INFORMATION SECURITY GROUP
Course Specification 2016-17

Code:	IY5512	**Course Value:**	20	**Status:**	Core A
Title:	**Computer Security (Operating Systems)**			**Availability:**	Autumn term
Prerequisites:	None			**Recommended:**	None
Co-ordinator:	Daniele Sgandurra				
Course Staff	Daniele Sgandurra				
Aims:	This course is concerned with security mechanisms in modern computer systems and will consider: • the core concepts: security policies, security models, subjects and objects, authorisation, and access rights • why operating systems and computer systems remain vulnerable to attack, and how vulnerable systems can be strengthened to increase their resistance to attackers • security issues for computer hardware and software • user authentication, including the use of tokens and biometrics • access control models and policies, and practical implementation of access control • how authentication and access control are implemented in commercial products				
Learning Outcomes:	On successful completion of the course the student will be able to: • demonstrate a comprehensive understanding of the role of security mechanisms for modern computer systems, including both hardware and software • understand the mechanisms that are generally used to implement security policies, and be aware of key examples of mechanisms within particular hardware and operating systems • understand the use and operation of a range of access control mechanisms • understand the use and operation of a range of user authentication mechanisms • understand the main issues relating to software security and their effect on the security of computer systems				
Course Content:	• *Concepts and Terminology:* security; confidentiality, integrity and availability; security policies; security models; mandatory and discretionary access control; access control matrix, capabilities and access control lists; information flow • *Security Models:* information flow policies; role-based access control • *Implementation of Mechanisms:* security mechanisms in hardware and operating systems; memory management, memory protection and logical protection; access control lists • *User authentication*: passwords, biometrics and user tokens; identity management • *Case Studies:* Intel processor family; Windows; Linux; Android; IoT • *Operating system vulnerabilities*: how they can be exploited and how they can be prevented • *Software security*: buffer overflows and exploits; validation errors and exploits; languages that improve software security				
Teaching & Learning Methods:	• Lectures and detailed case studies delivered by ISG staff and industry experts • Tutorial sessions				
Key Bibliography:	• D. Gollmann, *Computer Security*, John Wiley & Sons, 2011 (3rd edition) – the main text. • C. P. Pfleeger,S. L. Pfleeger and J. Margulies, *Security in Computing*, Prentice-Hall, 2015 (5th edition). • M. Bishop, *Computer Security: Art and Science*, Addison-Wesley, 2003.				
Formative Assessment and Feedback:	Tutorial sessions are used to provide feedback on student answers to exercise sheets, discuss model answers, and discuss any difficulties with course material. Formative feedback is provided on a comprehensive set of coursework.				
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				