Liverpool John Moores University

Title:	COMPUTER SECURITY
Status:	Definitive
Code:	**7007COMP** (103266)
Version Start Date:	01-08-2011
Owning School/Faculty:	Computing and Mathematical Sciences
Teaching School/Faculty:	Computing and Mathematical Sciences

Team	Leader
Kashif Kifayat	Y
Robert Askwith	

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
Essay	AS1	Research and develop a solution for a contemporary computer security problem.	25.0	
Exam	AS2	Examination.	75.0	2.00

Aims

To develop the 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 promote the use of appropriate methodologies and tools in the analysis, design, implementation and management of secure systems.

To examine current research issues in Computer Security.

Learning Outcomes

After completing the module the student should be able to:

1	Identify a variety of security threats and vulnerabilities and assess their impacts on given computer applications.
2	Specify appropriate security requirements for countering security problems identified for given applications.
3	Apply a variety of security techniques and tools to develop appropriate security mechanisms and solutions for protection of computer systems.
4	Demonstrate 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:

Computer security solution	1	2	4
Examination	3	4	

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: file protection and password selection criteria. Computer attacks: examples, sources and prevention. Secure operating systems: security models and design issues.

Network security - threats to computer networks. Network security countermeasures: firewalls and intrusion detection systems. Wireless security: vulnerabilities, security services and protocols in the wireless environment.

Encryption and decryption - 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 payment protocols.

Database security: Data classification. Security requirements: integrity, authentication and authorization. Techniques for multilevel security: access control models, data encryption and architectures.

Learning Activities

Lectures, tutorials and advanced individual research. The individual research builds on core computer security concepts covered in the lectures through reading books, journals and conference papers in the area of computer security.

References

Course Material	Book
Author	Anderson, R. J.
Publishing Year	2008
Title	Security Engineering: A Guide to Building Dependable Distributed Systems
Subtitle	
Edition	2nd Edition
Publisher	John Wiley & Sons
ISBN	0-470-06852-3

Course Material	Book
Author	Pfleeger, C.P. & Pfleeger, S
Publishing Year	2006
Title	Security in Computing
Subtitle	
Edition	4th Edition
Publisher	Prentice-Hall International
ISBN	0-132-39077-9

Course Material	Book
Author	Schneier, B.
Publishing Year	2007
Title	Schneier's Cryptography Classics Library:
Subtitle	Applied Cryptography, Secrets and Lies, and Practical Cryptography
Edition	
Publisher	John Wiley & Sons
ISBN	0-470-22626-9

Course Material	Book
Author	Schneier, B.
Publishing Year	2008
Title	Schneier on Security
Subtitle	
Edition	
Publisher	John Wiley & Sons
ISBN	0-470-39535-4

Course Material	Book
Author	Stallings, W.
Publishing Year	2006
Title	'Cryptography and Network Security: Principles and Practice
Subtitle	
Edition	4th Edition
Publisher	Prentice Hall
ISBN	0-131-87316-4

Notes

This advanced course is intended for post-graduate students interested in the field of computer security. The purpose of the course is to provide the fundamental technical concepts and research issues essential for computer security. This module develops the understanding of threats to and the security requirements of computer systems, as well as tools and techniques to enforce security.