Hardware Security -- Introduction

Cybersecurity Specialization

Cybersecurity Specialization

- Usable Security: J. Golbeck
- Software Security: M. Hicks
- Cryptography: J. Katz
- Hardware Security: G. Qu
- Capstone project
- Goal: provide students a broad and multidisciplinary perspective on current topics in cybersecurity.

Cybersecurity Specialization

- Provides the platform and support
- Needs SW, crypto, and usability in CAD tools and security solutions

Hardware Security: Coverage

- Hardware:
  - Integrated circuits (IC)
  - Field programmable gate arrays (FPGA)
  - Embedded systems
- Security
  - Vulnerabilities, threats, attacks from HW
  - HW design security
  - Hardware for security
    - Trusted IC, TPM, PUF, …

Course Organization

- 6 weeks, 3-5 hours of work per week
  - 1-1.5 hours of video clips (1.5-2.5 hours)
  - Weekly quizzes (1-2 hours)
  - (optional) readings (0-n hours)
- Background:
  - Digital logic design
  - Programming concepts
  - Finite state machine
  - Basic cryptography concepts

Course Objectives

Upon completion, you will be able to

- Understand the vulnerabilities and threats to a system from hardware (e.g. backdoor, hardware Trojan, counterfeiting) as well as the available countermeasures
- Perform a security evaluation for the hardware implementation of cryptographic primitives and security protocols
- Analyze and assess the tradeoff among system performance, cost, and security

Course Objectives

Upon completion, you will be able to

- Design and build ICs and embedded systems with enhanced security and trust (e.g. harden the design to avoid known vulnerabilities)
- Learn hardware security primitives (e.g. TPM, PUF, TRNG) and employ them for secure system design
- Know how to use self-protection methods (e.g. watermarking, fingerprinting, IC metering) to protect your IPs (in addition to patent, copyright, and other law enforcements)

Cybersecurity Specialization

Good luck and enjoy learning!