Master in Cyber Security
According to a study released by Frost & Sullivan, in Europe, Middle East and Africa there will be a need of 1,15 million Cyber Security Experts by 2015. Despite the strong demand, the education programs specific on Cyber Security are still very limited in most countries. The Global Cyber Security Center Foundation (GCSEC) recognizes the importance of higher education on Cyber Security and will deliver a Master on Cyber Security starting from Fall 2011.

The electronic handling of information is a defining technology 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. The field of Information Security, namely the study of countermeasures to real and serious threats to information security, has grown very rapidly in recent years. The subject embraces technologies such as cryptography, computer security, network security, digital forensics and fraud detection, as well as considering the management of security and the many trade-offs and subjective issues that need to be addressed when implementing information security within an organisation. This MSc is a non-mathematical course. The programme, which can be studied part-time (block mode) or by distance learning, provides students with a systematic understanding and critical awareness of current threats to the security of electronic information and the measures available to counteract these. It is designed to introduce all technical, legal and commercial aspects of Information Security and is intended as a foundation, or a building block, for a career in the field. Students come from a variety of backgrounds, ranging from new graduates through to very senior security managers (often from blue chip enterprises). They are seeking a formal qualification in Information Security on a course that is well respected and well-known as the first of its kind in the world. To date more than 1,500 students from over 40 countries have completed the course.
The program aims to target managers, executives and government officials who want to improve their knowledge and skills on Cyber Security through an internationally recognized Master. The Master is delivered in partnership with Royal Holloway University of London and is based on their famous program built by the historical Information Security Group. At the end of the Master, students will get a legally valid II Level Master Degree issued by GCSEC and Royal Holloway University of London. The program spans a wide range of topics, from technical security to information security governance, from cyber crime to cryptography. The Master has been specifically designed for working managers and executives: the program consists of six one-week modules, delivered in two years for a total of 240 hours of lessons. Students can follow the entire program in Rome, in the new headquarter of GCSEC Foundation, or up to two modules at the Royal Holloway campus in Egham (Surrey - United Kingdom). At the end of the Master program, students will develop a thesis based on a project, that can be hosted by GCSEC Members or Master Sponsors. Participants are expected to find employment in both industry and commerce as Security Managers/Executives: the need for such experts is likely to be very high for the foreseeable future. Each class will have a minimum number of 20 students. The Master will be delivered in English.
The **Global Cyber Security Center (GCSEC)** is an international not-for-profit Foundation based in Rome entirely dedicated to Cyber Security. Founded by Poste Italiane, GCSEC is supported by its members and participants: ENEL Group, Mastercard Corp. and Almaviva. GCSEC has also developed strategic Partnerships with Italian and International government institutions, private bodies and research institutions.

GCSEC is based on a collaborative model where international government institutions, academia, research, industry, operators and associations work together to develop and share knowledge on Cyber Security topics.

In particular the goals of GCSEC are to:
- Act as a leader, facilitator and resource of knowledge and culture in matters pertaining to Cyber Security
- Support Italian and international organizations in acquiring knowledge and experience
- Contribute towards the development of managerial, technical, and operational best practices and standards for better protection of citizens, the government and private organizations
- Advance the policy debate on issues relevant to the secure use of ICTs technologies
- Promote the global harmonization of laws and procedures to counter cybercrime.

The main activities of GCSEC include:
- Providing specialized education and training
- Promoting awareness and communication on Cyber Security
- Initiating and promoting applied Research & Development projects
- Facilitating the exchange of Information between public and private bodies at national and international level
- Providing specialized support to policy makers for the definition of national and international laws, best practices, strategies, and standards.

www.gcsec.org
The Information Security Group is an interdisciplinary research group of computer scientists, mathematicians and social scientists. It is one of the largest academic information security groups in the world (with visiting professors and fellows, research assistants, support staff and around 60 PhD students complementing the core team of 17 academic staff).

