CPR E 537: Wireless Network Security

Topics

With the penetration of mobile device use as well as embedded and cyber-physical systems deployment, the underlying wireless communication and network systems have become critical society infrastructures, and thus their security and privacy are critical to the wellbeing of our society. This course will exam the challenges in providing secure communication and network services in a variety of wireless systems, as well as the existing and emerging approaches to managing these challenges. *Focus* will be placed on securing the operation and performance of wireless networks, with less emphasis on information security. *Topics* to be covered include vulnerabilities, attacks, security mechanisms, and trade-offs at various layers of the network protocol stack, from aspects of physical communication to application and service security issues; examples include jamming, MAC-layer misbehavior, selective packet dropping, decentralized trust and reputation, and cross-layer holistic attacks. Systems of interest include, but are not limited to, personal devices, connected vehicles, IoT and cyber-physical systems, wireless infrastructure, and ad hoc networks.

A tentative schedule for the course is as follows: (note: the actual schedule is subject to change depending on class interest and progress.)

Week	*Topics*
Module 1: Foundation	
1-4	• Introduction to security of existing and emerging wireless networks • Introduction to wireless communication and networking • Introduction to cryptographic algorithms and protocols • Introduction to game theory • Case studies: cellular, WiFi, Bluetooth, MANET, VANET etc
Module 2: Secure Wireless Links	
5-6	• Physical-layer threats, jamming, eavesdropping, physical-layer security
7-10	• Naming and addressing, Sybil and replication attacks • Security associations • Secure neighbor discovery • Selfishness at MAC layer, MAC misbehavior • Data-driven misbehavior detection
Module 3: Secure Wireless Networks	
11-12	• Secure routing • Selfishness in packet forwarding • Wireless transport security
Module 4: Cross-Cutting & Adventure	
13-15	• Cross-layer attack and defense • Operators in shared spectrum • Privacy protection • Trust and reputation • Behavior enforcement • Bleeding-edge research (article) discussion (if time permits)

Besides lectures, the course will offer student-centered hands-on projects where students will have the opportunity to investigate, implement, and experiment with wireless security attacks and counter-measures.

Course Objectives

The objective of this course is to cultivate the following capabilities among students:

- Students will be able to remember and apply fundamental techniques of secure wireless systems. In particular, students will remember and apply threats and security techniques related to the following aspects of wireless systems:
  - Physical layer of wireless communication
  - Link layer of wireless networks: naming and addressing, associations, neighbor discovery, MAC
  - Network and transport layers of wireless networks: routing, packet forwarding, transport-layer messaging
  - Cross-cutting issues of wireless networks: spectrum sharing, cross-layer interactions, system-level behavior enforcement
  - Privacy, trust, and reputation
- Students will be able to analyze specific threats and countermeasures in case studies of wireless systems such as WiFi, Bluetooth, cellular, VANET, MANET, and Zigbee systems.
- Students will be able to implement wireless network threats and countermeasures.

Student Outcomes

Through the course, students will be able to:

- Demonstrate fundamental techniques of secure wireless systems.
- Use current techniques, skills, and tools necessary for secure wireless networking practice.
- Apply design and development principles in the construction of secure wireless networking systems of varying complexity.
- Analyze secure wireless networking problems and identify and define networking requirements appropriate to their solutions.
- Design, implement, and evaluate a secure wireless networking system, process, component, or program to meet desired needs.
- Function effectively on teams to accomplish a common goal.

Credits: 3

Prerequisites

CPR E 489 / CPR E 430, or equivalent.

References

- Levente Buttyan (BME) and Jean-Pierre Hubaux (EPFL), Security and Cooperation in Wireless Networks, Cambridge University, 2007
- Research articles

Grading

- The tentative grade weighting for the semester will be:
  - Class Participation: 10%
    - Through randomized in-class questions; for students in the online section, answers to the in-class questions are due within one week of the class through Canvas.
  - Quizzes: 45%
    - Via Canvas; for students in the online section, quizzes are due within one week after the they are given in class.
  - Projects: 45% (or 35% if paper presentation)
  - Paper presentation: 10% (if time permits)
- Letter grades will be assigned based on performance relative to other students. A tentative grading scale is as follows:

  93 – 100 = A
  90 – 92.99 = A-
  87 – 89.99 = B+
  83 – 86.99 = B
  80 – 82.99 = B-
  77 – 79.99 = C+
  73 – 76.99 = C
  70 – 72.99 = C-
  67 – 69.99 = D+
  63 – 66.99 = D
  60 – 62.99 = D-
  0 – 59.99 = F

Miscellaneous

Iowa State University is committed to assuring that all educational activities are free from discrimination and harassment based on disability status. Students requesting accommodations for a documented disability are required to work directly with staff in Student Accessibility Services (SAS) to establish eligibility and learn about related processes before accommodations will be identified. After eligibility is established, SAS staff will create and issue a Notification Letter for each course listing approved reasonable accommodations. This document will be made available to the student and instructor either electronically or in hard-copy every semester. Students and instructors are encouraged to review contents of the Notification Letters as early in the semester as possible to identify a specific, timely plan to deliver/receive the indicated accommodations. Reasonable accommodations are not retroactive in nature and are not intended to be an unfair advantage. Additional information or assistance is available online at www.sas.dso.iastate.edu, by contacting SAS staff by email at accessibility@iastate.edu, or by

calling 515-294-7220. Student Accessibility Services is a unit in the Dean of Students Office located at 1076 Student Services Building.