UNIVERSITÀ DI PAVIA

Anno Accademico 2018/2019

INFORMATION SECURITY

Anno immatricolazione	2017/2018
Anno offerta	2018/2019
Normativa	DM270
SSD	ING-INF/05 (SISTEMI DI ELABORAZIONE DELLE INFORMAZIONI)
Dipartimento	DIPARTIMENTO DI INGEGNERIA INDUSTRIALE E DELL'INFORMAZIONE
Corso di studio	COMPUTER ENGINEERING
Curriculum	Embedded and Control Systems
Anno di corso	2°
Periodo didattico	Primo Semestre (01/10/2018 - 18/01/2019)
Crediti	6
Ore	45 ore di attività frontale
Lingua insegnamento	English
Tipo esame	SCRITTO E ORALE CONGIUNTI
Docente	BARILI ANTONIO (titolare) - 6 CFU
Prerequisiti	Good knowledge of operating systems, networking and data base technologies.
Obiettivi formativi	Knowledge of information security techniques. Ability to assess the security level of some common software systems and to design improvement actions.
Programma e contenuti	Introduction Security vs. Safety. Physical security. Information security: privacy, avaliability, integrity, authenticity. Information security threats and countermeasures. Basic Information Theory and Cryptography Introduction to information theory and cryptography. Historical developement. Symmetric and asymmetric ciphers. Hashing functions

	and MACs. Pseudo-Random Number Generators. Digital certificates. Cryptanalysis. Digital Signature Digital documents and digital signatures. Creation, preservation and validation of digital documents. Digital documents as court evidence. Public key infrastructures. Italian and EU laws concerning digital signatures. Copyright Protection Introduction to copyright law. Software and database protection. Audio, video and picture protection. Digital rights management (DRM). Watermarking and steganography. Communication Protection Information communication and diffusion. Synchronous and asynchronous communication. E-mail. The Web as an information diffusion media. Communication privacy protection. Threats to the freedom and privacy of communications and countermeasures. Phishing. Systems and Networks Protection Access control: authentication, authorization and accounting. Physical and logical information protection. Networks protection. Firewalls. Threats to systems and communication networks. Malware. Incident Response e Digital Forensics Incident detection and response. System audit and log analysis. Intrusion Detection Systems. Introduction to digital forensics.
Metodi didattici	Lectures (hours/year in lecture theatre): 45 Practical class (hours/year in lecture theatre): 0 Practicals / Workshops (hours/year in lecture theatre): 0
Testi di riferimento	Lecture notes and online references provided by the instructor.
Modalità verifica apprendimento	Written test.
Altre informazioni	Written test.
Obiettivi Agenda 2030 per lo sviluppo sostenibile	$lbl_legenda_sviluppo_sostenibile