EECE 798
Special Topics – Wireless Security

Course description


Course pre-requisites

EECE 450 – Computer Networks, or equivalent
EECE 632 – Cryptography and Computer Security

Course instructor

Ayman Kayssi
Email: ayman at aub dot eduard lb
Extension: 3499
Office: 404 RGB
Office Hours: T, R 8:00 – 10:00 am and by appointment

Course objectives

The objectives of this course are to:
(1) Provide students with an overview of the general security challenges in wireless networks
(2) Gain insight into the security problems facing existing (GSM, UMTS, WiFi, Bluetooth) and upcoming (Mesh, Ad-hoc, Sensor, Mobile, Vehicular, RFID) wireless networks
(3) Prepare students for research in the area of wireless security
(4) Enhance students communication and team work skills

Course topics

- Vulnerabilities of wireless networks
- Security requirements in wireless networks
- How existing wireless networks are secured
  - GSM
  - UMTS
  - WiFi
  - Bluetooth
- Trends and security challenges in wireless networks for upcoming wireless networks
  - Mesh
  - Ad-hoc
  - Sensor
  - Mobile
Vehicular
- Trust
- Privacy protection
- Attacks against naming and addressing
- Establishment of security associations
- Securing neighbor discovery
- Secure routing in multi-hop wireless networks
- Selfish behavior

**Course outcomes**

By the end of the course, students:

1. Have an understanding of the security vulnerabilities of wireless networks
2. Are able to specify security requirements for wireless networks
3. Understand how existing wireless networks are secured
4. Appreciate the security challenges in upcoming wireless networks
5. Are able to define trust and how it applies to wireless networks
6. Have an understanding of privacy concerns and the need for its protection
7. Are able to detect and defend against attacks targeting naming and addressing
8. Understand the procedures for establishment of security associations
9. Appreciate the issues in securing neighbor discovery
10. Understand secure routing in multi-hop wireless networks
11. Are able to detect and guard against selfish behavior in wireless networks
12. Increased their interest in the field of wireless security research
13. Enhanced their team work skills
14. Enhanced their communication skills

**Course textbook**

In addition, a reading list will be posted on Moodle.

**Course assessment**

Students are expected to attend the lectures, contribute to class discussions, and perform wireless security research in a relevant area of their choice, with the approval of the course instructor. After reviewing the major research contributions from the literature in an area of choice (at least three papers), students should write a review and present it in class for discussion. Based on the research review, students will propose a research project idea in consultation with the course instructor. The idea will be developed during the semester and results will be prepared for publication as a research paper.

1. Research review 20%
2. Research project and results 25%
3. Research paper 30%
4. Contribution and participation 10%
5. Final exam 15%

**Course schedule**

Weekly: Two 75-minute lectures (T, R 2:00 – 3:15 pm)