UNIVERSITY OF LONDON
INTERNATIONAL PROGRAMMES

Programme Regulations 2016–17

Information Security

MSc
PGDip

Important document – please read
This document contains important information that governs your registration, assessment and programme of study

Contents

Important information regarding the Programme Regulations

About this document

Last revised 5 April 2016

Last revised 7 March 2016 (– removal of general provisions section and editing of About this document section)

As a student registered with the University of London you are governed by the current General Regulations and Programme Regulations associated with your programme of study.

The Programme Regulations are designed and developed by the College of the University of London responsible for the programme and they normally take account of the associated arrangements within the College. Programme Regulations, together with the Programme Handbook, will provide the detailed rules and guidance for your programme of study. Further information about how to use the Programme Regulations and Programme Handbook can be found in the Student Guide.

In addition to Programme Regulations you will have to abide by the General Regulations. These regulations apply to all students registered for a programme of study with the International Academy and provide the rules governing registration and assessment on all programmes; they also indicate what you may expect on completion of your programme of study and how you may pursue a complaint, should that be necessary.

Programme Regulations should be read in conjunction with the General Regulations.

A Glossary provides an explanation of the terms used in this document.

If you have a query about any of the programme information provided please contact us. You should use the *ask a question* tab in the student portal https://my.londoninternational.ac.uk.

To note:

Throughout the Regulations, ‘we’ ‘us’ and ‘our’ mean the University of London; ‘you’ and ‘your’ mean the student, or where applicable, all students.

Changes to Information Security Regulations 2016-17

Core modules have been renamed mandatory modules to align nomenclature to that used by Royal Holloway.

The scheme of award has been amended as a Merit will not be awarded if more than one attempt at the examination has been made. This aligns the regulations with those applied to postgraduate taught programmes on campus at Royal Holloway.

1 Structure

1.1

The MSc in Information Security consists of three elements:

- the Core element, comprising four mandatory modules (20 credits each) plus
- the Options element, comprising two modules (20 credits each) chosen from a list of options plus
- a compulsory Project (60 credits).

1.2

The Postgraduate Diploma in Information Security consists of two elements:

- the Core element, comprising four mandatory modules plus
- the Options element, comprising two modules chosen from a list of options.

1.3

The Postgraduate Certificate in Information Security is only available as an exit award.

Mixed mode

1.4

If you are registered for the MSc or Postgraduate Diploma in Information Security, you may be permitted to study one or more modules on campus at Royal Holloway, University of London, through Mixed-mode study.

Mixed-mode study enables students to study some modules by distance learning and others on campus at Royal Holloway, University of London. Whilst on campus, students may study a module over a single term, or over a concentrated period of time (normally one week). Full details on mixed-mode study can be obtained from the Programme Director.

Individual Modules

1.5

All modules from the Information Security degree programme except for the Project are available to study on a stand-alone basis.

1.6

We may decide that you must successfully complete two mandatory modules before we will consider allowing you to register for the Postgraduate Diploma or MSc in Information Security.

2 Registration

Effective date of registration

See the Glossary for the definition of 'effective date of registration'.

2.1

Your effective date of registration will be 1 September in the year that you initially registered. This allows you to sit your first examinations in the following May.

Period of registration

See the Programme Specification for the minimum and maximum periods of registration applicable to this programme.

2.2

If you start by taking Individual modules and then register for the Postgraduate Diploma or MSc in Information Security we will give you a new maximum period of registration for the Postgraduate Diploma or MSc.

Code of conduct

See the Student guide for the code of conduct for online behaviour.

2.3

During virtual seminars and during all other on-line contributions, you must observe the code of conduct for online behaviour.

Conditional offer

2.4

If we have to limit the number of students who can register in any one year and we are not able to offer you a place for that year we will make you a conditional offer of registration for the following year.

3 Recognition of prior learning and credit transfer

Recognition of prior learning

3.1

Accreditation of prior learning will not be considered for the Information Security programme.

Credit transfer

3.2

If you are a student or graduate of the University of London we will consider an application to transfer credit to the Postgraduate Diploma or MSc in Information Security on a discretionary basis. If you are not a student or graduate of the University of London we will not accredit prior learning for any element of the Postgraduate Diploma or MSc in Information Security.

