BANCA D'ITALIA

Master II livello in *Data Science for public decision making* dell'Università di Roma Tor Vergata, A.A. 2026–2027

Programma dell'insegnamento *Data Security*

novembre 2025

Docenti

Walter ARRIGHETTI	PhD, 2007	walter . arrighetti @ uniroma2.eu
Alessandro CIANI	Master, 2017	alessandro . ciani @ uniroma2.eu
Michela IEZZI	PhD, 2013	michela . iezzi @ uniroma2.eu
Marco PERICÒ	Master, 2018	marco . perico @ uniroma2.eu

Descrizione del corso

Lo scenario "*Big Data*" e l'utilizzo di servizi basati su AI offrono molti vantaggi per la collettività, ma anche sfide tecnologiche, organizzative e normative, legate al trattamento, anche automatizzato, di dati che devono essere disponibili, sempre e ovunque.

In questo cambiamento di paradigma, in cui si "dissolvono nel *Cloud*" concetti quali reti di calcolatori, identità, privacy degli utenti e persino il dato stesso – e diventa sempre più naturale accostare le parole "AI" ed "etica" – sono anche nate nuove opportunità di attacco da parte di diversi attori della minaccia *cyber*.

Dopo una parte introduttiva sulle tecnologie, i protocolli e i metodi della sicurezza informatica, gli studenti dell'insegnamento di *Data Security* saranno calati nello scenario evolutivo della minaccia *cyber* con particolare riferimento alla *data science* e acquisiranno conoscenze sulle principali tipologie di attacco ai dati e sui relativi metodi di difesa ricorrendo al metodo scientifico, alla tecnologia, ma anche agli strumenti normativi e alla corretta sensibilizzazione degli individui.

Obiettivi di apprendimento

- ✓ fornire il *know-how* su tecnologie, protocolli e soluzioni di sicurezza;
- ✓ fornire delle conoscenze pratiche degli attacchi informatici e delle relative difese tramite attività di laboratorio e pratiche su software e strumenti di sicurezza;
- ✓ evidenziare alcune sfide specifiche che emergono negli scenari di *Big Data* e fornire alcuni suggerimenti sulle metodologie e strumenti emergenti per affrontare tali sfide.

Metodologia

Didattica frontale; laboratori di tipo dimostrativo (in cui il docente mostra alcune operazioni su componenti software, siti web o macchine virtuali e gli studenti possono seguire da remoto e in alcuni casi replicare sui propri PC quello che fa il docente).

Valutazione

Valutazione mediante prova finale scritta.

Programma

1 Introduction

1.1 Course preview and motivations.
1.2 Triads of Security, cyberspace, and security-by-design concepts.
1.3 Privacy preservation and privacy-by-design.
1.4 Classification of threats and threat actors.
1.5 Elements of computer networking.
1.6 Elements of Cyber Threat Intelligence: from data to intelligence and its sources (CTI).

2 Cyber attacks, defence, and resilience

2.1 Basic cybersecurity taxonomy.
2.2 Classic cyber threats: malware types from viruses to RATs and APTs.
2.3 Large-scale cyber threats: ransomware, DDoS, supply chain attacks.
2.4 Social engineering based attacks.
2.5 Overview of cyber-defence technologies and procedures.
2.6 Security testing.

3 Cryptography

3.1 Symmetric and asymmetric cryptography.
3.2 Encryption/decryption and hashing labs.
3.3 From certification authorities (CA) to non-repudiation.
3.4 Secrets' management and perfect forward secrecy (PFS).
3.5 Post-quantum cryptography (PQC) and the risks posed by quantum computing.

4 Digital Trust and Electronic Identification

4.1 Trust services pursuant to the eIDAS Regulation.
4.2 Lab of digital and electronic signing.
4.3 Applied cryptography: payments cards; secure authentication (TLS); internet browsing.
4.4 Electronic identification, self-sovereign identity, the EUDI Wallet (+ labs).

5 Cybersecurity e "Big Data"

5.1 Structured, semi-structured and unstructured data.
5.2 Big Data characteristics: velocity, volume, value, variety and veracity.
5.3 Data anonymity (*DB*-anonymity).
5.4 Exploiting surface, deep and dark web (DDW) for information gathering.
5.5 Big Data analysis techniques for proactive threat detection.
5.6 *DB*-anonymity and information gathering labs.

6 Privacy-enhancing technologies (PETs) and labs

6.1 Introduction to Privacy-enhancing technologies.
6.2 Homomorphic encryption.
6.3 Secure multi-party computation and private set intersection.

6.4 Federated learning.
6.5 Differential privacy.
6.6 Synthetic data.
6.7 Labs of PETs.

7 Artificial Intelligence and Data Security

7.1 Research and development trends in AI use cases.
7.2 AI and LLM attack types and frameworks.
7.3 AI security testing, *aka* "AI red teaming".

Materiale didattico

Ai discenti saranno fornite le *slide* del corso, da usarsi esclusivamente per le finalità del Master.