ENG EC500 D1 Hardware Security - Spring 2020
Instructor Prof. Michel Kinsy

Course description

Hardware security sits at the intersection of cryptographic engineering and hardware design. It includes hardware-root-of-trust design techniques, access control, secure multi-party computation, code authenticity techniques, secure key storage, secure execution, side-channel analysis, obfuscation methods, and IC supply chain risks.

The course introduces students to hardware approaches to cybersecurity. Through lectures, reading assignments and projects, students will gain in-depth knowledge of the role that hardware plays in cybersecurity and computer hardware related attacks and defense in computing systems.

Topics covered are: (i) computing systems security requirements: integrity and authentication, among others; (ii) core security techniques: encryption algorithms, key distribution and management; (iii) hardware attacks: hardware Trojans, side-channel attacks, fault attacks, hardware counterfeiting; (iv) trusted hardware primitives: trusted digital system design, circuit obfuscation, trust platform modules, physical unclonable functions, true random number generators; and (v) secure embedded and mobile devices. Student will be introduced to major secure processor architectures or features such as Intel's Software Guard Extensions (SGX) and Trusted Execution Technology (TXT), ARM TrustZone Technology and derived processor architectures, MIT Aegis Secure Processor and Sanctum, Apple Secure Enclave Processor (SEP), Keystone, CHERI, and BU Hermes and Sphinx Architectures.

Project

The class project consists of building secure multi-core RISC-V ISA architecture. Using an out-of-order RISC-V processor template, students examine micro-architecture side-channel vulnerabilities, defenses, and trusted execution extensions and micro-architecture modifications.

Objectives

The course will enhance students' preparation to identify, understand and potential propose hardware-as-root-of-trust solutions for the most pressing cyber security problems. Upon successful completion of this course, students will be able to:

- distinguish between software and hardware security;
- identify the sources and manifestations of hardware-centric cyber threats;
- understand the potential of information leakage at microprocessors, memories and memory organizations, and on-chip networks levels;
- categorize hardware security solutions;
- evaluate computing system in terms of performance, reliability, and security;
- effectively assess new hardware security approaches.

Textbook (No Textbook Required)

M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer, 2011 (Recommended)

Recommended Background Courses

- ENG EC 311: Introduction to Logic Design
- ENG EC 327: Introduction to Software Engineering
- ENG EC 413: Computer Organization