

## **ECE 697AB Security Engineering**

### Spring 2010

**Course Meetings:** Tuesday and Thursday 1pm-2:15pm, room TBA

**Instructor:** Prof. Wayne Burleson, Electrical and Computer Engineering  
[burleson@ecs.umass.edu](mailto:burleson@ecs.umass.edu), Office: Knowles 309C

#### **Course Description:**

This graduate 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 by experts will allow students to appreciate a variety of perspectives on this exciting new field..

#### **Text:**

Ross Anderson, *Security Engineering*, 2<sup>nd</sup> edition, 2008 (note that the first edition is also useful and is available free on-line). The text will be supplemented with papers drawn from the technical and popular literature.

#### **Pre-requisites:**

Students will typically be seniors or graduate students in either Electrical and Computer Engineering or Computer Science. Other interested students should contact the instructor to see if they have the appropriate technical background.

#### **Grading:**

Exam on Security Engineering basics covered in first 1/3<sup>rd</sup> of course 30%  
Presentation/Report from the Literature 30%  
Project 40% (project typically involve programming, simulation or experiment)

#### **Selected Topics:**

- **Technical security 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