Tecnologias de Segurança (ou Segurança Aplicada)

Ibéria Medeiros

Departamento de Informática

Faculdade de Ciências da Universidade de Lisboa

Instructor

- ❑ Lectures
  - – Prof. Ibéria Medeiros (imedeiros@di.fc.ul.pt)   - course respons.
  - – Lecture times:
    - » Tuesday,   16h30-18h30, room 6.2.52
    - » Tuesday,   18h30-20h00, room 6.2.52
  - – Student contact hours:
    - » Thursday,   15h00-16h00, room 6.3.25

Communication

❑ Web Page:
- – https://moodle.fc.ul.pt
- – official and current information of the course

❑ News group:
- – available at moodle.fc.ul.pt
- – to be used by students and instructors for posting and discussion about all aspects of general interest

❑ Individual instructor email address:
- – use only when none of the above applies

❑ Student contact hours

Topics for the Semester

❑ Cryptography – a deeper look into selected algorithms/protocols

❑ Authentication and Key Distribution

❑ Wireless Communication – security in Personal/Local/Metro./Wide Networks

❑ RFID – Radio Frequency Identification security

❑ Network security – focus on IPsec

❑ Transport security – focus on SSL/TLS

❑ Electronic Payment Systems & Smart Cards Security

❑ Email security and Privacy Issues

Prior knowledge: should have attended a course in introductory security; and related subjects like networks, operating systems and distributed systems.

Bibliography

- William Stallings, **Cryptography and Network Security, 6ᵗʰ Edition, 2014** (there is a **new edition, the 7ᵗʰ, that came out in 2016**)

  Selected papers and other documents.

- Some other books:
  - Madjid Nakhjiri, Mahsa Nakhjiri, **AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility**
  - Selim Aissi, et al, **Security for Mobile Networks and Platforms** (Artech House Universal Personal Communications)
  - Frank Thornton, Chris Lanthem, **RFID Security**
  - Donal O´Mahony, et al, **Electronic Payment Systems for E-Commerce: Second Edition**
  - C. Kaufman, R. Perlman, M. Speciner, **Network Security: Private Communication in a Public World (Second Edition)**

Grading

❑ Main components of the evaluation:

  – 40% Project   (includes participation in classes)
  – 10% Paper presentation (includes participation in discussions)
  – 50% Final exam

❑ Notes

  –   There will be one project in two phases
               maybe related to the implementation of a cyber-range!
  – Projects and presentations are done in groups of 3 students
  – Dates for the projects are already available at the web site and there are **no extensions**

  – There is a minimum grade of 10 for both components of the evaluation!!!