See the Glossary for definitions of credit transfer and recognition of prior learning

4 Module selection

Appendix A provides details of the programme structures and module titles.

Changing modules

4.1

You can apply to change your choice of optional modules at any time. However, if you have notified us that you intend to enter the examination for the module concerned, we will not consider your application to change modules until all of the results for that session are published.

4.2

We will not allow you to change your choice of module if you have taken any element of the assessment for that module.

4.3

If you change your choice of optional modules we may charge you a transfer fee.

Individual modules

4.4

You may take up to four credit bearing modules on a stand-alone basis without being registered for the MSc degree or Postgraduate Diploma. If we allow you to progress to the MSc degree or Postgraduate Diploma you may be credited with any individual modules successfully completed.

5 Assessment for the programme

Assessment methods

Online seminars for modules are not compulsory, but you are strongly encouraged to participate.

5.1

Each module, except *Introduction to Cryptography* and the Project, will be assessed by one two-hour unseen written examination.

Introduction to Cryptography IYM002

5.2

If your effective date of registration is prior to 1 September 2015, the module *IYM002 (Introduction to Cryptography)* will be assessed by one two-hour unseen written examination.

5.3

If your effective date of registration is on or after 1 September 2015, the module *IYM002 (Introduction to Cryptography)* will be assessed by one two-hour unseen written examination (75%) and by submitted coursework (25%).

5.4

From 1 September 2017, all students registered for IYM002 will be assessed by one two-hour unseen written examination (75%) and by submitted coursework (25%).

Project IYM011

5.5

The Project will be assessed by one two-hour written paper and by a submitted dissertation (weighted 20:80).

5.6

The written paper and dissertation that constitute the assessed elements for the Project must be attempted, and respectively submitted, in the same academic year.

5.7

If you start the Project in one academic year, and do not submit the dissertation by 31 March in the same academic year, you will be deemed to have interrupted the Project.

5.8

Once you have been assigned a supervisor for the Project you must submit the Project dissertation and sit the Project examination within three years. If you fail to do so, you will be deemed to have failed the project module and you will be considered for the award of Postgraduate Diploma. If you were supervised for the project module in a session prior to 2015-2016, the three year limit will instead commence in September 2015. If you believe that you are experiencing, or have experienced, mitigating circumstances then you should write, with details, to the Programme Director to request an extension to the project period.

See the General Regulations for more information about mitigating circumstances.

Dates for examinations

5.9

Written examinations take place in May each year.

5.10

For the Project, you must submit an *outline plan* of the dissertation for approval to the Programme Director not later than 31 October in the academic year of submission of the dissertation.

5.11

For the Project, you must submit one *progress report* via your supervisor to the Programme Director by 31 January in the year in which the dissertation is to be submitted. The progress report will not form part of the final assessment, but is an essential study requirement. If you do not submit the progress report you may not be permitted to submit the dissertation.

5.12

You must submit an electronic version of the completed dissertation to arrive not later than 31 March (BST) in the academic year of submission. You must also post two hard copies of the same dissertation to University of London International Programmes. The postmark should confirm postage as no later than 31 March. A dissertation submitted or posted after this deadline may be given a mark of zero except where the Project has been interrupted. In the case of an interruption of the Project the dissertation should be submitted in the following year.

See the Glossary for the definition of ‘examination’ and ‘written examination’.
See General Regulations for further rules for taking written examinations
See the website for the list of examination centres.

6 Number of attempts permitted at an examination

6.1

The maximum number of attempts permitted at any examination is two.

6.2

If you obtain less than 50% in any module (which may include the Project) at a first attempt, and have not yet satisfied the criteria for the award, you may choose to make a second attempt at the examination for that module.

6.3

If you obtain 50% or more in any module (including the Project) you will not be permitted to make a second attempt at the examination for that module.

6.4

If you resit the Project you must re-take all assessed elements of the Project.

6.5

If you obtain less than 50% in any module (which may include the project) at the first attempt and subsequently pass at re-entry you will receive a capped mark of 50% for that module.

6.6

If you resit the assessment for any Core module, Options module or the Project you will carry forward the higher of the two marks achieved. The higher mark achieved will be used for classification purposes.

