Liverpool John Moores University

Title:	COMPUTER SECURITY
Status:	Definitive
Code:	**7505DCOM** (103696)
Version Start Date:	01-08-2012
Owning School/Faculty:	Computing and Mathematical Sciences
Teaching School/Faculty:	Dublin Business School

Team	Leader
Robert Askwith	Y

Academic Level:	FHEQ7	**Credit Value:**	15.00	**Total Delivered Hours:**	38.00
Total Learning Hours:	150	**Private Study:**	112		

Delivery Options
Course typically offered: Semester 1

Component	Contact Hours
Lecture	12.000
Tutorial	24.000

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Exam	AS1	Examination	50.0	2.00
Report	AS2	Study and critical evaluation of security strategies applied to a given case study	50.0	

Aims

To fully develop an in-depth knowledge of various security threats and vulnerabilities in computer systems as well as the importance of computer security.
To critically assess a variety of generic security technologies for protection of computer systems.
To synthesise and ensure the use of best practice methodologies and tools in the analysis, design and management of secure systems.
To critically examine current research issues in computer security.

Learning Outcomes

After completing the module the student should be able to:

1	Identify and critically analyse a variety of security threats and vulnerabilities and assess their impacts on given computer applications.
2	Select, specify and apply best practice security requirements for countering security problems identified for given applications.
3	Identify and apply a variety of security techniques and tools to develop appropriate security mechanisms and solutions for protection of computer systems.
4	Synthesise the knowledge of current research issues and directions of computer security.

Learning Outcomes of Assessments

The assessment item list is assessed via the learning outcomes listed:

EXAM	1	2	3	4
Report	1	2		

Outline Syllabus

Fundamentals of computer security - Security concepts: confidentiality, integrity, availability and security policies. Security problems: security breaches and vulnerabilities. Information encryption and decryption: terminology, systems and applications. Risk analysis and security management: principles, techniques, processes and standards.

Personal computer security - Security problems. Security measures: access control; file protection and password selection criteria. Computer viruses: examples, sources and prevention. Secure systems: security penetration, security models and design issues.

Network security - Threats to computer networks. Crypto key management: protocols and services. Digital signatures: importance and methods. Authentication: principles, protocols and services. Network access control: policies and mechanisms. Security applications: secure electronic commerce, and payment protocols.

Database security: Data classification. Security requirements: integrity, authentication and access control. Techniques for multilevel security: partitioning, integrity locking, data encryption, and secure interfaces.

Learning Activities

Fundamentals of computer security - Security concepts:confidentiality, integrity, availability and security policies. Security problems: security breaches and

vulnerabilities. Information encryption and decyprtion:terminology, systems and applications. risk analysis and security management:principles, techniques, processes and standards.

Personal computer security - Security problems. Security measures:access controls, file protection and password selection criteria. Computer viruses:examples, sources and prevention. Secure operating systems:penetration, security models and design issues.

Network security - Threats to computer networks. Crypto key management:protocols and services. digital signatures:importance and methods. Authentication:principles, protocols and services. Network access controls:policies and mechanisms. Security applications: secure electronic commerce and payment protocols.

Database security:Data classification. security requirements:integrity, authentication and access controls. techniques for multilevel security:partitioning, integrity locking, data encryption and secure interfaces.

References

Course Material	Book
Author	Pfleeger, C.P.
Publishing Year	2006
Title	Security in Computing
Subtitle	
Edition	4th
Publisher	Prentice Hall
ISBN	0132390779

Course Material	Book
Author	Stallings, W.
Publishing Year	2008
Title	Computer security: principles and practice
Subtitle	
Edition	
Publisher	Prentice Hall
ISBN	0136004245

Course Material	Book
Author	Konheim, A. G.
Publishing Year	2007
Title	Computer Security and Cryptography
Subtitle	
Edition	
Publisher	Wiley Blackwell
ISBN	0471947830

Course Material	Book
Author	Newman, R.C.
Publishing Year	2003
Title	Enterprise Security
Subtitle	
Edition	
Publisher	Prentice Hall
ISBN	0-13-047458-4

Notes

This module develops the understanding of threats to and the security requirements of computer systems, as well as tools and techniques to enforce security.