ELE 594: Special Topics on Hardware Security and Trust

***Class Hours*:** Tu,Th 12:30PM - 1:45PM

***Location*:** Swan Hall room 213

***Academic Term*:** Fall 2020

Instructor:

Name: Yu Bi, Ph.D.
Email: yu_bi@uri.edu
Telephone: (401)874-5846
Office Hour: Tu/Th 2-4 pm Fascitelli 410

Course Description:

Trust in hardware is the fundamental aspect to establish a secure cyber/information infrastructure. This course will investigate recent technology developments for the design and evaluation of secure and trustworthy hardware. Hardware security generally includes hardware-root-of-trust design techniques, secure key storage, secure execution, side-channel analysis, obfuscation methods, and IC supply chain risks. This course highlights the challenges arising from the end of Moore's law as well as the rapid evolution of attackers. 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 large-scale computing systems.

***Course Pre-requisite*:**

- Undergraduate classes in digital or analog circuit design;
- Students familiar with the coding skills such as C/C++, Python and Verilog.

Course Objectives:

This graduate-level course intends to help students:

- Familiarize themselves with the state-of-the-art in hardware security – hardware Trojan attacks and prevention, physical unclonable functions (PUFs), electronics counterfeit prevention, side-channel analysis etc. through lectures, student-led presentations, and literature surveys;
- Understand important and emerging hardware security topics such as hardware obfuscation, logic locking, split manufacturing, circuit camouflaging, IP encryption, security design rules, information flow tracking, and more through lectures, literature reviews, and labs/projects;

- Perform a literature survey and discuss emerging topic areas associated with security challenges and opportunities of nanoscale devices (memristor, magnetic memory, graphene, etc.), 2.5D/3D integration, Internet of Things (IoT), analog and mixed signal ICs, and FPGAs;
- Explore the emerging new hardware security opportunities and challenges, such as RowHammer, AI adversarial examples, BFA on AI inference etc.

***Grading*:**

The final grade will be computed as a weighted average of **Mid-term Exam** (30%), **Student Presentation** (30%) and **Final Project and Demo** (40%).

***Exam*:**
Mid-term Exam: Th 10-29-20, 12:30-13:45 am, 3-page summary

***Project**:*

- Individual or a group of max two students;
- Experiment might require hardware component (e.g FPGA);
- Project should be presented and video recorded.

***Textbook (Not Required)*:**

- P, Mishar, S. Bhunia, and M. Tehranipoor, "Hardware IP Security and Trust", Springer, 2016.
- M. Tehranipoor and C. Wang, "Introduction to Hardware Security and Trust", Springer, 2011

***Additional Materials*:**

- Collections of papers and reports will be distributed through the course
- Tools and benchmarks: https://trust-hub.org/
- Opencores: https://opencores.org/