CSE 707: Seminar: Wireless Networks Security – Principles and Practices

Fall 2023

Lecture Hours: Wednesdays 10:00 am - 12:50 pm, Davis 113A
Instructor and E-mail address: Dr. Shambhu Upadhyaya; shambhu@buffalo.edu
Office Hours: Wednesdays 8:30 am – 9:55 am

Educational Resources:

- Textbook: None
- Recommended Books: None
- Additional Resources: Papers from Journals and Conferences

Course Description:

The course includes several instructor presentations and student presentations. Further, students can investigate research problems or engage in simulation based experiments.

Topics included are: Overview of Security Issues in Wireless Networks, WEP Security, WPA and RSN, Security of MANETs, Security of Sensor Networks, Wireless Mesh Networks and Security, Trust in Wireless Networks, Vehicular Networks Security, Smart Grid Security and Security of Internet of Things (IoT).

Rationale:

Wireless networking/computing is now very popular. However due to power, size and bandwidth limitations, the network and security management of wireless nodes has become fragile. As a starting point, wireless networks have adopted many security mechanisms from the wired world. But due to the inherent limitations, they are more vulnerable to attacks than the wired network. Threats like intercepting and unauthorized access to wireless traffic are prevalent these days. More mature solutions to the security problems demand the need for an understanding of the current technologies and the security flaws.

Expanded Description:

The seminar will start with a sweeping overview of Wireless Networking, Security issues in Wireless Networks and the Challenges, Threats and Hacking

Methodologies. We will then cover Routing Security in Mobile Ad hoc Networks, Sensor Networks Security (Attacks and Countermeasures), Robust Localization in Sensor Networks, Security in Wireless Mesh Networks, QoS-Aware MAC Protocols and their security implications. We will also look into Vehicular Networks Security, Smart Grid Security, Security of Internet of Things (IoT), and Trustworthy AI in Wireless Networks, depending upon the student interests and time.

Student Background/Prerequisites:

A course on Computer Networks and basic knowledge of computer security. Some programming experience is essential.

Course Organization and Projects:

Most of the topics will be from research papers and Internet documents. Topics will be assigned to or selected by students who are required to study them, prepare presentations and discuss and critique them in class.

Week-by-week Schedule:

Week	Lecture
Weeks 1-4	Instructor presentations
Weeks 5-14	Student presentations
Week 15	Research round table discussion

Grading Policy:

Grading will be based on the presentations and research work or simulation projects. Attendance will also be a factor. S/U grades will be assigned for seminar courses.

Course Learning Outcomes (CLO):

Upon successful completion of this course, students will be able to:

1. Analyze the security posture of emerging wireless applications
2. Evaluate attack mitigation techniques and determine implementation methodologies
3. Critique state-of-the-art research in wireless networks security and orally present technical solutions and communicate related ethical issues of security

CLO Mapping to Program level learning objectives (PLO) and CLO Assessment Scheme:

PLO	CLO	Inst. Presentations	Student Presentations	Round table
2	1	x		
2	2		x	
4	3		x	x

This course satisfies one of the core requirements of the Advanced Certificate in Cybersecurity whose PLOs are:

1. Identify and apply the principles, methods, and practices of cybersecurity in multiple domains, including operating systems, networks, and software
2. Identify and evaluate cybersecurity risks and develop and implement appropriate solutions for those risks
3. Use penetration testing tools to identify potential weaknesses and use security hardening tools to address known weaknesses
4. Effectively recognize and communicate potential ethical issues related to cybersecurity systems, solutions, and technology to both technical and non-technical audiences

Accommodation Statement:

No particular product will be used in this class to complete assignments or access educational content. However, you may note that the University at Buffalo is committed to ensuring digital accessibility for people with disabilities. We are continually improving the user experience for everyone and applying the relevant accessibility standards to ensure we provide equal access to all users. If you experience any difficulty in accessing the content or services on any product you may use in this regard, we will provide an alternative means of access to the information and services presented through such products. To request assistance or provide suggestions about improving the user experience, please contact cse-consult via email (cse-consult@buffalo.edu) or phone (716-645-4744).

Academic Integrity:

The value of our courses, grades, degrees and research findings are dependent upon adherence to standards of ethical conduct. Plagiarism and inappropriate collaboration will not be tolerated. In this course we will adhere to the departmental standard for academic integrity. For more details, refer to the class webpage.