

Module Guide

Postgraduate Programme Academic Year 2009/2010 Semester 2

Module:	Building Secure Applications	
Web-site:	Richard Kay: http://bcu.copsewood.net/ Shahid Shabbir: http://mytid.bcu.ac.uk/staff/shabbirs/	
School:	CTN	
Module Co-ordinator:	Richard Kay	
Module Tutors:	Richard Kay, Shahid Shabbir	
Contact Information:	Richard.Kay@bcu.ac.uk , Shahid.Shabbir@bcu.ac.uk	
Brief Descriptions of the Items of Assessment: You will be expected to complete ALL Assessments.	<ol style="list-style-type: none"> 1. Securing a networked application coursework 2. Using identification devices coursework <p>Information is for guidance only. See ECMS My Course on the intranet for details.</p>	
Assessment Weighting:	See ECMS My Course on the intranet for details	
<p>Individual assignments. The work you submit shall be your own and not the product of collaboration with anyone else. Plagiarism will be penalised.</p> <p>In-course assessments shall be submitted through the Coursework Collection System, to the module co-ordinator.</p>		
Contents of Guide:		
Syllabus and supporting information Indicative content Recommended texts	Aims Learning outcomes Teaching schedule	

Syllabus and supporting information

Aims The aim of this theme is to provide a detailed knowledge of program level, system level and network level security, and the techniques which may be used to build a secure distributed application. It aims to equip students with the ability to develop applications securely and to analyse and mitigate security issues affecting or likely to affect a distributed application. Security advantages and limitations of bar-coding, RFID and smart card device technologies are also covered. This includes biometrics as a technique for personal identification and authentication, and experience of the integration of bar-code, RFID and smart card facilities into the design and operation of a distributed application in order to mitigate the disadvantages of password based security keying.

Indicative content

- Analysis of problems resulting from security vulnerabilities in distributed applications. Legislation relevant to distributed applications security, including the Computer Misuse Act and the Data Protection Act.
- Application and use of bar-coding, RFID and smart card devices on host systems in order to enhance the practical security of distributed applications.
- Cryptographic techniques at a conceptual level and the implementation of cryptography at the network communications level.
- Techniques and technologies for personal identification based on Biometric (anatomical and biodynamic) features.
- Evaluation of security of contemporary programs and systems. Exploiting simulated vulnerabilities using known exploits and readily available software tools within a suitably quarantined test environment.

Learning outcomes On completion of the theme, the student should be able to:

- 1 Analyse security issues, with a view to contribute towards the development and implementation of a security policy covering the realisation and use of a distributed application.
- 2 Design and develop a distributed application making use of public key algorithms for the purpose of encryption, decryption, signing of data and certification of users and platforms.
- 3 Integrate the use of smart card devices making use of secure algorithms and cryptographic techniques within a distributed application.
- 4 Investigate weaknesses within an existing distributed application, recommending remediation strategies based on a costs and benefits analysis.
- 5 Specify and select appropriate data structures, data carriers, track and traceability solutions and security support techniques to meet particular application and security needs.
- 6 Analyse vulnerability factors associated with data carriers and data capture appliances and onward transfer of data.
- 7 Appraise, specify and select personal identification systems to meet particular security and authentication application needs.

Recommended Texts

- Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2e Wiley. 2008
- Schneier, B. and Ferguson, N: *Practical Cryptography*. Wiley. 2003
- Glover, B. and Bhatt, H. *RFID Essentials*. O'Reilly. 2006.
- Finkenzeller, K. *RFID Handbook (Second Edition)*. Wiley. 2003.
- Rankl, W. and Effing, W. *Smart Card Handbook (Third Edition)*.

Teaching Schedule for: **Building Secure Applications**

Wk No	Date (Mon)	Lecturer	System and application security theme Richard Kay (Tuesdays MP050 11:00 – 15:00)	Auto identification theme Shahid Shabbir (Thursdays	Assignment *	
					Set	Due In
15	25-Jan-10	RK/SS	Password based authentication and entropy		A1	
16	01-Feb-10		Attacks: viruses, worms, Trojans		A2	
17	08-Feb-10		Virtual Private Networks and Firewalls			
18	15-Feb-10		Attacks: XSS, SQL Injection, buffer overflow			
19	22-Feb-10		Block ciphers, symmetric cryptography			
20	01-Mar-10		Asymmetric cryptography, concepts			
21	08-Mar-10		Asymmetric cryptography, practice & PKI			
22	15-Mar-10		Primes, RSA and Diffie Hellman protocols			
23	22-Mar-10		Security-relevant legislation			
Easter Vacation (3 weeks)						
24	19-Apr-10		Steganography, DRM and content protection			
25	26-Apr-10		Financial systems, transactions and security			
26	03-May-10		Spam and reputation.			
27	10-May-10					A1
28	17-May-10		Assessment & Examinations			A2
29	24-May-10					

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