



UNIVERSITÀ DI PAVIA

Anno Accademico 2021/2022

INFORMATION SECURITY

Anno immatricolazione	2020/2021
Anno offerta	2021/2022
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	Computer Science and Multimedia
Anno di corso	2°
Periodo didattico	Primo Semestre (27/09/2021 - 21/01/2022)
Crediti	6
Ore	45 ore di attività frontale
Lingua insegnamento	English
Tipo esame	SCRITTO
Docente	BARILI ANTONIO (titolare) - 6 CFU
Prerequisiti	Good knowledge of operating systems principles and applications, computer networking protocols 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	<p>Introduction Security vs. Safety. Physical security. Information security: privacy, availability, integrity, authenticity. Information security threats and countermeasures.</p> <p>Basic Information Theory and Cryptography Introduction to information theory and cryptography. Historical development. Symmetric and asymmetric ciphers. Hashing functions</p>

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.

Intellectual property

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.

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

Obiettivi Agenda 2030 per lo sviluppo sostenibile

[Gli obiettivi](#)