It has strong links with a number of industrial and government institutions and, in 1992, it introduced the MSc in Information Security, the first course of its kind in the world.

The Group holds a regular seminar series with considerable industrial participation and sponsorship, and the annual Hewlett-Packard Security Colloquium is held at Royal Holloway.

As well as conducting several research projects funded by government and industry, the information Security Group is active in the European Union research programme ECRYPT and contributes to the International Technology Alliance programme supported by the MoD and DoD.

The ISG incorporates the Smart Card Centre, a venture established by Royal Holloway, Giesecke & Devrient and Vodafone as a venue for research and teaching on smart cards and tokens and their applications.
Depending on students' backgrounds, they might be asked to attend an oral examination or an interview. They will be selected on the basis of their academic and professional curriculum and their knowledge of English. 

Entry requirements for Master are the following:

- Degree (five years) in a relevant discipline (includes, but is not restricted to, computer science, electronics, information systems and mathematics)
- Short degree (3 years) in a relevant discipline (includes, but is not restricted to, computer science, electronics, information systems and mathematics) to get a I Level Master Degree
- High School diploma with appropriate industrial or commercial experience
- A good knowledge of English language is required.

Non-standard applications are viewed sympathetically, each case being considered individually on its merits. Applicants with relevant work experience and industry certifications are particularly encouraged to apply.
The Master program is based on four mandatory courses and two options of alternative courses. At the end of the Master program, students will develop a thesis based on a project, that can be hosted by GCSEC Members or Master Sponsors. Students can follow the entire program in Rome, in the new headquarter of GCSEC Foundation, or up to two optional modules at the Royal Holloway campus in Egham (Surrey - United Kingdom).

**Mandatory Courses**
- Security Management
- Introduction to Cryptography and Security Mechanisms
- Legal and regulatory aspects of electronic commerce
- Security Technologies

**Alternative courses - option 1**
- Application and Business Security Development
- Standards and Evaluation Criteria

**Alternative courses - option 2**
- Computer Crime
- Smart Cards/Tokens Security and Applications

**Assessment**
The mandatory core element (total of four modules) contributes 50 percent towards the final award. The options element (total of two modules) contributes 25 percent towards the final award. The compulsory project element contributes 25 percent towards the final award.

The modules that comprise the core and options elements are all assessed by two-hour written examination papers. For the options element, students must sit at least two options exams. However, students can choose to sit three options exams. In this case, only the two highest marks will be used when determining the classification of the degree (but the degree transcript will still record information about all completed modules).

The Project is a significant piece of individual work assessed by a report of between 10,000 and 20,000 words. As a very rough guide, the project report should be around 50 pages long. This measure assumes fairly dense text, reasonable line spacing, font size (typically between 10 and 12) and the use of reasonable margins.
The Project and the optional modules give students the opportunity to pursue their own interests in more detail. 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.

Other extra optional modules that can be followed only in Royal Holloway campus:
- Network Security
- Computer Security (Operating Systems)
- Advanced Cryptography
- Database Security
- Software Security
- Digital Forensics
- Security Testing Theory & Practice

<table>
<thead>
<tr>
<th>Mandatory courses</th>
<th>Alternative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management</td>
<td>Application &amp; Business Security Development</td>
</tr>
<tr>
<td>Introduction to Cryptography &amp; Security Mechanisms</td>
<td>Security Technologies</td>
</tr>
<tr>
<td>Legal and Regulatory Aspects of e-Commerce</td>
<td>Standard &amp; Evaluation Criteria</td>
</tr>
<tr>
<td>Security Technologies</td>
<td>Computer Crime</td>
</tr>
</tbody>
</table>

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

To pass the MSc 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 merit in the MSc programme the student will normally need to achieve each of the following:
- an average of at least 60%, 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% in each of the three elements (i.e. in the core, options, and project elements).

To be awarded a distinction in the MSc 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 50% in each of the three elements (i.e. in the core, options, and project elements).

