

# Module Guide

## *Undergraduate Programme Academic Year 2009/2010*

<b>Module:</b>	Security Systems Theory UG2
<b>Web-site:</b>	<a href="http://bcu.copsewood.net/">http://bcu.copsewood.net/</a>
<b>School:</b>	Computing, Telecommunications and Networks
<b>Module Co-ordinator:</b>	Richard Kay
<b>Module Tutors:</b>	Richard Kay, Yonghao Wang
<b>Contact Information:</b>	By email: <a href="mailto:Richard.Kay@bcu.ac.uk">Richard.Kay@bcu.ac.uk</a> , <a href="mailto:Yonghao.Wang@bcu.ac.uk">Yonghao.Wang@bcu.ac.uk</a>
<b>Brief Descriptions of the Items of Assessment:</b>  <b>You will be expected to complete ALL Assessments.</b>	<p>1. Assessment 1 comprises:</p> <ul style="list-style-type: none"> <li>a. An in class test covering taught material preparing students for carrying out a security investigation.</li> <li>b. An individual security investigation and report.</li> </ul> <p>2. Assessment 2 comprises a closed-book written examination.</p> <p>Information is for guidance only. See ECMS My Course on the intranet for details.</p>
<b>Assessment Weighting:</b>	See ECMS My Course on the intranet for details
<p><b>Individual assignments. The work you submit shall be your own and not the product of collaboration with anyone else. Plagiarism will be penalised.</b></p> <p><b>In-course assessments shall be submitted through the Coursework Collection System, to the module co-ordinator.</b></p>	
<b>Contents of Guide:</b>	
Syllabus and supporting information	Teaching Schedule

# **Syllabus and supporting information**

## **Recommended Texts**

Anderson, R. (2001) Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley Computer Publishing.

Ferguson, N. & Schneier, B. (2003) Practical Cryptography, John Wiley & Sons.

Shah, S. (2005) Linux Administration: A Beginner's Guide. 4e McGraw Hill.

## **Aims of Module**

The module has been designed to provide the necessary theoretical framework, foundations and practical support for effectively pursuing security solutions with respect to data / information, processing and procedures, networks, communications and physical security. This is underpinned by providing an understanding of cryptography and formal security models and their respective roles in realising security solutions. It introduces the student to the theory and practice of systems administration and protection and the various aspects of security monitoring and evaluation.

The module also introduces the student to the requirements and techniques for risk identification and assessment and the elements of security management from a human and technological perspective and with respect to appropriate laws and standards.

## **Brief Module Description**

The module introduces the students to a variety of security topics:

Nature and scope of security engineering, definitions, the significance and importance of protocols and consideration of legal, ethical and standardisation requirements in information systems security. Basic principles of access control and access security, systems administration, attack scenarios, failure mechanisms and defensive solutions. Embedded and distributed systems for security support purposes. Hierarchical security requirements and handling strategies with particular reference to information, process, network, communications and physical security. Error control theory, cryptography and steganography. quantum cryptography, cryptographic filesystems and tamper-resistant devices. Systems protection. Security monitoring, intrusion detection systems. Emissions analysis and evaluation techniques. Risk assessment. Security management and standards.

## Teaching Schedule for: **Security Systems Theory UG2**

Wk No	Date (Mon)	Lecturer	Lecture Topic	Tutorial / Lab Topic	Assignment *	
					Set	Due In
1	28-Sep-09	RK	Module introduction. Security theory and practice.	Use of Linux virtual machines		
2	05-Oct-09		Password based security systems	Simple Unix/Linux shell commands		
3	12-Oct-09		Introduction to entropy and key strength	Unix/Linux pipelines and I/O redirection		
4	19-Oct-09		Backing up data and disaster recovery	Use of filters: awk, sed, grep sort etc.		
5	26-Oct-09		Scripting on Linux. Bash, Perl and Python.	Further pipeline and filter exercises		
6	02-Nov-09		Unix/Linux file permissions and ownership.	Simple bash shell scripting		
7	09-Nov-09		Special program privileges: setuid/setgid	Use of chmod, chown, chgrp		
8	16-Nov-09		Threats 1: viruses, trojans and worms	Mock in-class test		
9	23-Nov-09		Assignment Completion			
10	30-Nov-09		Networked authentication using Kerberos	Mock test feedback		
11	07-Dec-09		In-class test	Assignment 1.2 briefing	A1.1	A1.1
12	14-Dec-09		Multi-level and multilateral security. Permissions, capabilities, ACLs, SELinux.	Project selection surgery	A1.2	
Christmas Vacation (3 weeks)						
13	11-Jan-10		Threats 2: Buffer overflow, SQL injection, Cross-site scripting	Ubuntu package installation, use of mount command, VM networking.		
14	18-Jan-10		Firewalls	Assignment 1.2 surgery		
15	25-Jan-10		Virtual Private Networks (VPNs)	Assignment 1.2 surgery		
16	01-Feb-10		Crypto 1: symmetrical block ciphers	Assignment 1.2 surgery		
17	08-Feb-10		Crypto 2: asymmetrical public key concepts	Assignment 1.2 surgery		
18	15-Feb-10		Assignment Completion			
19	22-Feb-10		Crypto 3: public key practice - use of GPG	Assignment 1.2 surgery		
20	01-Mar-10		Crypto 4: prime number theory and Diffie Hellman	Assignment 1.2 surgery		
21	08-Mar-10		Security-relevant legislation	Assignment 1.2 surgery		
22	15-Mar-10		Copy prevention, steganography and DRM	Assignment 1.2 surgery		
23	22-Mar-10		Email security and spam reduction	Assignment 1.2 surgery		A1.2

Wk No	Date (Mon)	Lecturer	Lecture Topic	Tutorial / Lab Topic	Assignment		
					Set	Due In	
			Easter Vacation (3 weeks)				
24	19-Apr-10	RK	Financial transaction security procedures	Reading/discussion exam topics			
25	26-Apr-10		Review and revision hints	Reading/discussion exam topics			
26	03-May-10		Final week of teaching (revision classes) (Monday – Bank Holiday)	Reading/discussion exam topics			
27	10-May-10		Exams		A2	A2	
28	17-May-10		Exams				
29	24-May-10						

\* Assignment Set and Due week indication above is for guidance only. See ECMS My Course on the intranet for details.