinatorics, finite geometry and their applications in information security. Siaw-Lynn was appointed as a lecturer in 2001.

**Kenny Paterson BSc (Glasgow) PhD (London)**

Kenny Paterson obtained his BSc (Hons) in 1990 from the University of Glasgow and a PhD from the University of London in 1993, both in mathematics. He was a Royal Society Fellow at the Swiss Federal Institute of Technology, Zurich, from 1993 to 1994, investigating algebraic properties of block ciphers. After that, he was Lloyd's of London Tercentenary Foundation Fellow at the University of London from 1994 to 1996, working on digital signatures. He joined the mathematics group at Hewlett-Packard Laboratories Bristol in November 1996, becoming project manager in 1999. His technical work there involved him in international standards setting, internal consultancy on a wide range of mathematical and cryptographic subjects, and intellectual property generation. He also continued with more academic activities. As

project manager, he was responsible for running the group and particularly enjoyed the challenge of managing new technology development and transfer to company divisions. Kenny's research interests span a wide range of topics: cryptography and protocols, network security, finite fields and exponential sums, sequences, coding theory and information theory.

**Professor Fred Piper, Information Security Group Director, BSc PhD (London) CEng CMath FIEE ARCS DIC FIMA CISSP**

Fred Piper has been a Professor of Mathematics at the University of London since 1975 and has worked in security since 1979. In 1985 he formed a company, Codes & Ciphers Ltd., which offers consultancy advice in all aspects of information security. He has acted as a consultant to over 50 companies including a number of financial institutions and major industrial companies in the UK, Europe and USA. The consultancy work has been varied and has included algorithm design and analysis, work on EFTPOS and ATM networks, data systems, security audits, risk analysis and the formulation of security policies. He has lectured world-wide on information security, both academically and commercially, has published a number of cryptographic papers, and is joint author of Cipher Systems (1982), one of the first books to be published on the subject of protection of communications, Secure Speech Communications (1985) and Cryptography: A very short introduction (2002). He was a member of ITSAG, the DTI's Information Technology Advisory Group from 1989 – 1991. From 1992 to 1995 he was a member of ITSSQC, the advisory committee to DTI on IT Standards, Security and Quality. He is currently a member of the Foresight Crime

Prevention Panel: IT, Electronics and Communications Task Force, a member of the DTI Management of Information for Fraud Control, Security and Privacy Link Programme, and a member of the Scientific Council of the Smith Institute. He is a member of the Board of Trustees for Bletchley Park. In 2002 he was awarded an IMA gold medal for "services to mathematics" and received an honorary CISSP for "leadership in Information Security".

**Matt Robshaw BSc (St Andrews) PhD (London)**

Matt Robshaw received his BSc Hons from St. Andrews University, and his PhD from Royal Holloway, University of London. Before joining the Information Security Group he was Principal Research Scientist at RSA Laboratories, San Mateo, California where he had worked for six years. He has broad cryptographic research interests, but particularly focuses on the design, analysis, and implementation of cryptographic algorithms. He is a co-designer of the block cipher RC6.

**Scarlet Schwiderski-Grosche Diplom-Informatikerin (Germany) PhD (Cambridge)**

Scarlet finished her degree in computer science at the Technical University of Braunschweig in Germany with the degree of "Diplom-Informatikerin" in 1992. She was awarded a PhD in distributed systems technology (on composite event detection in distributed systems) from Cambridge University in 1996. After a one-year post-doctoral research position in Cambridge, Scarlet worked as a post-doctoral researcher in Darmstadt (Germany) at the GMD - German National Research Centre for

Information Technology (now part of Fraunhofer) on biometrics and wireless communication protocols. In August 2001, she joined the Information Security Group at Royal Holloway to work on an EU-project called SHAMAN (<http://www.ist-shaman.org/>). Scarlet was appointed as Lecturer in Information Security at the beginning of 2003. Her special interests are security in mobile telecommunications systems, e-payment in m-commerce and e-commerce systems, and biometrics.

