CSCE 790: Security and Privacy for Emerging Ubiquitous Communication system

Course Syllabus

Catalog Description:

This course will be an introduction to the security and privacy issues associated with wireless networks.

Prerequisite(s) by Topic:

Basic background knowledge of wireless networks and cryptography are preferred but not required.

Format:

The format of the course will be a combination of formal lectures, paper reading and student presentation. The instructor will first give overview lectures on the background, and then students will present papers in the field.

Textbook:

No book is required. The lecture material will be derived from a number of background papers.

Tentative list of wireless networks that will be covered:

- Bluetooth
- WiFi/802.11
- Vehicular Networks
- Sensor Network
- RFID (Radio-Frequency Identification)

Tentative topics include but not limited to:

- Secure localization;
- RFID privacy;
- Spoofing attacks;
- Jamming attacks;
- Temporal-location privacy in sensor network
- Wormhole attacks;
- Selfish behavior;
- Secure routing
- Spatio-temporal Access Control

Student work:

Papers will be presented by students. Each week, the presenter must meet with the instructor during office hour to go over presentations to be given that week. Other students must post a summary for each paper to be discussed that week before class.

Students MUST do a team project and write a position paper.

Grading:

20% presentations
10% paper summaries (Summarize 80% of the required readings before class)
40% project
10% position paper
20% class discussions and participation