Faculty of
Technology, Engineering and the Environment

Module Guide

Undergraduate Programme
Academic Year 2011/2012

Module:	Security Systems Theory UG2
Web-site:	http://bcu.copsewood.net/
School:	CTN
Module Co-ordinator:	Richard Kay
Module Tutors:	Richard Kay, Stish Sarna
Contact Information:	Richard.Kay@bcu.ac.uk, Stish.Sarna@bcu.ac.uk
Brief Descriptions of the Items of Assessment: **You will be expected to complete ALL Assessments.**	1. Coursework involving a. cryptography questions and b. miniproject. 2. A closed-book 2 hour written examination. Information is for guidance only. See ECMS My Course on the intranet for details.
Assessment Weightings:	See ECMS My Course on the intranet for details

Individual assignments. The work you submit shall be your own and not the product of collaboration with anyone else. Plagiarism will be penalised.

In-course assessments shall be submitted through the Coursework Collection System, to the module co-ordinator.

Contents of Guide:

Syllabus and supporting information

Recommended Texts

Anderson, R. (2008) Security Engineering: A Guide to Building Dependable Distributed Systems, 2e, Wiley Computer Publishing.
Ferguson, N. & Schneier, B. (2003) Practical Cryptography, John Wiley & Sons.

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	26-Sep-11	RK	Module Intro. Security theory and practice	Linux virtual machines and openssl		
2	03-Oct-11	RK	Password-based security systems	Use of password hash cracker		
3	10-Oct-11	RK	Symmetric cryptography concepts	GPG/OpenSSL symmetric crypto		
4	17-Oct-11	RK	Asymmetric cryptography concepts	GPG using public/private keys	A1.1	
5	24-Oct-11	RK	Entropy in passwords and key generation	GPG involving TTP certifiers		
6	31-Oct-11	RK	Public Key Infrastructure	Coursework exercise preparation		
7	07-Nov-11	RK	OS Security: Linux chmod/chown and setuid	User account administration on Linux		
8	14-Nov-11	RK	Discretionary and mandatory access control, type enforcement, role based access control.	Mandatory access control tutorial		
9	21-Nov-11		Reading Week			
10	28-Nov-11	SS	Prime number theory and factorisation.	PKI class discussion		
11	05-Dec-11	SS	Modular Exponentiation and inverse ME	Coursework completion		A1.1
12	12-Dec-11	SS	Fermat, Miller-Rabin and other primality tests	Miniproject selection tutorial	A1.2	
			Christmas Vacation (3 weeks)			
13	09-Jan-12	SS	Diffie Hellman protocol and RSA mathematics	Modular exponentiation software		
14	16-Jan-12	RK	Threats 1: Malware, worms, viruses, trojans	Miniproject objectives and info location		
15	23-Jan-12	RK	LAN Security: Kerberos and Active Directory	Miniproject surgery		
16	30-Jan-12	RK	Threats 2: SQL injection, buffer overflows, cross site scripting	Miniproject surgery		
17	06-Feb-12	RK	Copy prevention, TPM and DRM technologies	Miniproject surgery		
18	13-Feb-12		Reading Week			
19	20-Feb-12	RK	Network Firewalls	Miniproject surgery		
20	27-Feb-12	RK	Virtual Private Networks	Miniproject surgery		
21	05-Mar-12	RK	Financial security models	Miniproject surgery		
22	12-Mar-12	RK	Security-relevant legislation	Miniproject surgery		
23	19-Mar-12	RK	Email security, spam and sender reputation	Completing assignment		A1.2
24	26-Mar-12	RK	DNSSEC securing the Domain Name System	Exam revision guided reading		
			Easter Vacation (3 weeks)			

Wk No	Date (Mon)	Lecturer	Lecture Topic	Tutorial / Lab Topic	Assignment *	
					Set	Due In
25	23-Apr-12	RK	Exam revision 1: security knowledge questions	Exam revision guided reading		
26	30-Apr-12	SS	Exam revision 2: mathematical cryptography	Exam revision crypto computations		
27	07-May-12		Exams (Monday – Bank Holiday)			A2
28	14-May-12		Exams			
29	21-May-12					

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