Advanced Topics in Information Security

LESI/LMCC

M. B. Barbosa (mbb@di.uminho.pt)
J. Barros (barros@dcc.fc.up.pt)
J. M. Valença (jmvalenca@di.uminho.pt)
A. V. Zúquete (avz@det.ua.pt)

2007/2008

Overview

- The objective of this course is to expose students to **cutting-edge research topics in relevant areas of information security**.
- The course will cover both **theoretical and applied issues in information security**.
- It will address the **computational and information-theoretic views of security**, as well as their combined use in cryptography.
- **Critical information society services**, such as electronic voting, secure identification and privacy protection, **will be used as case studies**.
- The course has been **accredited by CMU**.

Organisation

- **Information-theoretic Security and Quantum Cryptography**
  Speaker: João Barros, DCC, FC, U. Porto
  Schedule: 15/10/07 - 5/11/07
- **Applications of Computational Number Theory to Cryptography**
  Speaker: José Manuel Valença, DI/CCTC, U. Minho
  Schedule: 12/11/07 - 3/12/07
- **Foundations of Cryptography**
  Speaker: Manuel Bernardo Barbosa, DI/CCTC, U. Minho
  Schedule: 10/12/07 - 14/1/08
- **Privacy and Anonymity Concerns and Solutions**
  Speaker: André Zúquete, DET/IEETA, U. Aveiro
  Schedule: 21/1/08 - 11/2/08

Evaluation

- Final mark will have **5 components of equal weight**.
- **Each of the four modules will end with a written test.**
- **All students will be required to present** (at least) **a paper** from a selection of ground-breaking papers in information security.

Information Theoretic Security and Quantum Cryptography

- Fundamentals of Information Theory
- Perfect Secrecy and Information-Theoretic Security
- Secrecy Capacity of Wiretap, Gaussian and Wireless Channels
- Interplay between information-theoretic security and upper-layer cryptography
- Security Protocols and Secret Key Distribution at the Physical Layer
- Parallels with Quantum Cryptography
- Secure Network Coding and Secure Multi-Party Computation
- Slides available at `http://www.dcc.fc.up.pt/~barros`

Applications of Number Theory to Cryptography

- Applications of elliptic curves to cryptography.
- Hard problems from computational number theory with application in cryptography:
  - Factoring and RSA problem.
  - Discrete Logarithm problem.
  - Diffie-Hellman problem variants.
- Pairings over groups of points of elliptic curves and their constructive and destructive applications.
  - Weak elliptic curves.
  - Identity based cryptography.

Foundations of Cryptography

- Security reductions, sequences of games and other computational security concepts and technicalities.
- Rigourous definition of security for public-key encryption.
- Construction of secure public-key encryption from trapdoor permutations.
- Chosen-ciphertext security for public-key encryption.
- Rigourous definition of security for digital signatures.
- The Random Oracle Model and security proofs for digital signature schemes.
- Combination of encryption and signature primitives.
- Interactive proofs and proofs of knowledge.

Privacy and Anonymity Concerns and Solutions

- Privacy concerns, anonymity requirements, security risks
- Anonymity taxonomy
- Anonymous relaying
- Anonymous routing
- Anonymization solutions for e-voting
- Anonymization solutions for e-commerce
- Anonymization and P2P
- k-anonymity