Proposed course in the BS, MS, PhD CS/CY program: CY4760/CY6760 Security of Wireless and Mobile Systems

This course focuses on Security and Privacy in Mobile and Wireless Systems. Recent years have seen massive deployment of wireless devices and technologies around us. They are deployed in a wide variety of systems such as telephony, navigation, sensor networks, critical infrastructures etc. With the advent of the Internet of Things and autonomous cyber-physical systems, the proliferation of these wireless systems is only bound to increase. The broadcast nature of wireless technologies and the increased availability of software defined radios have not only improved quality of life but pose significant security challenges.

This course provides the foundations to understand the security and privacy threats and defenses in wireless and mobile systems specially in the era of softwarization of wireless networks. After this course, the students should be able to describe and classify security goals and attacks in modern wireless networks. They should be able to identify the unique security implications of these effects and how to mitigate security issues associated with them.

Required topics include:

- ✤ Basic security concepts:
 - ➤ confidentiality, authentication, integrity
 - > symmetric key and asymmetric key cryptography and ciphers
 - ➤ example ciphers such as AES, RSA, RC4
- ✤ Fundamentals of wireless & mobile systems:
 - ➤ key features and mechanisms of wireless and mobile systems,
 - ➤ basic signal processing topics such as frequency transforms, filtering, radio transceiver architecture.
- Availability/Integrity issues in wireless networks:
 - ➤ jamming/anti-jamming techniques,
 - eavesdropping, insertion/modification,
 - ➤ wireless channel based key agreement
 - broadcast authentication techniques
 - ➤ secure key distribution in large scale ad-hoc networks
- Security and privacy issues in current wireless & mobile Systems:
 - ➤ WiFi security (WEP, WPA, WPA-Enterprise, WPA2, WPA3)
 - ➤ Cellular security (GSM, 3G, LTE, 5G-NR),
 - ➤ location tracking, traffic analysis.
 - ➤ ciphers KASUMI, A5, SNOW
- Low-power Wireless Network Security and Privacy:
 - ≻ Bluetooth
 - ➤ Zigbee, LoRA

- ≻ RFID
- Secure Localization and Proximity Verification:
 - ➤ GNSS (GPS, Galileo, Glonass) security,
 - ➤ ranging protocols and their vulnerabilities

Pre-requisites: none

Textbook for the course

• None Required.

After completing this course, the student will be able to demonstrate the following competencies:

1) Describe and classify security goals and attacks in modern wireless networks. 2) Identify the unique security implications of these effects and how to mitigate security issues associated with them.

Deliverables

The coursework includes review of state-of-art in wireless security and producing one-page summaries along with two presentations of research published in top-tier conferences. There will be a set of practical laboratory assignments that will support the concepts taught during the lectures. The students will also submit an end-of-semester project chosen from the concepts covered during the lectures.

Justifications

Wireless systems and networks are ubiquitous and key in enabling many security- and safety-critical applications and services. The broadcast and erratic nature of wireless signals have significant impact on the security and privacy implications requiring unique methodologies to address fundamental security and privacy challenges of authentication, identification, confidentiality, and reliability. Recent years have also seen an increasing number of threats and vulnerabilities in prominent wireless systems (e.g., WiFi passphrase cracking, GPS spoofing, jamming, mobile user location tracking). This course will enable students understand, describe, and implement a secure wireless network using physical- and logical-layer primitives.

This course complements CS4710/CS6710 Wireless Networks/Mobile Systems course. The proposed course will become an essential course for BS students who are concentrating in Cybersecurity Concentration in Cyber Operation and is required to meet NSA designation.

Related courses

CS4710/6710 – Covers fundamentals of wireless and mobile networks. Does not cover security and privacy issues as per the charter.

CS5700 – Covers the architecture, algorithms, and protocols of the Internet with topics such as local area networking, routing, congestion control, network security, and applications such as peer-to-peer and content distribution networks. Does not cover wireless protocols and networks.