See Appendix C for information on how to achieve a particular mark.

6.7

An interrupted Project can be resumed the following year and, depending on how much supervision you have received in the academic year the Project was started, the amount of supervision when the Project is resumed will be limited to the unused supervision time. A new supervisor may be appointed if the original one is no longer available.

6.8

If you interrupt your Project in two successive years you will have used up all your due supervision and will have the following options:

- to keep the same Project topic and make another attempt with no further supervision;
- to keep the same Project topic (or a related topic) and make another attempt with reduced supervision;
- to start again with a new Project topic and full supervision.

6.9

If you retake the Project module you have the following options:

- to keep the same Project topic and make another attempt with no further supervision

- to keep the same Project topic (or a related topic) and make another attempt with reduced supervision
- to start again with a new Project topic and full supervision.

6.10

If you submit a Project dissertation you will be considered to have made an attempt at the Project.

See the Fee Schedule for details of fees that may be payable.

7 Progression within the programme

See section 4 for method of assessment.

7.1

In any one year you may attempt examinations of up to a maximum of six modules, excluding re-sits.

7.2

If you are registered for the MSc in Information Security you must have completed the Core element, obtained at least 40% in all examined modules and not have more than two module marks below 50% before proceeding to the Project.

Transfer from the Postgraduate Diploma in Information Security to the MSc in Information Security

7.3

If you successfully complete the Postgraduate Diploma in Information Security you will normally be permitted to transfer your registration to the MSc in Information Security and receive appropriate credits.

7.4

To progress to the MSc degree in Information Security you must have qualified for the award of the Postgraduate Diploma in Information Security, and received a recommendation from the Board of Examiners that you may register for the Project element for the MSc degree. If you satisfy these requirements and wish to progress you must do so in the same year that you qualify for the Postgraduate Diploma. There is no automatic progression.

Transfer from the MSc in Information Security to the Postgraduate Diploma in Information Security

7.5

If you are registered for the MSc degree in Information Security you may transfer to the Postgraduate Diploma at any time providing you are able to satisfy the conditions for that award.

Transfer from Individual modules

7.6

A mark or grade awarded for completion of an individual module may not be used to replace any mark or grade for a degree or diploma already awarded.

Previous study recommended for Options modules

7.7

Students with relevant professional experience are not required to have completed the previous study before taking Options modules, but are recommended to have done so.

Options module	Recommended previous study
Application Security	Security Management Introduction to Cryptography and Security Mechanisms Network Security
Advanced Cryptography	An Introduction to Cryptography and Security Mechanisms
Database security	None
Cybercrime	None
Smart cards/tokens security and applications	An Introduction to Cryptography and Security Mechanisms
Digital Forensics	Network Security Computer Security
Security Testing: Theory and Practice	Network Security Computer Security

8 Schemes of award

MSc in Information Security

8.1

To be considered for the award of the MSc, you must have:

attempted the examinations and dissertation for all three elements of the degree:

- the Core element [comprising four mandatory core modules];
- the Options element [comprising two modules chosen from a list of options]
- the Project element [comprising one examination and one dissertation]

and

- obtained an overall module average of at least 50% (where each module is weighted according to its credit value, namely 60 for the project and 20 otherwise) **and**
- obtained at least 40% in every Core and Options module **and**
- obtained at least 50% in at least four of the Core and Options modules **and**
- obtained at least 50% in the Project element.

8.2

To be considered for an award with *distinction* for the MSc in Information Security, you must have obtained an overall average of at least 70% (using the same weighting as applies in 8.1).

If you have made more than one attempt at the examination for a module you will not normally be considered for the award of distinction.

8.3

To be considered for an award with *merit* for the MSc in Information Security, you must have obtained an overall average of at least 60% (using the same weighting as applies in 8.1).

If you have made more than one attempt at the examination for a module you will not normally be considered for the award of merit.

Postgraduate Diploma in Information Security

8.4

To be considered for the award of the Postgraduate Diploma, you must have:

attempted the examinations for both elements of the Postgraduate Diploma:

- the Core element [comprising of four mandatory modules];
- the Options element [comprising two modules chosen from a list of options]

and

- obtained an overall average of at least 50% (where all modules have equal weight) **and**
- obtained at least 40% in every module **and**
- obtained at least 50% in at least four modules.

