Information Security
MSc and Postgraduate Diploma

Syllabus

Security management [690IC01]
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.

An introduction to cryptography and security mechanisms [690IC02]
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.

Network security [690IC03]
Aims
This module is concerned with the protect-ion 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.

Computer security [690IC04]
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.

Secure electronic commerce and other applications [690OPT5]
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.

Standards and evaluation criteria [690OPT7]
Aims
Over the last few years, a variety of security-related standards have been produced by international standards bodies. 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.

Advanced cryptography [690OPT8]
Aims
This module follows on from the introductory cryptography module (IC02). In IC02 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.

Database security [690OPT9]
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.

Information crime [690OPT10]
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.

Smart cards/tokens security and applications [690OP12]

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 the 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, evaluate the possible range of services and security measures
- understand the main standards and applications of smart cards for banking and finance, compare with earlier card solutions and analyse strengths and weaknesses of approaches
- analyse the key role of the smart card for passports, IDs and satellite TV, evaluate the security measures that have protected past and current cards
- identify and describe new technologies, including TPM and apply them to new application and evaluate the likely suitability/success of approach
- explain how common criteria may affect smart card design/development, analyse the different approaches and compare 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.

Digital forensics [IYM015]

Aims

The objective of this module is to provide the foundations and theoretical underpinnings for an understanding of the way in which data that can subsequently be used as evidence is generated, stored, and transmitted. Based on this, methods for the collection and analysis of digital evidence are covered which will not alter the underlying data or potentially trigger destructive mechanisms and which can be reproduced reliably. Beyond the technical underpinnings, the module is to provide an understanding of general and UK legal requirements as well as resulting frameworks for the handling and processing of such evidence.

Objectives

After completing this course, students will have:

- an understanding of the legal requirements for gathering, storing, transmitting, and processing evidence mainly within the United Kingdom and, where appropriate, in other European Union member states
- learned about procedures and recognised practices for handling digital evidence
- gained an understanding of audit and indirect activity records retained by operating systems, particularly in file systems, and on how to retrieve such information
- understanding of selected network protocols and the collection and derivation of evidence leading to the reconstruction of system and user activity based on network trace information
- learned about infiltration and anti-forensics techniques used particularly by malicious software
- gained an overview of steganographic and particularly steganalytical methods for different types of media
- obtained understanding of retention characteristics of storage systems and non-standard devices such as mobile/smart phones, cloud computing, and vehicular systems.

Project [6900011]

Aims

A 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 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.

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.