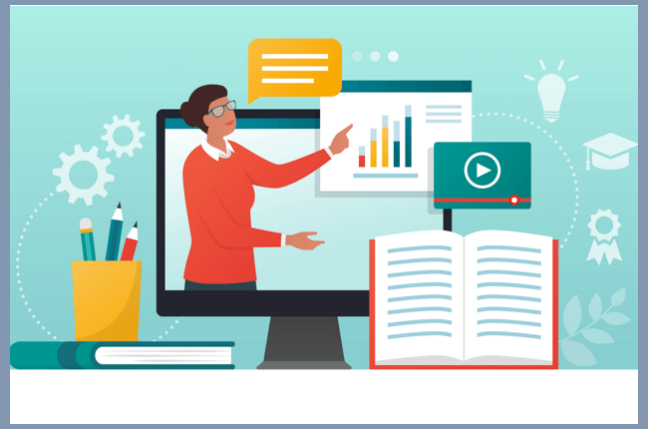
Security and Privacy

2023/2024

Presentation

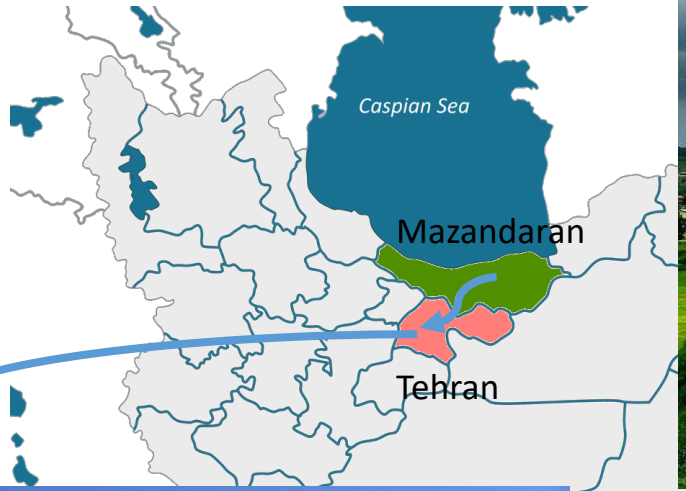


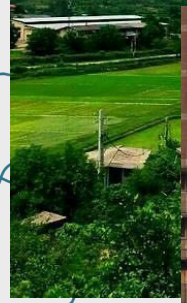
- Overview & Organization
- Course Contents
- Course Schedule
- Evaluation
- Bibliography

Professor

- Name: Naghmeh Ivaki
- Email: naghmeh@dei.uc.pt
- Office: D2.21
- Service Time: Tuesday 13h30 – 17h00
- Skype: naghmeh.ivaki
- Personal Zoom: https://videoconf-colibri.zoom.us/j/7035229271
- Website: https://eden.dei.uc.pt/~naghmeh/

About me





Professor

- Finished Ph.D in in Information Science and Technology, in 2016
- Taught practical classes in 5 editions of subjects at the University of Coimbra (From 2014 to 2018) as invited assistant professor
- Invited Professor at the department of informatics engineering, at the superior school of technology and management of the polytechnic institute of Viseu (IPV) in 2018-2019 (1 semester)
- Invited Professor at ISCAS (1 semester)
- Currently
  - Assistant Professor At the University of Coimbra
  - Full member of Software and Systems Engineering Group (SSE) of the Centre for Informatics and Systems (CISUC), Department of Informatics Engineering, University of Coimbra

Professor

- **Research Interests**

  - Dependability and Security Assessment
  - Secure Coding
  - Safety and security of Unmanned Areal vehicles (UAV)
  - U-space services Security of Blockchain and Smart Contracts

Presentation of Course

- Scientific Area: Security

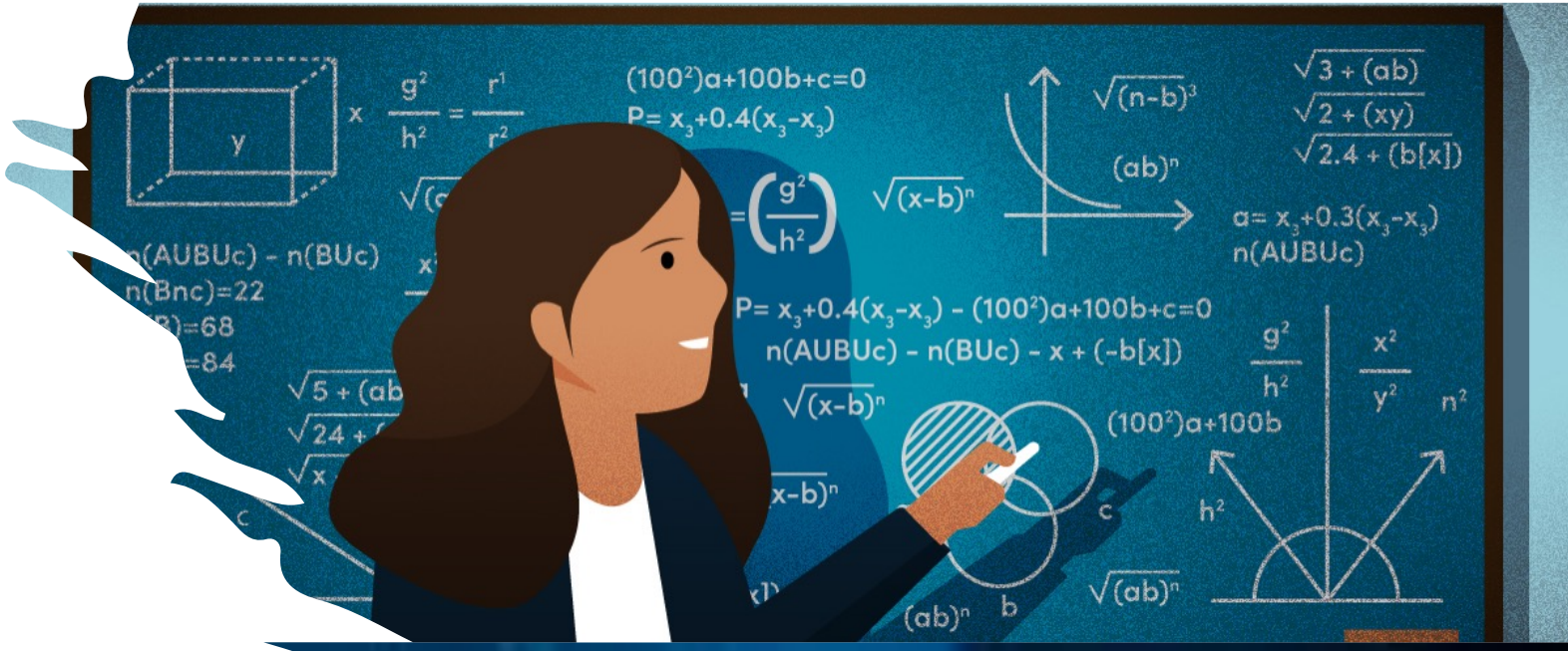
  - Major: Master in Data Science and Engineering
  - 1st Year, 1st Semester
  - Corresponds to **6 ECTS** (a total of 4 hours of classes)