**Professor Michael Walker BSc PhD (London) Dr.rer.nat.(habil) (Tübingen) CMath FIMA**

Professor Michael Walker is Head of the Communications Security and Advanced Development department at Vodafone and the Vodafone Professor of Telecommunications at Royal Holloway. He is responsible for the security of the Vodafone networks and services and for heading all of the company's research activities. His work includes the new third generation (3G) mobile systems and mobile e-commerce. Prior to joining Vodafone he was Head of Mathematics at Racal Research Ltd. He has led a number of UK and EU collaborative projects on security for mobile communications, and he has designed cryptographic algorithms and security systems for mobile communications systems, satellite systems, EFTPOS, ATM and military tactical radio. He has also acted as a security consultant to a number of financial institutions. Before joining Racal he was a lecturer at the University of Tübingen, where his research interests included geometry, groups, combinatorics and coding theory. He is Chairman of 3GPP SA3, the group responsible for the security features of 3G, and Chairman of ETSI SMG

10 which is responsible for security of GSM. Formally he was Chairman of the ETSI DECT security expert group, Chairman of ETSI TC Security, member of ETSI SAGE and member of BSI IST/33. He has been BSI Principal Technical Expert to ISO/IEC JTC1/SC27.

**Professor Peter Wild BSc (Adelaide) PhD (London)**

Peter Wild received his BSc (Hons) degree in Pure Mathematics in 1976 from the University of Adelaide and the PhD degree in Mathematics in 1980 from the University of London. He has worked at the Ohio State University, Columbus, Ohio; the University of Adelaide; and with the CSIRO, Australia. In 1984 he joined Royal Holloway where he is currently employed as a Professor in Mathematics. His research interests are in combinatorics, design theory, cryptography and coding theory. He has acted as a data security consultant for a number of companies offering advice in algorithm analysis, key management and user identification protocols.

**VISITING PROFESSORS AND SENIOR VISITING FELLOWS**

**Professor Henry Beker BSc PhD (London) BA (Open University) CEng MIEE FIMA FREng**

In 1988 Henry J Beker founded Zergo Limited (which later became Baltimore Technologies plc) and, as Chairman and Chief Executive, steered the company through listings on both sides of the Atlantic and presided over its phenomenal growth. Prior to this, Henry Beker was Managing Director of Racal-Guardata Ltd, having previously held positions of Head of Mathematics Department, Racal Comsec Ltd., and Technical Director at Racal Research Ltd.

In addition to providing security systems to a number of financial institutions worldwide, Henry Beker has also been very actively involved within various Standards bodies. This includes the American National Standards Institute's work on wholesale and retail banking and the Standards Association of Australia formulating their EFTPOS Standards. He is joint author of *Cipher Systems* (1982), one of the first books to be published on the subject of protection of communications, and *Secure Speech Communications* (1985). From 1987-89 he was Vice-President of the IMA, and was appointed President in 1998.

Having relinquished his roles at Baltimore Technologies plc of Chief Executive (in 1999) and Chairman (in 2000), Henry is now devoting more time to his academic, educational and business interests.. Henry is currently leading the e-Learning Foundation initiative to provide portable computers for every schoolchild in the UK and has been instrumental in engaging governmental interest. Henry is Chairman of OverNet Data, an interactive wireless data solutions provider. Henry is also a Non-Executive Director of i-net Venture Capital Trust plc, and of Close Finsbury Eurotech Trust plc.

**Robert Carolina BA (Dayton) JD (Georgetown) LL.M (London) Attorney-at-Law (Illinois, USA) Solicitor (England & Wales), Senior Visiting Fellow**  
Robert Carolina is a Partner in the information technology and communications practice of London law firm Tarlo Lyons, and Senior Visiting Fellow to the Information Security Group. After qualifying as a lawyer in 1991, Robert began his legal career as an in-house lawyer with an Internet software developer in the US. He then worked in the specialist

telecommunications and technology law practice of the world's largest law firm, before joining the partnership of Tarlo Lyons in 1998. His practice focuses entirely upon commercial transactions and projects involving telecommunications and information technology. Robert routinely represents users, purchasers, developers, and vendors of IT and telecommunications products and services, and regularly advises on electronic commerce transactions and projects. His clients include major multinational financial institutions, as well as technology and e-commerce venture companies located in Europe and the US.

