ECE 547/647 Security Engineering

Syllabus, Spring 2020

Course Meetings: Tuesday and Thursday, 11:30am-12:45pm, room: Marston 211

Instructor: Wayne Burleson, Electrical and Computer Engineering
Contact: burleson@umass.edu , Office: Knowles 309B
Office Hours: Tues/Thurs 1pm-2pm (tentative)
Teaching Assistant: Jackie Lagasse

Course Description:

This course surveys recent advances in Security Engineering, and provides examples drawn from recent research at UMASS and elsewhere. Security Engineering is a multi-disciplinary field combining technical aspects of Applied Cryptography, Computer Engineering, and Networking as well as issues from Psychology, Sociology, Policy and Economics. Several guest lectures will be presented by experts in these disciplines. The graduate version 647 will involve a more extensive and sophisticated project while the undergraduate version 547 will be more of a survey course with an implementation project.

Optional Text:

Ross Anderson, Security Engineering - A Guide to Building Dependable Distributed Systems , 3rd edition, 2019. Most chapters are available free on-line. Also see the author's web-site: http://www.cl.cam.ac.uk/~rja14/ . The text will be supplemented with papers drawn from the literature.

Pre-requisites:

547 students should be juniors or seniors who have taken ECE 371 Introduction to Security Engineering. 647 students should be graduate students with some background in cryptography and system security. Other seniors or graduate students in either Electrical and Computer Engineering or Computer Science should contact the instructor.

Grading:

Exam, quizzes and homework on topics covered in first portion of course 40%
Presentation/Report from the Literature 30%
Project 30%

Selected Topics:

- **Technical engineering basics** — Review of Security Engineering (ECE 371)
- **Hardware Security**: TRNG, PUF, Side-channels, Row-hammer,
- **CPU Security**: Meltdown/Spectre, ARM. RISC-V
- **Block Chain and Cryptocurrencies**: Implementations, Vulnerabilities, Societal Impacts

- **Embedded and IoT Security**: Applications: Smart home, medical, automotive, drone,…
- **Human Factors**: passwords
- **ML Security**: adversarial ML

These technical areas will be studied in the context of a research survey and project:

- How to explore, read, critique, present and extend a wide variety of **research literature** in security engineering and related fields.
- How to plan, execute and report a small **research or implementation project**

March - **Student Presentations:** Groups of 4 students as 2 teams of 2 will make a ½ hour presentation of 2-3 papers on an important topic in Security Engineering. Papers should be summarized, critiqued, compared and suggestions made for improvement and extension. Topics can be drawn from the extensive bibliography in the textbook as well as recent research at UMass and elsewhere. It is expected that this presentation will lead into your project. Depending on the enrollment of the course, this should take about 3-4 weeks with 2 presentations per class period. All students are expected to attend all presentations, read all of the papers in advance, and actively participate in the discussion. This is part of the presentation grade.

April **- Projects:** Groups of 4 students as 2 teams of 2 will build on the presentation. Projects will probably involve one of the following: 1) simulation, 2) implementation, 3) comparison, 4) vulnerability analysis. Projects should also consider at least one multi-disciplinary aspect such as Psychology, Economics, Policy, Ethics, etc. Project ideas should be discussed with the instructor and written 5 page proposals will be due in early April. Final project reports will be due at the end of the semester. A typical project might design an implementation of a cryptosystem and analysis of its vulnerabilities across a wide spectrum. Another possible project could be a study of threat models in a particular application domain and recommendations for protection mechanisms including economic implications. These are just examples. I am open to your ideas and welcome discussion early in the semester.