Organization of the Classes

- Weekly distribution of the classes
  - **Theoretical** classes: 2h00
  - **Practical** classes: 2h00

- **Theoretical** classes (Lecture classes):
  - Theory & Concepts
  - Thursday 16:00 - 18:00

- **Practical** classes (Lab classes):
  - Practice and support to assignments
  - Thursday 18:00 - 20:00



Classes

- Presential

- Materials: https://ucstudent.uc.pt
- Assignments: https://inforestudante.uc.pt

Course contents

- Security & Privacy Concepts
- Cryptography: Symmetric and Asymmetric
- Privacy-Preserving Data Publishing (PPDP)
- Synthetic Data
- Secure Multiparty Computation and Privacy (SMC)
- Adversarial Machine Learning
- Homomorphic Encryption
- Federated Learning Privacy
- Enterprise Privacy: Principles, Laws and Ethics

Lectures schedule

Week	Month	Date	Theoritical Classes	Assignments	Case Studies	Practical Classes
1	September	21	Course Presentation; Security & Privacy Concepts			WEB AND MOBILE PRIVACY AWARENESS
2	September	28	Cryptography: Symmetric and Hashing			Excercises with Symmetric Encryption and Hashing
3	October	12	Cryptography: Assymetric, Signatures, Communication	Assignment 1 (3 weeks)	Case study 1 (3 weeks)	Exercises with assymmetric encryption and signatures
4	October	19	Privacy-preserving Data Publishing I : Privacy Models, Risk and Information Loss			ARX - DISTINCTION, SEPARATION, RE-IDENTIFICATION RISK
5	October	26	Privacy-preserving Data Publishing III : LKC and Diferential privacy			Exercises with diferential privacy
6	November	2	**CS1: Disscusion**			**Assignment 1 Defence**
7	November	9	Synthetic data			Exercises with synthetic data
8	November	16	Secure Multiparty Computation (SMC) and Private Data Mining	Assignment 2 (4 weeks)	Case study 2 (4 weeks)	Secure Multiparty Computation (SMC) techniques in practice
9	November	23	Homomorphic Encryption for Data Scientists (Qianying Liao)			Exercises with homomorphic and searchable encryption
10	November	30	Adversarial Machine Learning (Inês Valentim)			Adversarial ML Exercises
11	December	7	Federated Learning Privacy (João Vilela)			Support to Practical Assignment
12	December	14	Enterprise Privacy: Principles, Laws and Ethics + **CS2: Discussion**			**Assignment 2 Defence**

Evaluation

- Final exam: `10 points`
- 2 Assignments: `8 points`
  - Individual/Group
  - Presented/discussed in Lab classes
  - Defense is individual
- 2 Case-studies: `2 points`
  - Individual
  - Writing up to 1 page on the given subject
  - Presented/discussed in lecture class
- Pass thresholds
  - Exam **35.0%**
  - Final grade (total) **47.5% (>=9.5 out of 20)**

Plagiarism implies exclusion from course

Assignment 1

- Group work allowed (maximum 2 students)
- Release: October 12
- Deadline: November 01

- Defenses:
  - Slots will be made available on inforestudante

Assignment 2

- Group work allowed (maximum 2 students)
- Release: November 16
- Deadline: December 13

- Defenses:
  - Slots will be made available on inforestudante

Bibliography

- **Introduction to Computer Security**, *Goodrich & Tamassia, Pearson, 2014*
- **Cryptography and network security**, *Stallings, Pearson, 2017*
- **Network Security Essentials: Applications and Standards,** *Stallings, 2016*
- **Guide to the De-identification of Personal Health Information**, *Khaled El Emam, CRC 2013*
- **Anonymizing Health Data, Khaled El Emam**, *Luk Arbuckle, O'Reilly, 2014*
- **Information Security: Principles and Practice**, *Stamp, Wiley, 2011*
- **Introduction to Privacy-Preserving Data Publishing Concepts and Techniques**, *Fung et al., CRC 2011*

Acknowledgment

Some Materials are based on materials of:

- **João Vilela's MSI_SP_2019**
- **Nuno Antunes's MSI_SP_2022**
- **Antunes's MECD_SP_2022**