The formal Programme Specification is available at:
**Introduction to Cryptography & Security Mechanisms**


**Aims**

The approach of this module is non-technical. The primary objectives are to explain why cryptography is needed, what it provides, how basic cryptographic mechanisms work and what issues need to be addressed when implementing cryptography. The mathematical content of this module is minimal. Tutorial support for the elementary mathematics needed for this part of the course will be provided for those who require it.

**Objectives**

At the end of this module, students should be able to:
- explain exactly what cryptography can be used for
- appreciate the differences between various types of cryptosystems 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.

**Course content**

This course is divided into three parts:

1. Setting the Scene: the need for cryptography; core security services provided by cryptography; basic model of a cryptosystem; historical cryptosystems; security in theory and practice
2. The Cryptographic Toolkit: symmetric encryption algorithms; hash functions; message authentication codes; entity authentication techniques; pseudorandom number generators; public key encryption algorithms; digital signatures; freshness techniques; cryptographic protocols
3. Cryptography in Practice: key management; public key infrastructures; legal aspects of cryptography; cryptographic applications.
Academic staff

Prof Keith Martin B.Sc. (Glasgow), PhD (London), CMath FIMA, is Director of the Information Security Group. He joined the ISG 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 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, working on security for third generation mobile communications. Keith’s current research interests include key management, combinatorial cryptography, applications of cryptography and wireless sensor network security. Keith became Director of the ISG in 2010. He is an Associate Editor of IEEE Transactions on Information Theory in the area of Complexity and Cryptography.

Essential reading:
Highly recommended:

Legal & Regulatory Aspects of Electronic Commerce
Mandatory course, Rome, 20 February-24 February, 2012

Aims
This course, which will be directed almost entirely to non-criminal law with an emphasis on legal obligations and liabilities between private parties, will consider fundamental legal concepts and rules which apply to e-commerce activities; legal risk management techniques for information security managers, and the most significant of the regulatory aspects which apply to secure electronic commerce.
Objectives
On completion of this module, students will have gained an understanding of the legal underpinnings and government regulations applying to the use of e-commerce, as well as an understanding of managing legal risk.

Course content
The module will be divided into three main parts and will involve lectures from a number of legal experts.

Part I: The rules – an introduction to the law
Part II: The rules applied – an introduction to corporate legal risk management
Part III: Regulatory aspects of e-commerce

Academic staff
Mr Robert Carolina B.A. (Dayton) J.D. (Georgetown) LL.M. (London) Attorney-at-Law (Illinois, USA) Solicitor (England & Wales) is a Solicitor of the Supreme Court of England & Wales, and a member of both the American and Illinois Bar Associations. He holds degrees from the University of Dayton (B.A.) Georgetown University (Juris Doctor) and the London School of Economics and Political Science (LL.M in International Business Law). Following a period as an in-house with an Internet software development company, he moved to London in 1992. Robert is a principal with Origin, a law firm based in London that specialises in intellectual property and information technology. 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. Recognised as a leading UK expert on IT law and e-commerce law, he regularly presents academic and commercial courses and workshops on legal aspects of technology procurement and e-commerce. He also serves as the co-editor of Sweet & Maxwell’s Encyclopedia of E-Commerce Law.

Essential reading
Christopher Reed, Internet Law: Text and Materials, Butterworths, 2004

Computer Crime

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, and appreciate the views of business, governments and the media to instances of computer crime.

Course content
- Introduction: types of computer crime, history, surveys, statistics and global connections
- Legal measures: computer misuse, criminal damage, software piracy, forgery, investigative powers
- Case studies: investigations into hacking, cases and PC misuse
- Social engineering
- Spam, phishing and pharming, malware
- DoS and distributed DoS: the causes, mechanisms, case studies and counter-measures
- Network crimes: hacking methodologies via the Internet and attacks to other networks
- Investigations, incident handling and forensic examination
- The future: the expansion of the Internet, pornography and other unsuitable material
- Identity theft and fraud.

