Liverpool John Moores University

Title:	COMPUTER SECURITY
Status:	Definitive
Code:	**7006ONLINE** (103113)
Version Start Date:	01-08-2012
Owning School/Faculty:	Computing and Mathematical Sciences
Teaching School/Faculty:	Computing and Mathematical Sciences

Team	Leader
David Llewellyn-Jones	Y

Academic Level:	FHEQ7	**Credit Value:**	15.00	**Total Delivered Hours:**	36.00
Total Learning Hours:	150	**Private Study:**	114		

Delivery Options
Course typically offered: Runs Twice - S1 & S2

Component	Contact Hours
Lecture	12.000
Seminar	12.000
Tutorial	12.000

Grading Basis: 40 %

Assessment Details

Category	Short Description	Description	Weighting (%)	Exam Duration
Essay	AS1	Essay discussing practical elements of computer security within a given scenario. This includes discussion of current research issues and the application of specific security solutions applied to the scenario.	50.0	
Essay	AS2	Essay discussing the technical details and application of cryptography within a given scenario. This includes the identification of requirements and threats, the development of protocols to address them and	50.0	

Category	Short Description	Description	Weighting (%)	Exam Duration
		the assessment of these protocols to justify their appropriateness.		

Aims

To develop the knowledge of various security threats and vulnerabilities in computer systems as well as the importance of Computer Security.

To assess critically 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 Use 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 essay	2	4
Application of cryptography	1	3

Outline Syllabus

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.

Learning Activities

Includes accessing online lectures and online tutorials, as well as reading books and handouts.

References

Course Material	Book
Author	Anderson, R. J.
Publishing Year	2008
Title	Security Engineering
Subtitle	A Guide to Building Dependable Distributed Systems
Edition	2nd
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
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 Inc
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
Subtitle	Principles and Practice
Edition	
Publisher	Prentice-Hall
ISBN	0-131-87316-4

Course Material	Journal / Article
Author	
Publishing Year	
Title	Computers and Security
Subtitle	
Edition	
Publisher	Elsevier
ISBN	

Course Material	Journal / Article
Author	
Publishing Year	
Title	Computer Security
Subtitle	
Edition	
Publisher	IOS Press
ISBN	

Course Material	Journal / Article
Author	
Publishing Year	
Title	Security and Communication Networks
Subtitle	
Edition	
Publisher	John Wiley & Sons
ISBN	

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. All online activities are scheduled.