INFORMATION SECURITY GROUP

Course Specification 2013-14

Code:	IY5511	**Course Value:**	0.5	**Status:**	Core A
Title:	**Network Security**			**Availability:**	Autumn term
Prerequisites:	None			**Recommended:**	None
Co-ordinator:	Jason Crampton				
Course Staff	Jason Crampton				
Aims:	This course will: ▪ consider information networks and their operation. ▪ examine the security threats and risks arising in particular types of networks. ▪ identify and evaluate countermeasures that can be used to enhance the security of networks.				
Learning Outcomes:	On successful completion of the course students will: ▪ have a systematic understanding of information networks and their operation; ▪ have a clear understanding of the components of the TCP/IP protocol stack, the OSI 7 layer model, and the associated security architecture as specified in ISO/IEC 7498-2; ▪ have a critical awareness of key security threats and risks faced in network environments, and be able to specify appropriate countermeasures; ▪ have a comprehensive understanding of the methods by which strong authentication protocols and key exchange mechanisms suitable for use on open networks can be constructed; ▪ understand the security architecture and design rationale for the Kerberos system; ▪ have a comprehensive understanding of the security architecture and design rationale of selected protocols, such as the IPSec protocol suite, and how they can be applied in single-sign on, e-commerce, virtual private networking and remote access applications; ▪ be able to analyse critically the benefits and drawbacks of applying security controls at different network layers; ▪ understand the design rationale for the security architecture in GSM and UMTS systems and be able to compare and evaluate the security in the two systems; ▪ be able to evaluate the security threats in wireless LANs and the strength of security countermeasures offered by current standards; ▪ be able to assess the security offered by different firewall technologies as well as their limitations; ▪ understand the value of Intrusion Detection Systems and related network security technologies.				
Course Content:	Introduction to Reliable and Secure Communication Channels; Introduction to Networking and Network Security, Introduction to Secure Protocols; Secure Protocols – IPSec, SSL/TLS and SSH; GSM and UMTS Security; Wireless LAN Security; Firewalls; Intrusion Detection Systems and related network security technologies; E-mail Security				
Teaching & Learning Methods:	Lectures delivered by industry experts & ISG staff. Small group and individual tutorials. Optional weekly exercise sheets to reinforce learning and provide directions for further study. Course website, hosted on Moodle, with teaching materials, links, and bibliography.				
Key Bibliography:	N. Ferguson, B. Schneier, and T. Kohno. Cryptography Engineering: Design Principles and Practical Applications, John Wiley & Sons, 2010. C. Kaufman, R. Perlman, and M. Speciner, Network Security: Private Communication in a Public World, Prentice Hall, 2002. W. Stallings, Network Security Essentials (3rd ed.), Prentice Hall, 2007. L.L. Peterson and B.S. Davie. Computer Networks: A Systems Approach, Morgan Kaufman (5th ed.), 2011. D.E. Comer, Computer Networks and Internets (4th ed.), Prentice Hall, 2004.				
Formative Assessment and Feedback:	There will be two compulsory pieces of coursework with deadlines during the first semester. These will be marked and returned to the students. Marks obtained in these assessments will NOT contribute towards the final assessment for this course.				
Summative Assessment:	**Exam:** 100(%) This course is assessed solely by written examination consisting of a two-hour exam. **Coursework:** 0(%) Coursework does not contribute to the final assessment for this course. **Deadlines:** The written examination will be held in the Summer term.				