Academic staff
Mr John Austen B.A. FBCS NEBSS 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.
Essential reading
Hedley & Aplin, Blackstone's Statutes on IT and E-Commerce, Oxford University Press.

Security Management

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

Objectives
On completion of the module, the student will be able to evaluate security management requirements; critically analyze alternative security management strategies and methods; propose effective methods for solving security management problems, and compare and critically evaluate different approaches to security management.

Course content
The lectures given on this course will mirror the lectures that are given on campus at Royal Holloway. The typical topics that should be covered include Information Security Principles and Management, Governance and the Law, Internal Control and Audit, Risk analysis and Management, Trust, ISO 27001, and Business Continuity.
Dr Lizzie Coles-Kemp B.A.(Hons), M.Sc. Ph.D. (London) was awarded a B.A (Hons) in Scandinavian Studies and Linguistics from the University of Hull in 1988. She then worked as a UNIX software trainer and translator for several years, specialising in applications adapted for variants of secure UNIX. In 1991 she joined the Swedish security software company, Dynamic Software AB, eventually becoming director of the UK subsidiary, DynaSoft Ltd, with responsibility for UNIX security and smart card projects across Europe and in the US. In 1997 Lizzie left DynaSoft to become global IT Security Officer for the British Council and completed the Information Security MSc at Royal Holloway. She was also a Lead Assessor for Lloyds Register Quality Assurance (LRQA) auditing organisations to ISO/IEC 27001 and tScheme. She now works for the ISG as a senior lecturer in information governance and security management for the BSc in Biomedical Informatics which is a collaborative programme between St George’s, University of London, Kingston University and Royal Holloway. Lizzie also contributes to the distance learning version of the Information Security MSc. Her academic research areas are organisational theories applied to design aspects of information security management systems and the visualisation of information security concepts. In 2008 Lizzie completed a Ph.D. in information security management systems at King’s College, London. She is a Primary Investigator on the Visualisation and Other Methods of Expression (VOME) project which is joint research between Cranfield University, Salford University, Royal Holloway (University of London), Sunderland City Council and Consult Hyperion. The project is funded by The Technology Strategy Board, Engineering and Physical Sciences Research Council (EPSRC) and Economic and Social Research Council (ESRC).

Essential reading
Aims
This training programme in smart cards, tokens, security and applications is believed to be unique in terms of its breadth of content material, the depth of information and the quality of international expert lecturers. There is strong emphasis on real-world applications and linkages with industry, making the course an ideal grounding for students considering a future career or preparing for further research in this field.

The course assumes little previous knowledge of smart cards and Radio Frequency Identifiers (RFIDs), and initially leads the students through the basics of smart card and token platforms as well as an in-depth coverage of their secure manufacture. The course moves on to consider major applications of the technology with particular focus on mobile communication, banking, passports/ID, Transport and satellite TV, but also looks to the future and discusses the impact of new technologies, including Trusted Platform Modules (TPM) and Near Field Communication (NFC).

There is a strong emphasis on security aspects through the course, but in particular the formal design criteria for secure smart card/token systems is introduced as well as an insight to the wide range of security attacks and countermeasures that need to be considered when planning commercial products.

The course does not end at the theoretical level but addresses the practical development of applications for smart cards (with particular emphasis on JAVA) and subsequent operational management of issued devices using OTA (Over The Air) and related techniques.

