Cryptography and Information Security
MAP-I Curricular Unit 2017-18

Summary

This document describes a Ph.D. level course, corresponding to a CurriculaR Unit credited with 5 ECTS. It is offered jointly by the Departamento de Informática at Universidade do Minho, the Departamento de Electrónica, Telecomunicações e Informática at Universidade de Aveiro and the Departamento de Ciência de Computadores at Universidade do Porto in the MAP-I doctoral program.

Coordinators:

José Manuel E. Valença (DI-UM), André Zúquete (DETI-UA)
Luís Antunes, Manuel Barbosa (DCC-FCUP)

Context

This document describes a Ph.D. level course, corresponding to a Curricular Unit credited with 5 ECTS. It is offered jointly by the Departamento de Ciência de Computadores at Universidade do Porto, and the Departamento de Informática at Universidade do Minho in the MAP-I doctoral program.

Objective

The objective of this course is to expose students to cutting-edge research topics in relevant areas in information security, namely cryptography and systems' and network security.

It is not intended as an introductory survey in any of these areas. Instead, the focus will be on advanced topics and recent results. The course will emphasise definitions, foundations, and a formal approach to information security.
The course is at a similar level and covers overlapping material with the following advanced modules taught at leading academic institutions in the information security area, namely:

- Advanced Topics in Cryptography, J. Katz, Univ. of Maryland
- Foundations of Cryptography, M. Naor, Weizmann Institute of Science
- Network Security, Jason Crampton, Royal Holloway.
- Computer Security, Chris Mitchell, Royal Holloway.

Instructors

- Manuel E. Valença (DI-UM)
- André Zúquete (DETI-UA)
- Luís Antunes (DCC-FCUP)
- Manuel B. Barbosa (DCC-FCUP)

Prerequisites

Basic knowledge of cryptography and networking are desirable, but not necessary. Students who have not previously taken courses in these topics may have to work harder and do more outside reading in order to keep up.

Learning outcomes

- Familiarity with scientific challenges in cryptography and information security.
- Ability to extract information from scientific papers in the area.
- Technical writing and presentation skills.
- Comfortability with security proofs and ability to think abstractly about information security problems.
- Understand the use and operation of a range of access control and user authentication mechanisms.

Format

Lectures (including guest lectures), discussions and student presentations.

Grading

The evaluation is divided in four equal parts, each corresponding to each of the four main content parts. The evaluation may include a writen exam, a project, or a written assignment and a presentation.

Course Content

- Foundations of Cryptography
  - One-way functions, commitment schemes, one-way permutations, hard-core bits, and pseudorandomness.
  - Public-key encryption: security definitions, hybrid encryption, example schemes.

  - Zero Knowledge, Non-Interactive Zero-Knowledge and its use in achieving chosen ciphertext security.
  - Public-key signatures: security definitions, one-time signatures, examples schemes.

- Network security
  - Introduction to Networking, Network Security and Secure Protocols.
  - Public key certification.
  - Secure Protocols: IPSec, SSL/TLS and SSH.
  - Network security architectures: 802.11i.

- Access control and user authentication mechanisms
  - Security policies; security models; mandatory and discretionary access control; access control matrix, capabilities and access control lists.
  - User authentication: passwords, biometrics and user tokens; identity management.
  - Introduction to Smart Cards; Assets for Cyber Security.
  - Smart Cards in eIDs/Passports

- Privacy and Legal Aspects
  - Privacy by Design
  - Anonimization Techniques
  - Data protection legislation

Textbooks and Reading Material

- Foundations of cryptography Vol. 1 and 2, Oded Goldreich, Cambridge university press.
- Lecture Notes on Cryptography, M. Bellare and S. Goldwasser (available on-line).
- Introduction to Modern Cryptography, Mihir Bellare and Phillip Rogaway (available on-line).
- Segurança em Redes Informáticas. André Zúquete, Editora FCA, (4th edition).
- N. Ferguson, B. Schneier, and T. Kohno. Cryptography Engineering: Design Principles and Practical Applications, John Wiley & Sons, 2010.
- D. Gollmann, Computer Security, John Wiley & Sons, 2011 (3rd edition).