Spring 2017

Lecture Hours: Mondays 4:00 pm - 6:00 pm (113A Davis)
Instructor and E-mail address: Dr. Shambhu Upadhyaya; shambhu@buffalo.edu
Office Hours: Mondays 9:30 am – 11:00 am

Text Book and Recommended Books:

- None.

Course Description:
The course includes several instructor presentations and student presentations. Further, students can investigate research problems or engage in projects - simulation based or hands-on experiments.


Rationale: Wireless networking/computing is becoming increasingly 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, Trust issues in MANETs, and QoS-Aware MAC Protocols and their security implications. We will also look into Vehicular Networks Security, Smart Grid Security and Security of Internet of Things (IoT), depending upon the student interests and time.

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 the class. The Wireless Networks Security lab in 301C Davis could be used to perform certain security experiments.

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

Grading Policy:
Grading will be based on the presentations and research work or experimental projects. Attendance will also be a factor. S/U grades will be assigned unless prior arrangement is made for letter grades.

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.