**Professor Yvo Desmedt PhD (Leuven)**

Yvo Desmedt was awarded his PhD (Summa cum Laude) from the University of Leuven, Belgium (1984) on industrial cryptography. He is currently Professor in the Department of Computer Science at Florida State University, and Visiting Professor of Information Security at Royal Holloway, University of London. Prior to this he was Professor at the University of Wisconsin – Milwaukee (Computer Science). His interests include cryptography, network security and computer security. He has authored more than 90 papers in international conferences and journals. His research on threshold cryptography is currently funded by the National Science Foundation. His research on survivable computation is funded by DARPA. He was program chair of Crypto '94, has served on more than 10 program committees of conferences on security, and was a director of the International Association for Cryptologic Research. He was the founding director of the Center for Cryptography, Computer and Network Security at the

University of Wisconsin – Milwaukee. He has given 80 invited lectures at such institutes as: Stanford University, Purdue University, University of Cambridge (UK), Oxford University (UK), IBM Research (USA), the National Institute of Standards and Technology (USA), Mitsubishi (Japan), NTT Lab. (Japan), Philips (The Netherlands), etc. He has been an invited speaker at conferences in Australia, France, Italy and Japan. He had visiting positions at ADFA (Australia), the Université de Montréal (Canada), the University of Karlsruhe (Germany), Technion (Israel), the University of New Mexico (USA), the University of Wollongong (Australia), etc. He was also a co-recipient of the first S.W.I.F.T. award.

**Professor Whitfield Diffie, BSc (MIT) Dr. sc. techn. (hc, ETH Zurich)**

Whitfield Diffie, Chief Security Officer of Sun Microsystems, has been at Sun since 1991. Prior to Sun, Diffie was Manager of Secure Systems Research at Northern Telecom, a position he held since 1978. Best known for his 1975 discovery of the concept of public key cryptography, Diffie spent the 1990s working primarily on the public policy aspects of cryptography. His position in opposition to limitations on the business and personal use of cryptography is the subject of a recent book, *\_Crypto\_*, by Steven Levy of Newsweek. In addition, Diffie has been featured in articles of multiple publications, New York Times Magazine, Newsweek, Wired, Omni, and Discover as well as on CNN, the Discovery Channel, the BBC, and the Japanese TV network NHK. Diffie is a fellow of the Marconi Foundation and author, jointly with Susan Landau, of the book *\_Privacy on*

the Line\_. Diffie is a graduate in mathematics of MIT and Dr. sc. techn. (hc) of the ETH in Zurich.

**Professor Dieter Gollmann Dipl.-Ing. Dr.techn. (Linz) Dr.habil. (Karlsruhe)**

Dieter Gollmann received his Dipl.-Ing. in Engineering Mathematics (1979) and Dr.techn. (1984) from the University of Linz, Austria, where he was a research assistant in the Department for System Science. He was a Lecturer in Computer Science at Royal Holloway and later a scientific assistant at the University of Karlsruhe, Germany, where he also served as deputy head of the E.I.S.S. and was awarded the 'venia legendi' for computer science in 1991. He rejoined Royal Holloway in 1990, initially as a Senior Lecturer in Computer Science, subsequently as a Reader, and finally as a Professor. He was a Visiting Professor at the Technical University of Graz in 1991 and an Adjunct Professor at the Information Security Research Centre, QUT, Brisbane, in 1995. He has contributed to national and European projects in the areas of dependable communications and computing. He has been acting as a consultant for HP Laboratories (Bristol). He has been serving on the program committees of the major European conferences on computer security (ESORICS), and cryptography (EUROCRYPT) as well as other international conferences in these areas. Currently, Dieter Gollmann is at Microsoft Research based in Cambridge (UK).

**Professor Richard Walton BSc PhD (Nottingham) BA (Open University) CMath FIMA**

Richard received his BSc (Hons) and PhD in Mathematics from the University of Nottingham in 1968 and 1971 respectively. He studied with the Open University during

the 1980s taking mainly Electronics courses and received his BA (Hons) in 1987. From 1971-1973 he was a lecturer in Mathematics at the North Staffordshire Polytechnic before joining GCHQ as a Mathematician at the end of 1973. His GCHQ career culminated in his appointment in January 1999 to the GCHQ Board as Director CESH, the National Technical Authority for Information Assurance. He held this post until October 2002 when he was seconded to the Cabinet Office for six months to lead the production of a National Strategy on Information Assurance. His earlier posts included Head of the Division employing most of the GCHQ Mathematicians (1996-1999) and Head of the Mathematical Services Group in CESH (1985-1991). In the 1980s he initiated many of the changes in CESH's public profile as they started to engage in open fora, both national and international, during the early stages of the development of open standards for computer security. He was the first member of GCHQ to attend open cryptographic conferences (Eurocrypt in 1982 Crypto in 1985). His actions were instrumental in achieving the change of GCHQ policy to publish the early CESH work on Public Key Cryptography.