Objectives
By the end of the module the students should:

- have a general understanding of smart cards, RFIDs and their underlying technologies;
- have an appreciation of the trusted production environment used to manufacture smart cards;
- know the various operating systems in use, plus associated interoperability and security properties; understand SIM/USIM cards and how security is provided for mobile telephony;
- have an overview of how smart cards are used for secure banking and finance;
- understand how smart cards are used for passports, IDs and satellite TV;
- be aware of new smart chip & token technologies (including TPM/NFC) for securing platforms and applications;
- understand common-criteria security applied to smart cards and tokens;
- be aware of the range of attacks used against smart cards/RFIDs and their countermeasures plus how smart cards are tested/evaluated;
- understand remote communication with the SIM (OTA) and secure SIM lifecycle management.
**Academic staff**

**Dr Kostas Markantonakis**  B.Sc. (Lancaster University), M.Sc., Ph.D. (London)  
Dr Konstantinos Markantonakis  B.Sc. (Lancaster University), M.Sc., Ph.D. (London)  
received his BSc (Hons) in Computer Science from Lancaster University in 1995, his MSc in Information Security in 1996, his PhD in 2000 and his MBA in International Management in 2005 from Royal Holloway, University of London.  
He is currently a Reader in the Information Security Group. His main research interests include smart card security and applications, secure cryptographic protocol design, Public Key Infrastructures, key management, mobile phone security, embedded systems. 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 Information Security Consultant for Steer Davies Gleave, 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 continues to act as a consultant on a variety of topics including smart card security, key management, information security protocols, mobile devices, smart card migration program planning/project management for financial institutions, transport operators and technology integrators.

**Dr Keith Mayes**  B.Sc. Ph.D. (Bath) CEng MIEE  
received his BSc (Hons) in Electronic Engineering in 1983 from the University of Bath, and his PhD degree in Digital Image Processing in 1987. He is an active researcher/author with publications in numerous conferences, books and journals. His interests include the design of secure protocols, communications architectures and security tokens as well as associated attacks/countermeasures. 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 where 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 (ETSI SMG2). Later he led the Maths & Modelling team and eventually took charge of the 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. 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 Crisp Telecom and in November 2002 he was also appointed as the Director of the Smart Card Centre at Royal Holloway within the Information Security Group. Keith is a Founder Associate Member of the Institute of Information Security Professionals and a member of the Advisory Board for the Sensing and Security Group SIG within the London Technology Network (LTN). He has also had director experience within a London stock market listed company and a subsidiary of an American communications company. Recent high profile activity included leading the expert team that carried out counter-expertise work on the Ov-Chipkaart for the Dutch transport ministry, following published attacks on the MIFARE Classic chip card.

Dr Gerhard Hancke (B.Eng, M.Eng, PhD, CSCIP) received a Bachelor of Engineering degree in Computer Engineering from the University of Pretoria (South Africa) in 2002 and a Masters of Engineering degree from the same institution in 2003, both with distinction. In 2003 he started reading for a PhD in Computer Science with the Security group at the University of Cambridge’s Computer Laboratory, which he completed in 2008. He joined the Information Security Group in 2007 and is responsible for the ISG Smart Card Centre’s RFID/Contactless research track and RF/Hardware laboratory. His main interests are smart hardware tokens and their applications, mobile systems and pervasive computing. Gerhard was recently appointed as a Teaching Fellow within the Information Security Group at Royal Holloway.

**Essential reading**


Security Technologies

Aims
This course will:
- provide an overview of the fundamental technologies underpinning computer and networked applications, along with the associated security issues;
- examine how maintaining security through separation is a key aspect of operating system design;
- provide an overview of the main types of authentication mechanisms used in computer systems;
- describe the fundamental types of access control mechanisms;
- overview the fundamental principles of secure protocol design, and how they are used in deployed security protocols;
- examine the security threats and vulnerabilities found in particular types of networks;
- assess mobile and wireless communication technologies in terms of their security vulnerabilities.

Objectives
On successful completion of the course students will be able to:
- demonstrate a systematic understanding of the construction of information networks, specifically the architecture and operation of the Internet Protocol suite;
- explain the causes and potential effects of vulnerabilities that affect computer systems and identify appropriate countermeasures;
- demonstrate a comprehensive understanding of different types of user authentication mechanisms in use within modern computer systems;
- provide an overview of different access control mechanisms used within computer systems, and evaluate the suitability of different access control mechanisms for different security requirements;
- provide a clear understanding of how strong authentication protocols, key exchange protocols and key exchange mechanisms suitable for use on open networks can be constructed; demonstrate a clear understanding of
how the design principles for secure protocols are applied to the Internet, focussing on SSL/TLS; identify the key security threats faced in network environments, and be able to specify appropriate countermeasures; explain the basic differences between different wireless technologies, and evaluate the security requirements according to the particular needs of different wireless networking technologies.

