Advanced Topics in Information Security
MAP-I Curricular Unit – 2009/2010

Summary

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

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

Coordinators: Manuel B. Barbosa, José Manuel Valença, (DI-UM)
João Barros, (DEEC-FEUP), André Zúquete (DETI-UA)

Context

This document describes a Ph.D. level course of the MAP-I doctoral program, offered jointly by the Departamento de Informática at Universidade do Minho, the Departamento de Ciência de Computadores at Universidade do Porto and the Departamento de Electrónica, Telecomunicações e Informática at Universidade de Aveiro.

This proposal is an updated version of the 2007/2008 and 2008/2009 editions of the same course, which were accepted for the MAP-I doctoral program under the Foundations of Computing topic, and accredited by Carnegie Mellon University within the CMU-Portugal initiative.

This proposal aims to instantiate the Curricular Unit in Theory and Foundations of Computer Science or, alternatively, the Curricular Unit in Technologies.

Course Description

This course covers both computational and information-theoretic security approaches, as well as their combined use in cryptography. These complementary views are presented by instructors who conduct active research in these fields. The course also covers the application of information security technology to real life problems, including selected computer and network security topics. Critical information society services, such as electronic voting, secure identification and privacy protection, will be used as case studies of both the theoretical and

practical issues involved, taking advantage of the experience of the instructors in these areas.

The course is not intended as an introductory survey in any of these areas, although it is planned that, throughout the course, some of the lectures will be crash-courses where relevant background is revised. Instead, the focus will be on advanced topics and recent results. The course will emphasise definitions, foundations, and a formal approach to information security.

Prerequisites

Basic knowledge of cryptography, complexity theory 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.

Textbooks and Other Required Materials

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:

- Topics in Cryptography, D. Boneh, Stanford University
- Advanced Topics in Cryptography, J. Katz, Univ. of Maryland
- Number Theory/Cryptology course, R. Cramer, University of Ultrecht
- Current Topics in Information Security, U. Maurer, ETH Zurich
- Foundations of Cryptography, Y. Lindell, Bar Ilan University
- Foundations of Cryptography, M. Naor, Weizmann Institute of Science
- Privacy and Anonymity in Data, L. Sweeney, CMU
- System Security, A. Myers, Cornell University

Recommended reading materials include:

- 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)
- A Computational Introduction to Number Theory and Algebra, Victor Shoup, Cambridge University Press

- Handbook of Applied Cryptography, A.J. Menezes, P.C. van Ooorschot, and S.A. Vanstone (available on-line)
- Quantum Computation and Quantum Information, M.A. Nielsen, I. L. Chuang, Cambridge University Press
- Secret key agreement by public discussion from common information, U. Maurer, IEEE Transactions on Information Theory, 1993 Ueli Maurer
- Information-Theoretic Cryptography, Advances in Cryptology, LNCS Vol. 1666, Springer-Verlag, 1999.
- Seminal and high-impact publications in information security.
- Selected publications by the instructors.

Course Objective

The objective of this course is to expose students to cutting-edge research topics in relevant areas in information security. The course will cover both theoretical and applied issues in information security and students are expected to acquire the following skills:

- Familiarity with scientific challenges in 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.
- Increased sensibility to privacy issues, anonymity requirements and related protection/anonymisation techniques.

Topics Covered

- Foundations of cryptography
  - Introduction and background: a rigourous approach to cryptography, the focus of the foundations of cryptography, background of the computational model.
  - One-way functions, trapdoor permutations, hard-core predicates, computational indistinguishability and pseudorandomness.
  - Reductionistic security arguments, the Random Oracle Model and the Generic Group Model.
  - 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, example schemes.

- Applications of computational number theory to cryptography
  - Background topics in elementary number theory
  - Prime numbers, primality testing and factorisation
  - Finite groups, finite fields and discrete logarithm cryptosystems
  - Elliptic and hyperelliptic curve cryptography
  - Bilinear pairings in cryptography and algebraic immunity

- Information theoretic security and quantum cryptography
  - Basic elements of Shannon Theory
  - Unconditional authentication
  - Unconditional secrecy
  - Unconditional secret key agreement
  - Privacy Amplification
  - Secrecy capacity of communication networks with eavesdroppers
  - Secure multi-party computation, commitment, oblivious transfer
  - Basic aspects of quantum mechanics
  - Quantum information Theory
  - Quantum key distribution

- Privacy and anonymity concerns and solutions
  - Identification data (biometric data, genomic data, digital identity)
  - Daily-life data (phones, e-mails, bank accounts, visa cards, etc.)
  - Behaviour profiles (shopping, web browsing, exchanging mail, etc.)
  - Malware, spyware, phishing, cookie management.
  - Examples of anonymity requirements (e-comerce, e-voting, etc.)
  - Examples of anonymity annoyances (IP spoofing, spamming, etc.)
  - Anonymization techniques, services and networks.
  - Counter-measures against anonymity annoyances.
  - Reputation systems.

Expected Number of Students

Expected number of students is 15.

Class Schedule

Lectures, discussions and student presentations. The course corresponds to 42 lecturing hours, during one complete semester. Tentative class schedule: 2 hour lecture + 1 hour tutorial per week, for 14 weeks.

Student Evaluation Criteria

- 50% Final exam
- 40% Written assignments (scribing) and paper presentations
- 10% Class participation

A total final score under 50% means the student fails the course. To recover the course credits, and assuming the MAP-i program operation allows for this possibility, a failed student must re-take the final exam which will then represent 100% of the final score.

Course Staff

Teaching workload will be evenly distributed among the following instructors:

- Manuel B. Barbosa (DI-UM) – Contact person (`mbb@di.uminho.pt`)
- João Barros (DEEC-FEUP)
- José M. Valença (DI-UM)
- André Zúquete (DETI-UA)

Course Web Page

The web-page for the 2007/2008 edition of the course can be found at the following address `http://www.dcc.fc.up.pt/~barros/teaching/atis0708/`.