INFORMATION SECURITY GROUP
Course Specification 2013-14

Code:	IY5522	**Course Value:**	0.5	**Status:**	Core B
Title:	**Security Technologies**			**Availability:**	Autumn term
Prerequisites:	None			**Recommended:**	None
Co-ordinator:	TBC				
Course Staff	TBC				
Aims:	This course will: • provide an overview of the fundamental technologies underpinning computer and networked applications, along with the associated security issues • examine how maintaining security through separation is a key aspect of operating system design • provide an overview of the main types of authentication mechanisms used in computer systems • describe the fundamental types of access control mechanisms • overview the fundamental principles of secure protocol design, and how they are used in deployed security protocols • examine the security threats and vulnerabilities found in particular types of networks • assess mobile and wireless communication technologies in terms of their security vulnerabilities				
Learning Outcomes:	On successful completion of the course students will be able to: • demonstrate a systematic understanding of the construction of information networks, specifically the architecture and operation of the Internet Protocol suite. • demonstrate a clear understanding of the construction of a modern computer system, specifically the different hardware and software components which support multiprocessing. • explain the causes and potential effects of vulnerabilities that affect computer systems and identify appropriate countermeasures. • demonstrate a comprehensive understanding of different types of user authentication mechanisms in use within modern computer systems. • provide an overview of different access control mechanisms used within computer systems, and evaluate the suitability of different access control mechanisms for different security requirements. • provide a clear understanding of how strong authentication protocols, key exchange protocols and key exchange mechanisms suitable for use on open networks can be constructed. • demonstrate a clear understanding of how the design principles for secure protocols are applied to the Internet, focussing on SSL/TLS. • identify the key security threats faced in network environments, and be able to specify appropriate countermeasures. • explain the basic differences between different wireless technologies, and evaluate the security requirements according to the particular needs of different wireless networking technologies.				
Course Content:	The course will cover the following topics: • Introduction to Computer and Network Architectures • Introduction to Security • Platform and Operating System Security • User Authentication Mechanisms, Security Models and Access Control Mechanisms • Malicious Code, Introduction to Security Protocols • Network Security Threats and Countermeasures • Web Security • Wireless (WLAN and GSM/UMTS) Security				
Teaching & Learning Methods	Lectures delivered by ISG staff, Tutorial sessions. Optional exercise sheets to reinforce learning and provide directions for further study. Use of course website with teaching materials, links, and bibliography.				
Key Bibliography:	D. Gollmann, *Computer Security(2nd Edition)*, John Wiley & Sons, 2006. C.P. Pfleeger and S.L. Pfleeger, *Security in Computing (3rd Edition)*, Prentice-Hall, 2002. W. Stallings, *Network Security Essentials (2nd Edition)*, Prentice-Hall, 2002.				
Formative Assessment and Feedback:	Two sets of exercise sheets will be set. These are expected to be handed in for marking and feedback. Additionally, problem sheets will be set weekly on which students will receive feedback in tutorials.				
Summative Assessment:	**Exam** 100(%) This course is assessed solely by written examination consisting of a two-hour-exam. *(3 out of 5 questions)* **Coursework** 0(%) Coursework does not contribute to the final assessment for this course. **Deadlines:** The written examination will be held in the Summer term				

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department's policy of continuous improvement and development. Every effort will be made to notify you of any such changes.