**Course content**

- Introduction to Computer and Network Architectures
- Introduction to Security
- Platform and Operating System Security
- User Authentication Mechanisms
- Security Models and Access Control Mechanisms
- Malicious Code
- Introduction to Security Protocols
- Network Security Threats and Countermeasures
- Web Security
- Wireless (WLAN and GSM/UMTS) Security

**Essential reading**


**Application & Business Security Developments**

Optional course.

**Aims**

This module will provide an in-depth coverage of some of the current issues and technological developments relating to the security of business and e-commerce applications. It will consider the role of security in perspective and demonstrate how security techniques form part of an application system. It will also examine 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, students should be able to:
unu
identify and analyse the security issues that arise in a variety of applications;
unu
understand how and why particular applications address specific security concerns;
unu
analyze the various security issues in a particular application and explain how they relate to one another, and review how the security aims are met in a particular application.

Course content
The main lectures in this module are delivered by ISG staff, although descriptions of individual case studies may be given by visiting experts in several security application areas who discuss their own specialist topic. There is opportunity for questions and discussion. The precise list of security applications may vary slightly to reflect developments in the subject. However, the initial set of application domains are likely to include: payment and e-commerce applications; web applications, identity management.

Standards & Evaluation Criteria
Optional course.

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 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.

Objectives
At the end of the module, students should:
unu
have a clear understanding and critical awareness of the need for standard information security techniques, and be aware of the various sources for these techniques;
unu
understand the role and basic framework for information security management proposed by ISO/IEC 27001 and ISO/IEC 27002;
unu
understand the risks and safeguards associated with delegating a security service to a third party; understand the differences between a security service and a security mechanism, and how security services and mechanisms are used in the context of the OSI communications architecture;
unu
analyze the security frameworks for key management, access control and authentication;
unu
understand the history and the latest encryption algorithms;
unu
be able to analyze and evaluate the different standardized methods for constructing MACs, hash functions and digital signature schemes from lower level primitives, and compare critically the usefulness of different algorithm choices in different situations;
be able to analyze and evaluate a variety of standardized protocols for providing two parties with entity authentication and key agreement, and compare critically the usefulness of different protocols in different situations;

be able to discuss the development of modern security evaluation criteria;

understand the Common Criteria framework for security evaluation.

Course content
The course consists of 11 lectures covering the following topics: introduction of cryptographic and information security standards; Security Management; Security Architectures; Security Algorithms; Security Protocols; and Evaluation Criteria.

Network Security
This module is concerned with the protection of data transferred over public information networks, including computer and telecommunications networks. After an initial brief study of current networking concepts, a variety of generic security technologies are studied, including user identification techniques, authentication protocols and key distribution mechanisms. This leads naturally to consideration of security solutions for a number of network types, including LANs, WANs and routing aspects, proprietary computer networks, mobile and wireless networks and higher-level applications as exemplified by electronic mail.
Computer Security (Operating Systems)
This course deals with security mechanisms in modern computer systems and will consider the core concepts of memory protections; authentication; important access control models and policies; how access control is implemented in commercial products why operating systems and computer systems remain vulnerable to attack, and how vulnerable systems can be strengthened to increase resistance to attackers.

Advanced Cryptography
This course will introduce students to commonly used cryptographic algorithms; explain the need for algorithms with different properties; cover a wide variety of algorithms and their analysis; study the performance and security trade-offs between different kinds of algorithms, and develop an appreciation of the role of cryptographic algorithms as part of a solution.

Database Security
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 databases.