8.5

To be considered for an award with *distinction* for the Postgraduate Diploma in Information Security, you must have:

- obtained an overall average of at least 70%.

If you have made more than one attempt at the examination for a module you will not normally be considered for the award of distinction.

8.6

To be considered for an award with *merit* for the Postgraduate Diploma in Information Security, you must have:

- obtained an overall average of at least 60%.

If you have made more than one attempt at the examination for a module you will not normally be considered for the award of merit.

Postgraduate Diploma in Information Security as an intermediate or exit award

8.7

If you registered for the MSc degree in Information Security you may be awarded the Postgraduate Diploma as an exit award if you are unable to complete the requirements of the MSc degree but you have attempted all assessment components for at least 120 credits' worth of modules, which may include the Project, and, for these modules

- obtained an overall average of at least 50% (where each module is weighted according to its credit value, namely 60 for the Project and 20 otherwise) **and**
- obtained at least 40% in each module **and**
- obtained at least 50% over at least 100 credits' worth.

In this event, the date of award for the Postgraduate Diploma will be the year in which you satisfied these requirements.

8.8

The Postgraduate Diploma in Information Security as an intermediate or exit award may be awarded with merit or with distinction. If the Project element has been taken, this too, can be considered for grading purposes by the Board of Examiners along with the core and options modules.

Postgraduate Certificate in Information Security as an exit award

8.9

We may award the Postgraduate Certificate in Information Security as an exit award if you do not complete the requirements of the Postgraduate Diploma or MSc degree, but do pass (with a mark of at least 50%) taught (i.e. non-Project) modules to the value of at least 60 credits.

8.10

The Board of Examiners will decide if you can be awarded the Postgraduate Certificate in Information Security. The Board of Examiners must be satisfied that the award represents a coherent programme of study.

8.11

To be considered for an award with distinction for the Postgraduate Certificate in Information Security, you must have obtained an overall average of at least 70%. If you have made more than one attempt at the examination for a module which contributes to the certificate you will not normally be considered for the award of distinction.

8.12

To be considered for an award with merit for the Postgraduate Certificate in Information Security, you must have obtained an overall average of at least 60%.

8.13

All assessments for the Postgraduate Certificate are marked and graded according to the assessment criteria for the degree in Information Security.

8.14

If we award you the Postgraduate Certificate in Information Security you may not subsequently be awarded the Postgraduate Diploma or MSc in Information Security.

Appendix A – Structure of the programmes

The syllabus for each module is provided in Appendix B.

Postgraduate Diploma in Information Security

Core element

Four mandatory modules:

Security management [IYM001] *(20 credits)*

An introduction to cryptography and security mechanisms [IYM002] *(20 credits)*

Network security [IYM003] *(20 credits)*

Computer security [IYM004] *(20 credits)*

+

Options element

Two modules chosen from the following:

Application security [IYM005] *(formerly known as Secure electronic commerce and other applications) (20 credits)*

Advanced cryptography [IYM008] *(20 credits)*

Database security [IYM009] * (*20 credits)*

Cybercrime [IYM010] *(formerly known as Information crime) (20 credits)*

Smart cards/tokens security and applications [IYM012] (*20 credits)*

Digital forensics [IYM015] *(20 credits)*

Security testing – theory and practice [IYM016] (*20 credits)*

Note

1. * Database security [IYM009] is scheduled for closure. The module is only available to students with an effective date of registration of 1 September 2015 or before. Database Security [IYM009] will be tutored for the last time in 2016-17. Examinations (be it a first or second attempt) will be held in May 2017 and for the final time in May 2018.
2. The examination numbers are appended to the module titles in Appendix B and these numbers should be used when completing examination entry forms.
3. For mixed-mode study options see also regulation 1.4.