## CONSULTANTS TO THE GROUP

**John Austen BA FBICS NEBSS**

John Austen is a director of QCC InfoSec Training Ltd and Course Director for the Royal Holloway Diploma in Information Security. He was the Head of the Computer Crime Unit, New Scotland Yard, until September 1996. He was a career detective for 30 years, investigating the first major UK computer crime in 1976 and founding the Computer Crime Unit in 1984 – the first of its type in the world. He was responsible for

the first successful arrests and prosecutions against hackers, organised crime groups, and information brokers. He trained all of his own staff, officers from each of the UK Police Forces, and latterly police from Eastern Europe on courses held at the National Police Staff College (in Bramshill, Hampshire). He was the first Chairman of the Interpol Computer Crime Committee, serving from 1991 to 1996 and was responsible for the worldwide standardisation of Police procedure. He is a Fellow of the British Computer Society and a member of its Security Committee. He is a consultant to the Government on Computer Security, the Computer Misuse Act, and British Standard 7799. He is a scientific expert to the Legal Affairs Committee, Council of Europe, Strasbourg, and a contributor to its Recommendation for Criminal Procedural Law on Computer Related Crime published in 1995. He has been an official adviser to the Governments of the Czech Republic, Poland, and Croatia. During the last 10 years he has presented lectures to Government committees and international conferences throughout the world.

**Andreas Fuchsberger BSc MSc (London)**

Andreas Fuchsberger received a BSc (Hons) in Computer Science in 1992 and an MSc in Information Security in 1993, both from Royal Holloway, University of London. His research interests lie in the design of security systems using smart cards for use in multimedia applications such as access and intellectual property right control. He is currently completing his PhD thesis on 'The application of smart cards using micropayments for Internet based real-time multimedia'. From 1999 until 2000 he has been employed as a principal Consultant for ISS until he joined eSecurity Inc as Professional Services Director for EMEA.

**Mick Ganley BSc PhD (London)**

Mick graduated from Royal Holloway College in 1968 with a BSc in Mathematics and then obtained a PhD in Algebra and Geometry from Westfield College in 1971. He then held academic appointments in the Mathematics Departments at York University and Glasgow University, with time spent at Washington State University and the University of Western Australia. His primary research interests were in the areas of combinatorics, geometry, algebra and number theory. In 1987 Mick moved into industry, working for the cryptographic security division of Racal. Subsequently, he was made a Racal Senior Manager and appointed as Head of Consultancy and Security Analysis. His main functions included managing all security analysis, audit and consultancy activities carried out by the security division; liaising with other Racal companies and the central Racal product team on new security products and systems; providing security input from research work, new techniques and conference/press feedback; liaising with CESA and the DTI on various security issues relating to the company and carrying out research work and presenting results in published papers and at conferences. During all of this time he maintained close links with Royal Holloway. In 2000, Mick left Racal to take up the position of Director of Consultancy at Cylink Consultancy Ltd. He left this company in mid-2002, to work as a freelance security consultant. His current client list includes a number of major multi-national organisations. He also has a part-time contract with the ISG, for the provision of various consultancy services. Currently, this includes running the IC4 (Computer Security) module of the MSc in Information Security and helping with the development of Distance Learning material.

**Antony Stone BSc (Salford)**

Antony Stone received a BSc (Hons) in Biomedical Electronics from Salford University in 1984, and subsequently joined the DTI Teaching Company Scheme as an Associate. In 1987 he joined an Oxford-based medical electronics company, where he was responsible for developing safety-critical software for patient anaesthesia monitoring systems, and from 1990 to 1998 he ran his own computer consultancy business, specialising in networking and security. He is now Technical Director of Rockstone Ltd, a supplier of Linux-based Firewall systems, and is also on contract to Hewlett-Packard Laboratories in Bristol, working in their Trusted Systems division. He joined the ISG in 2000 as a student on the Information Security MSc, and is now a visiting lecturer in network security and secure operating systems.

*The terms and conditions on which Royal Holloway, University of London makes offers of admission to its programmes of study, including those covered in this booklet, may be found in the Introduction to Postgraduate Study, copies of which are available from the Educational and International Liaison Office in Registry.*

December 2002



## INFORMATION SECURITY GROUP

ROYAL HOLLOWAY, UNIVERSITY OF LONDON  
EGHAM, SURREY TW20 0EX

[www.rhul.ac.uk](http://www.rhul.ac.uk)