Software Security
This course will identify the vulnerabilities that can be introduced into programs through language features and poor programming practice; discuss the generic techniques that can be applied to improve the security of programs and applications, and consider the specific support provided for developing secure applications in the .NET Framework and JAVA.
**Digital Forensics**
The module provides a fast-paced overview of the field of digital forensics, covering approaches and techniques for gathering and analysing traces of human and computer-generated activity in such a way that it is suitable for presentation in a court of law. Beginning with legal and procedural aspects, the module encompasses live as well as conventional storage and network forensics with particular emphasis on the limitations and possible counter-forensics techniques employed by skilled adversaries. The module aims to help gain an appreciation of underlying first principles of ways in which data that can subsequently be used as evidence is generated, stored, and transmitted in different environments and mechanisms for both collection and analysis.

**Security Testing Theory & Practice**
The aim of this module is to provide the foundations and theoretical underpinnings for an understanding of the way in which IT systems can be attacked and penetrated by circumventing security or exploiting vulnerabilities in the system. This will form the basis of a methodical approach to surveying and auditing systems, and prepare candidates to design secure systems, identify vulnerabilities, and defend systems against intrusion.
**Overview**
This is a compulsory course that contributes 25 percent to the total marks for the determination of the degree classification.

**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 a 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;
produce a well-structured report, with introduction, motivation, analysis and relevant references to existing work.

Each student will have an academic project supervisor who may give advice on the conduct of the project and will monitor its progress. However, it is primarily the responsibility of the student to define and plan the MSc project.

Some projects may be supported by industrial partners of the Information Security Group.

**Assessment**
Projects will be assessed on the basis of the written report, and possibly on the basis of a demonstration or evaluation of an artifact such as a computer program. An oral examination may take place at the discretion of the examiners.

**Timetable for project work:**

**First term**
At the beginning of the first term each student is assigned a personal advisor. During the term, students should consider, in consultation with their advisor, the topic area in which they wish to do their project. The advisor may act as supervisor of the project or suggest other members of staff whom the student may approach to be their supervisor.

The number of students that any one member of staff may supervise is limited. Students are advised to consult members of staff to ascertain whether they would be able and willing to supervise their proposed project topic. Students may nominate a willing member of staff to be their supervisor in week nine of the first term. Students who do not do so by week 11 will be assigned a supervisor. It is possible to change supervisor (and topic) but such a change would need approval by all parties concerned and fall within the constraints on numbers of students supervised by each individual supervisor.
Second term
Each student should meet his/her supervisor to discuss the scope of the project; such meetings should normally continue through the life of the project. Should students be seeking an industrial placement, they should also meet prospective industrial collaborators. Every student shall provide his/her supervisor with a completed Project Description form by the end of the second term. This form gives details of the project plan, including title, objectives, methods to be used, and work plan.

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 an almost final draft of their project dissertation at least two weeks before the submission deadline.

Guidance on structure and content of project 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 reference their source material appropriately and demonstrate that they appreciate how the topics discussed relate to one another and to the rest of the subject area concerned.

LOCATION
The Master courses location is in Rome, Viale Europa 175, at Poste Italiane offices.
The Global Cyber Security Center is looking for scholarships; companies and institutions that are interested can contact GCSEC at master@gcsec.org

Sponsoring institutions will benefit of the following advantages:

- **visibility to national and international organizations** that will be the target audience for the Master (large corporations, governments, etc)
- **visibility to the international community**; GCSEC will launch and promote the Master at international level through an ad-hoc communication program. Logo of the sponsoring institution will be printed on all the publications and advertising of the MSc Programme (brochure, report, website); the sponsoring Institutions will be invited to participate to all the events related to the MSc Programme, including a launch event in Rome with the participation of Senior Government Representatives
- **engagement with students**, through the scholarship and project.

The engagement of the Sponsoring organisation can also be enriched with other initiatives.

This is a great opportunity to build skills and capabilities in Information Security both in Italy and worldwide.