Mobile Security and Privacy

Shengli Yuan, University of Houston - Downtown

Lila Ghermi, Texas Southern University

Objectives:

- Introduce the concepts of security and privacy of mobile infrastructure, mobile devices, and mobile applications.
- Discuss the types of threats that can potentially undermine mobile security and privacy.
- Study the methods and approaches to protect and enhance mobile security and privacy.

Overview:

- Intended audience: Seniors or first year graduate students.
- Prerequisites:
    - Introductory network course
    - Security course
    - Programming course
- Hours: A total of 12 hours including lectures and labs.

Topics:

- Overview: 2 hours
    - Definition of Security and Privacy
    - Hackers, Governments
    - Security Goals: Prevention, Traceability and Auditing, Monitoring, Privacy and Confidentially
- Mobile infrastructure security: 6 hours
- Mobile device security: 2 hours
- Mobile application security: 2 hours

Mobile Infrastructure Security:

- Objectives:
    - Understand the security and privacy threats to the mobile infrastructure
    - Understand the basic strategies and approaches to enhance mobile infrastructure security and privacy.
- Lectures: 4 hours
    - Carrier networks: cellular networks
    - Enterprise networks: Wifi networks

        - Treats: Eavesdropping, interceptions, tracking, unauthorized access, malware.
        - Mitigations: Encryptions, VPN, carrier SLA, authentication, malware scan
- Labs: 2 hour
    - Install and configure a 802.11 network.
    - Simulate eavesdropping attack. Install and configure software to capture and decrypt WiFi traffic. Deploy security tools to counter eavesdroppers.

Mobile Device Security:

- Objectives:
    - Understand the security and privacy threats to the mobile devices
    - Understand the basic strategies and approaches to enhance mobile device security and privacy.
- Lectures: 2 hours
    - Treats: Physical threats, unauthorized user, data and location privacy, vulnerable OS, malware, data loss
    - Mitigations: Device configuration, user authentication, apps certification, data encryption

Mobile Application Security:

- Objectives:
    - Understand the security and privacy threats to the mobile applications
    - Understand the basic strategies and approaches to enhance mobile application security and privacy.
- Lectures: 2 hours
    - Treats: coding vulnerability, data and location privacy, malware, data leakage
    - Mitigations: Application certification and configuration, encryption, key management, location management

References:

- Introduction to Network Security, by N. Kravets, Thomson
- 802.11 Wireless Networks, by M. Gast, O'Reilly
- Building Secure software, by J. Viega and G. McGraw, Addison-Wesley , 2005
- http://www.usatoday.com/tech/news/story/2012-03-22/lost-phones/53707448/1
- US-CERT Resource: Paul Ruggiero and Jon Foote, "Cyber Threats to Mobile Phones"
- http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf)
- https://sites.google.com/site/mobilesecuritylabware/home