ECE 597AB/697AB Security Engineering

Syllabus, Spring 2012

Course Meetings: Tuesday and Thursday 1pm-2:15pm, room ELAB 327
Instructor: Wayne Burleson, Electrical and Computer Engineering
Contact: burleson@ecs.umass.edu , Office: Knowles 309C, Office Hours: TBD
Course Description:

This course provides an introduction to the new area of 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 697AB will involve a more extensive and sophisticated project while the undergraduate version 597AB will be more of a survey course with an implementation project.

Text:

Ross Anderson, Security Engineering - A Guide to Building Dependable Distributed Systems , 2nd edition, 2008. Strongly consider paying the extra $14 and getting the on-line version as well. Note that the first edition is also useful and is available free on-line. The text will be supplemented with papers drawn from the literature.

Pre-requisites:

Students should be seniors or graduate students in either Electrical and Computer Engineering or Computer Science. Other students should contact the instructor.

Grading:

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

Selected Topics:

- **Technical engineering basics** — cryptography, protocols, access controls, cryptography hardware and software implementations.
- **Types of attack** — web exploits, card fraud, hardware hacks, electronic warfare , tampering, side-channels, malicious hardware
- **Specialized protection mechanisms** — biometrics, seals, smartcards, RFID, alarms, and DRM, and how they fail
- **Security economics** — why companies build insecure systems, why it's tough to manage security projects, and how to cope

- **Security psychology** — the privacy dilemma, what makes security too hard to use, and why deception will keep increasing
- **Ethics** — vulnerability disclosure
- **Policy** — why governments waste money on security, why societies are vulnerable to terrorism, and what to do about it
- 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 **research project**

Early April - **Student Presentations:** 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 3-5 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.

Late April - Early May - **Projects:** Projects can be individual or small groups (2-3 students) and should 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 aspects 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.

Some project ideas:

- Implementation of a cryptosystem and analysis of its vulnerabilities across a wide spectrum
- Study of threat models in a particular application domain and recommendations for protection mechanisms including economic implications.

  See research ideas at the end of each textbook. e.g. here are some on p 61.

  - ❖ Are there any neat ways to combine things like Passwords, CAPTCHAs, images and games so as to provide sufficiently dependable two-way authentication between humans and computers?
  - ❖ Are there any ways of making middleperson attacks sufficiently harder that it doesn't matter if the Mafia owns your ISP?