MSc in Information Security

Core element

Four mandatory modules:

Security management [IYM001] *(20 credits)*

An introduction to cryptography and security mechanisms [IYM002] *(20 credits)*

Network security [IYM003] *(20 credits)*

Computer security [IYM004] *(20 credits)*

+

Options element

Two modules chosen from the following:

Application security [IYM005] *(formerly known as Secure electronic commerce and other applications) (20 credits)*

Advanced cryptography [IYM008] *(20 credits)*

Database security [IYM009] **(20 credits)*

Cybercrime [IYM010] *(formerly known as Information crime) (20 credits)*

Smart cards/tokens security and applications [IYM012] *(20 credits)*

Digital forensics [IYM015] *(20 credits)*

Security testing – theory and practice [IYM016] *(20 credits)*

+

Project element

Project *[IYM011]* *(compulsory) (60 credits)*

Note

1. * Database security [IYM009] is scheduled for closure. The module is only available to students with an effective date of registration of 1 September 2015 or before. Database Security [IYM009] will be tutored for the last time in 2016-17. Examinations (be it a first or second attempt) will be held in May 2017 and for the final time in May 2018.
2. The examination numbers are appended to the module titles in Appendix B and these numbers should be used when completing examination entry forms.
3. For mixed-mode study options see also regulation 1.4.

Appendix B – Module Outlines

Core element

Security management [IYM001]

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.

Assessment

One two-hour unseen written paper.

An introduction to cryptography and security mechanisms [IYM002]

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. Support materials for the elementary mathematics needed for this module will be provided.

Objectives

On completion of this module students will have gained an understanding of the use of, and services provided by, the main types of cryptographic scheme. They should also have gained an appreciation of the need for good key management. This will include an appreciation of the general nature of: encryption techniques for providing confidentiality services (including stream ciphers, block ciphers and public key techniques), mechanisms for providing data integrity and origin authentication, including MACs and digital signatures, message exchanges to provide entity authentication and/or key establishment, and the use of Trusted Third Parties, such as Certification Authorities (CAs), to provide and support Public Key Infrastructures.

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

Assessment

One two-hour unseen written paper (75%) and one assignment (25%).

Permitted Aids in the written examination: A hand-held non-programmable calculator may be used in this examination.

Network security [IYM003]

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.

Assessment

One two-hour unseen written paper.

Computer security [IYM004]

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.

Assessment

One two-hour unseen written paper.

Options element

Application Security [IYM005] (formerly known as Secure electronic commerce and other applications [IYM005])

Aims

This module analyses the role of security from the perspective of business application design. The aim is to learn the fundamental processes that need to be incorporated into the application development lifecycle, and thus how to integrate security as a core component within an application architecture. This module uses case studies to support the learning of these fundamental application security design skills, to understand what decisions need to be made to both meet business requirements and to mitigate information security risks.

Objectives

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

- Recognise a variety of security issues that arise in applications
- Review how the various security issues in a particular application relate to one another
- Understand how and why businesses address specific security concerns in their applications
- Appreciate the various aspects of integrating security into the application development lifecycle
- Analyse how security aims are met in a particular application
- Evaluate the effectiveness of security mechanisms in the technical and business context of the case studies.

Assessment

One two-hour unseen written paper.

Advanced cryptography [IYM008]

Aims

This module follows on from the introductory cryptography module (IYM002). In that module, cryptographic algorithms were introduced according to the properties they possessed and how they might fit into a larger security architecture. In this unit we look inside some of the most popular and widely deployed algorithms and we highlight design and cryptanalytic trends over the past twenty years. This course is, by necessity, somewhat mathematical and some basic mathematical techniques will be used. However, despite this reliance on mathematical techniques, the emphasis of the module is on understanding the more practical aspects of the performance and security of some of the most widely used cryptographic algorithms.

Objectives

On completion of this module, students will gain a broad familiarity of the inner-workings of many of today's most widely deployed cryptographic algorithms. Students will also develop a more detailed understanding of some of the most prominent algorithms.

Assessment

One two-hour unseen written paper.
Permitted Aids in the written examination: A hand-held non-programmable calculator may be used in this examination.

Database security [IYM009]

Note

Database security [IYM009] is scheduled for closure. The module is only available to students with an effective date of registration of 1 September 2015 or before. Database Security [IYM009] will be tutored for the last time in 2016-17. Examinations (be it a first or second attempt) will be held in May 2017 and for the final time in May 2018.

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.

Assessment

One two-hour unseen written paper.

