

Module code: MOD005438	Version: 1 Date Amended: 04/May/2016
-------------------------------	--

1. Module Title
Principles of Digital Security

2a. Module Leader
Chris Jakeman

2b. Department
Department of Computing and Technology

2c. Faculty
Faculty of Science and Technology

3a. Level
5

3b. Module Type
Standard (fine graded)

4a. Credits
15

4b. Study Hours
150

5. Restrictions			
Type	Module Code	Module Name	Condition
Pre-requisites:	None		
Co-requisites:	None		
Exclusions:	None		
Courses to which this module is restricted:			

LEARNING, TEACHING AND ASSESSMENT INFORMATION

6a. Module Description

This module is related to e-Commerce and e-Crime but explores the technology and practices required to provide security in digital systems.

The students study programming techniques to defend against attacks such as SQL Injection and buffer overflow.

Encryption algorithms are researched and critically assessed.

Identity and authentication is researched with techniques to protect passwords. The students will be able to set up systems which can be attacked and defended.

Programming practices such as fail-safe, defence-in-depth and least privilege are studied.

Students study the public key infrastructure (PKI) which is the foundation for secure communications including financial transactions. They will set up networks attempting to eavesdrop on conversations, carry out man-in-the-middle exploits and defend against them.

A feature of the module is that students will be assigned weekly challenges to research and present back to the class.

Assessment is by building and demonstrating a system secured against selected threats and a report evaluating performance and justifying the choices made.

6b. Outline Content

Defensive programming

Cryptographic Principles

Password protection

Public Key Infrastructures and Digital Signatures

Man-in-the-middle attacks

6c. Key Texts/Literature

The reading list to support this module is available at: <http://readinglists.anglia.ac.uk/modules/mod005438>

6d. Specialist Learning Resources

Virtual machine software to host vulnerable systems

7. Learning Outcomes (threshold standards)		
No.	Type	On successful completion of this module the student will be expected to be able to:
1	Knowledge and Understanding	Compare and contrast the use of cryptographic techniques for ensuring the confidentiality, integrity and availability of user data.
2	Knowledge and Understanding	Explain how to attack and gain control of a given computer system.
3	Intellectual, practical, affective and transferrable skills	Demonstrate how digital data security can be achieved in given scenario so that the principles of security are maintained
4	Intellectual, practical, affective and transferrable skills	Configure and implement key digital security techniques to protect servers and applications from common vulnerabilities and security issues.

8a. Module Occurrence to which this MDF Refers				
Year	Occurrence	Period	Location	Mode of Delivery
2017/8	F01UCP	Semester 2	University Centre, Peterborough	Face to Face

8b. Learning Activities for the above Module Occurrence			
Learning Activities	Hours	Learning Outcomes	Details of Duration, frequency and other comments
Lectures	12	1,2,3,4	Lecture 1 hr x 12 weeks
Other teacher managed learning	24	1,2,3,4	Practical 2 hr x 12 weeks
Student managed learning	114	1,2,3,4	reading, research, skills practice, assignment
TOTAL:	150		

9. Assessment for the above Module Occurrence					
Assessment No.	Assessment Method	Learning Outcomes	Weighting (%)	Fine Grade or Pass/Fail	Qualifying Mark (%)
010	Practical	1,2	0 (%)	Pass/Fail	100 (%)
15 minutes presentation of secure system to meet brief (1,000 words equivalent)					
Assessment No.	Assessment Method	Learning Outcomes	Weighting (%)	Fine Grade or Pass/Fail	Qualifying Mark (%)
011	Coursework	3,4	100 (%)	Fine Grade	30 (%)
Documentation including design and testing of secure system - 2,000 words					
<p>In order to pass this module, students are required to achieve an overall mark of 40%.</p> <p>In addition, students are required to:</p> <p>(a) achieve the qualifying mark for each element of fine graded assessment of as specified above</p> <p>(b) pass any pass/fail elements</p>					