INFORMATION SECURITY GROUP

Course Specification 2013-14

Code:	IY5610	**Course Value:**	0.5	**Status:**	Option
Title:	**Security Testing Theory and Practice**			**Availability:**	Spring Term
Prerequisites:	IY5511			**Recommended:**	IY5607, IY5512
Co-ordinator:	Carlos Cid				
Course Staff	Carlos Cid, Allan Tomlinson and John Austen				
Aims:	This course will provide the foundations and theoretical underpinnings for an understanding of the way in which IT systems can be attacked and penetrated by circumventing security or exploiting vulnerabilities in the system. This will form the basis of a methodical approach to surveying and auditing systems, and prepare candidates to design secure systems, identify vulnerabilities, and defend systems against intrusion.				
Learning Outcomes:	On successful completion of the course students will be able to: • Gained an understanding of the legal aspects of carrying out a penetration test and an approach to preparing and managing such an audit. • Gained an in-depth understanding of network protocols; computer system architectures; and application systems. • Gained an understanding of the vulnerabilities in existing protocols, systems, and applications; and an understanding of the security technologies designed to mitigate these vulnerabilities. • Gained practical experience of how these vulnerabilities may be exploited in practice to penetrate a system.				
Course Content:	The course will cover the following topics: • Introduction to security testing, legal aspects of penetration testing, standards and certification. • Security testing frameworks and methodologies, and how to prepare, manage and conduct a professional penetration testing. • Technical aspects of network security covering standards, protocols, routing, firewalls showing the theoretical basis of vulnerabilities and how these may be exploited in practice. • Technical aspects of computer security covering operating systems, access control in windows and linux/unix, host based intrusion detection, escalation of privileges and how to exploit these vulnerabilities in practice and how to harden systems. • Technical aspects of Internet based applications, web services, protocols, languages (e.g. SQL) and how these may be exploited using for example SQL injection and cross-site scripting; how to exploit these vulnerabilities in practice, and how to harden the applications. • A survey of non-standard and emerging technologies and review of potential threats these may lead to.				
Teaching & Learning Methods	Lectures and selected supervised and self-directed laboratory sessions to reinforce material covered in lectures. Guest lectures from practitioners in the field.				
Key Bibliography:	T. Wilhelm, Professional Penetration Testing, Syngress, 2010. S. McClure et al., Hacking Exposed 7: Network Security Secrets and Solutions. McGraw-Hill, 2012. A Harper et al., Gray Hat Hacking, 3^{rd} ed. McGraw Hill, 2011. R. Stevens, TCP/IP Illustrated, Volume 1: The Protocols, Addison-Wesley, 1994. D. Stuttard, M.Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. John Wiley & Sons, 2011. 2^{nd} edition. M. Dowd et al., The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Addison Wesley, 2006.				
Formative Assessment and Feedback:	Formative feedback will be given during the module in the form of exercise sheets which will be marked and used as the basis for feedback.				
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.