Cybercrime [IYM010]

(Formerly known as Information crime [IYM010])

Aims

This module complements other modules by examining the subject from the criminal angle and presenting a study of cybercrime and the cyber 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 cybercrime 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
- understand the need to gather and preserve digital evidence correctly so that legal actions can be brought.

Assessment

One two-hour unseen written paper.

Smart cards/tokens security and applications [IYM012]

Aims

This course will:

- provide an overview of smart cards/tokens and their properties
- introduce various applications that exploit smart cards/tokens
- examine benefits, threats and attacks
- consider systems for the development, manufacture and management of smart cards/tokens
- review smart card standards and security evaluation methodologies

Objectives

On completion of this module students will be able to:

- identify constituent components, analyse strengths and weaknesses and identify new applications of smart cards
- identify the steps in the manufacturing/personalisation processes, analyse and evaluate potential risks, and compare security safeguards
- identify and compare the systems in use, analyse their strengths and weaknesses, and evaluate interoperability and security issues
- analyse the range of capabilities of SIM/USIM cards and apply them to new service ideas, and evaluate the possible range of services and security measures
- understand the main standards and applications of smart cards for banking and finance, compare them with earlier card solutions, and analyse strengths and weaknesses of the approaches
- analyse the key role of the smart card for passports, IDs and satellite TV, and evaluate the security measures that have protected past and current cards
- identify and describe new technologies, including TPMs, apply them to new applications and evaluate the likely suitability/success of such approaches
- explain how Common Criteria may affect smart card design/development, analyse the different approaches and compare them with less formal methods

- identify and describe the classes of attack and notable methods within each class, analyse countermeasures and evaluate practicality of attacks
- identify, compare and evaluate different methods of developing applications for smart cards, and understand the development cycle and the use of practical tools
- analyse the issues concerning smart card lifestyle management, and evaluate and compare methods of local and remote card management.

Assessment

One two-hour unseen written paper.

Digital forensics [IYM015]

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.

Learning Outcomes

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.

Assessment

One two-hour unseen written paper.

Security testing – theory and practice [IYM016]

Aims

This course provide the foundation and theoretical underpinning which aims to give an understanding of the way in which IT systems can be attacked and penetrated by circumventing security or exploiting vulnerabilities in the system. This foundation forms the basis of a methodical approach to surveying and auditing systems, and prepares candidates to design secure systems, identify vulnerabilities, and defend systems against intrusion.

Objectives

On completion of this module students will have:

- Gained an understanding of common approaches and methodologies used for carrying out and managing security and penetration testing, as well as an understanding of the legal aspects involved in such audits.

- Gained a detailed understanding of some typical network protocols, relevant computer system architectures, and web application systems.
- Gained an understanding of the vulnerabilities in some existing protocols, systems, and applications, and some common forms of attack; in addition, an understanding of the security technologies designed to mitigate these vulnerabilities.
- Gained practical experience of how these vulnerabilities may be exploited in practice to penetrate a system.

Assessment

One two-hour unseen written paper.

Project element

Project [IYM011]

Aims

The Project is a major individual piece of work. It can be of academic nature and aimed 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 an information security topic. 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.

Supervisor

Each student will be assigned 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.

Assessment

One two-hour unseen written paper and by submission of a dissertation.

Appendix C – Assessment Criteria

Where examinations feature essay-style questions, the following grade description criteria apply:

