ECE 697AB „Security Engineering"

Spring 2013

Instructor: Georg T. Becker (becker@ecs.umass.edu)
Day & Time: Tuesday and Thursday 2:30pm-3:45pm

Course Description:
The course "Security Engineering" will provide an introduction to computer security and the challenges security engineers face. The first part will cover basic cryptographic concepts and protocols needed to understand most security systems. In the second part selected topics of security engineering will be discussed in more detail. Here a special focus is given to hardware security. Guest lecturers will give an overview of current research in security engineering in- and outside of UMass.

Text:
The first part of the lecture will be based on the book "Understanding Cryptography" by Christof Paar and Jan Pelzl. http://www.crypto-textbook.com/. Purchasing the book is not mandatory but recommended.

Pre-requisites:
You should be graduate students in either Electrical and Computer Engineering or Computer Science.

Grading:
The grading will be divided into a midterm (30%), a final (40%), homework (10%) and reviews (20%). In the second part of the lecture, you will have to make critical reviews of selected papers in security engineering. The reviews should include a brief summary of the paper, a short summery of related work and a critical comment describing the advantages and disadvantages of the paper.

Selected Topics:
- Block ciphers
- Stream ciphers
- Public key cryptography
- Security services and protocols
- Side-channel attacks
- Fault attacks
- Privacy protection
- Real-world attacks on embedded systems
- Hardware Trojans and IP protection
- Medical device security
- Chip & Pin is broken: The problem of backwards compatibility