COM-301 Computer security
Troncoso Carmela

Summary
This is an introductory course to computer security and privacy. Its goal is to provide students with means to reason about security and privacy problems, and provide them with tools to confront them.

Content
• Security principles
• Access control
• Authentication mechanisms: biometrics, tokens, passwords
• Applied cryptography: basic notions and algorithms
• Privacy in a digitalized world

Learning Prerequisites
Recommended courses
CS-233 Introduction to Machine Learning (for programming)
COM-208 Computer Networks

Important concepts to start the course
Basic notions TCP/IP, basic notions programming

Learning Outcomes
By the end of the course, the student must be able to:
• Recognize security properties of systems, as well as formulate security policies, and model the threats they may face.

Teaching methods
Lectures with real world examples, and complementary exercises to reinforce basic concepts.
Practical homeworks to better understand adversarial behavior

Expected student activities
Attending lectures, solving exercises, reading and demonstrating understanding of provided materials.

Supervision
Resources

Bibliography
Computer security by Dieter Gollmann
Security Engineering by Ross Anderson
Computer Security: Principles and Practice by Stallings and Brown

Prerequisite for
• COM-402 Information security and privacy
• CS-523 Advanced topics on privacy enhancing technologies