%	No specific marks are awarded for spelling, punctuation or grammar. However, any significant weaknesses in these areas which result in the examiner having difficulty comprehending an answer may result in less credit being awarded.
85+	Outstanding levels of accuracy and technical competence; deep understanding; near-comprehensive knowledge; exceptional independence of thought; exceptionally well-organised and original answers; high levels of ability in analysis of information; coherent structure; completely addresses all aspects of the question. As good as could be expected under examination conditions.
70-84	Very high levels of accuracy and technical competence; deep understanding; detailed knowledge; may show some originality in interpretation or analysis; high degree of creativity and independence of thought; high levels of ability in the analysis of quantitative or qualitative information; coherent structure; completely addresses all aspects of the question.
60-69	Good degree of accuracy and technical competence; clear understanding; good breadth of knowledge; some evidence of creativity and independence of thought; generally effective analysis of quantitative or qualitative information; coherent structure; arguments are well constructed; addresses most key aspects of the question.
50-59	Satisfactory degree of competence and technical accuracy; sound understanding and knowledge; familiarity with correct strategies for analysis of quantitative or qualitative information, but possibly with limitations in the process of analysis; adequate structure; there may be some omissions, limited clarity of expression and partial or incomplete understanding of some areas of the topic; addresses some key aspects of the question.
Pass at 50	
40-49	There are some significant omissions or technical inaccuracies; some general understanding and knowledge; weaknesses in detail; the essay may not be fully focused on the question asked; familiarity with correct strategies for analysis of quantitative or qualitative information, but with significant errors in the process of analysis; simple structure.
Condonable 40	
20-39	There are serious technical errors and/or omissions that indicate poor understanding; there may be a failure to address the question as asked; information largely erroneous or has little or no relevance to the question; significant confusion over appropriate analysis of quantitative or qualitative information; analytical work incomplete and erroneous; inadequate structure, with no sense of logical argument.

0-19	The answer shows a clear lack of understanding with major technical errors and omissions; there is little attempt to address the question; information erroneous or has no relevance to the question; substantial error and confusion over appropriate analysis of quantitative or qualitative information; complete inability to analyse information; incomplete, fragmentary or chaotic structure. Individual marks may be gained for individual accurate facts.

Grade description for Dissertation

%	
85+	Exceptional understanding of subject area; exceptional depth of content; outstanding technical accuracy and competence; significant originality in the construction of its research aims and questions; penetrating analysis and critical evaluation; ability to make informed judgements and develop original insights; ability to establish original lines of inquiry; employ different approaches to provide solutions to highly complex and novel problems. Professionally presented; written in an incisive and fluent style with few or no errors; clearly publishable standard of referencing. A high level distinction dissertation should be publishable with editing and minor revision.
70–84	Authoritative understanding of subject area; high degree of depth of content; very high technical accuracy and competence; some originality in statement and fulfilment of aims; ability to analyse critically and formulate questions; excellent research potential; ability to employ different approaches to the solution of complex and novel problems. Excellent presentation; written in a fluent and incisive style with no significant errors; close to publishable standard of referencing. A distinction dissertation should demonstrate professional standards of research.
60–69	Convincing display of understanding of subject area; good all round depth of content; good technical accuracy and competence; very satisfactory fulfilment of aims; challenging in parts; ability to analyse critically; clear evidence of the potential to undertake original research given appropriate guidance and support; ability to solve complex, though not entirely original problems. Well-presented and structured; written in a fluent style, with few errors; good referencing standard.

50–59	Sound knowledge and understanding of subject area; satisfactory depth of content; satisfactory sufficiency of content; satisfactory technical accuracy and competence; aims and objectives represent an acceptable challenge; satisfactory fulfilment of aims and objectives; ability to construct coherent and relevant answers to questions; few signs of originality and independence of thought; adequately presented and structured; straightforward presentational style with some errors; adequate referencing standard.
Pass at 50	
40–49	Basic knowledge and understanding of subject area; basic depth of content; borderline sufficiency of content; lack of clarity and accuracy in technical competence; aims fall just below an acceptable standard *and/or* failure to fulfil stated aims; answers are either incomplete or not entirely coherent; little evidence of independent thought; weak presentation *or* limited structure; presentation lacks clarity; significant errors of spelling, punctuation or grammar; weak referencing *and/or* inadequate bibliography.
Condonable 40	
20–39	Fragmentary knowledge and understanding of subject area; limited depth of content; limited sufficiency of content; little or fragmentary accuracy of technical content; no clear aims or questions asked; answers show only a limited degree of understanding; almost no evidence of independent thought. Poorly presented *and/or* inadequate structure; consistent lack of clarity throughout; significant errors of spelling, punctuation or grammar; little or no referencing and inadequate bibliography.
0–19	Entirely lacking in knowledge and understanding of subject area; totally inappropriate depth of content; totally inappropriate sufficiency of content; entirely lacking accuracy of technical content; no aims or questions asked; totally devoid of independent thought; poorly presented and/or inadequate structure; confused and incoherent; substantial errors of spelling, punctuation or grammar; no references and absent bibliography.