ECE 525: Hardware-Oriented Security and Trust

Catalog description: A knowledge-based economy depends extensively on electronic information and control. In mainstream information technology, the authenticity, integrity and confidentiality of this information is protected with secure and trustworthy protocols in software. However, secure information technology has now progressed well beyond the boundaries of traditional computing. Networks of embedded computers are controlling critical infrastructures such as water, food, manufacturing, transportation and medical systems. Trustworthy platforms are essential in a multitude of commercial and financial applications. This turns counterfeiting, intellectual property theft and subversion of trustworthiness into a lucrative activity, threatening both hardware and software. In contrast to software, where security risks are better understood, addressing the threat to the hardware platform remains an open challenge. The overarching importance of this topic led to several national publications and programs authored by Senator Joe Lieberman [1], DARPA [2][3] and the National Academy of Engineering [4].

This course investigates recent technology developments for the design and evaluation of secure and trustworthy hardware. Hardware security and trust techniques are required to ensure that chips remains secure and trustworthy during its entire lifecycle from design to manufacturing, deployment, service and retirement. The following topics are covered in this course as well as their application to the Internet-of-Things (IoT), autonomous cars, smart homes, smart grid, factory automation, smart infrastructure and cloud computing.

- Hardware security primitives, including Physical Unclonable Functions (PUFs), are investigated that are capable of generating unique, unclonable chip identifiers and secret bitstrings. Internal chip-generated secrets can be used to detect counterfeiting, for implementing intellectual property licensing and metering schemes, and to provide a root-of-trust for secure boot and for authentication and encryption between Internet-of-Things (IoT) devices.
- Techniques are discussed that are designed to detect Hardware Trojans inserted by adversaries to provide 'back-doors' and 'kill switches' in chips.
- Circuit design techniques are investigated that can protect chips against unauthorized extraction of private information within chips using Side-Channel attacks.
- Circuit obfuscation methods are discussed that prevent black-market cloning, reverse engineering and intellectual property theft.

Recommended course prerequisite: C programming, HDL, statistics, VLSI
Level: Graduate
Credits: 3

[1] Senator Joe Lieberman, "National Security Aspects of the Global Migration of the U.S. Semiconductor Industry," http://lieberman.senate.gov/documents/whitepapers/semiconductor.pdf, June 2003.
[2] http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf
[3] http://www.darpa.mil/mto/solicitations/baa07-24/index.html
[4] "Grand Challenges for Engineering", http://www.engineeringchallenges.org/cms/8996/9042.aspx