ITPF UCF Course for 2015 Fall
EEE 4346C - Hardware Security and Trusted Circuit Design

Dr. Yier Jin
Department of Electrical Engineering and Computer Science
University of Central Florida
Phone: 407-823-5321
Email: yier.jin@eecs.ucf.edu

Office Hours:

- TBD

Lectures:

- Time: TBD Room: TBD

Textbooks: (recommended)

- *Introduction to Hardware Security and Trust*, Edited by M. Tehranipoor and C. Wang, September 2011, Springer, ISBN-13: 978-1441980793
- *Digital VLSI Design with Verilog: A Textbook from Silicon Valley Technical Institute*, by John Williams and Don Thomas, August 2008, Springer, ISBN-13: 978-1402084454

Prerequisites:

- EEL 3801C – Computer Organization or C.I.

Course Objective:

The purpose of this course is to introduce a newly emerged area, trusted integrated circuits and prepare students for challenges in the field of **hardware security**. The concept and taxonomy of hardware Trojans will be introduced as well as their malicious impact to both critical and commercial device. Considering the fact that cryptographic embedded systems are often the target of hardware Trojans, cryptographic embedded systems and their vulnerabilities when attacked by hardware Trojans will also be discussed in the course.

The course will also prepare students for the Embedded System Challenge in Cybersecurity Awareness Week (CSAW) hosted by NYU-Poly every November. Therefore, the objective of the course are (1) to give students the idea of hardware security: identify the vulnerabilities of circuit designs, (2) to understand the principles of hardware Trojan detection methods and propose new detection methods to ensure the trustworthiness of the integrated circuits, and (3) to prepare students for the challenge of embedded system security. **Proposed circuit trust evaluation methods will be simulated based on commercial EDA tools.**

Lecture Topics:

1. Introduction to hardware security
2. Introduction to cryptographic embedded systems
3. Security issues in processors and microprocessors
4. A review of hardware Trojan detection methods
5. Fault attacks and countermeasures
6. Design of Physical Unclonable Function (PUF)

7. Advanced topics in hardware security
    a. IP protection, e.g., logic encryption, design obfuscation, split manufacturing
    b. IC overproduction prevention, e.g., hardware metering
    c. Counterfeiting chips detection and prevention

Lab work/Homework:

Note: For students who take the course remotely through the ITPF program, lab equipment will be provided by the course instructor and the report will be turned in through emails.

Lab/HW 1: Hardware Trojan Design in AES Crypto-System (CSAW 2008 ESC)

Lab/HW 2: Hardware Security Primitive - PUF Designs (CSAW 2011 ESC - Part II)

Lab/HW 3: Vulnerabilities of Computing Platforms (CSAW 2011 ESC - Part I)

Lab/HW 4: Hardware Trojan Detection in FPGA Bit Files (CSAW 2012 ESC)

Lab Hours:

- TBD (No dedicated lab hours for students taking the class remotely)

Grading:

- Exams (30%)
    - Midterm (10%)
    - Final Exam / Presentation (20%)
- Homework/Projects (50%)
- Final Project/Final Report (20%)

Anyone who wins an award from CSAW, any of its competitions, will get an 'A' automatically for this course. What are you waiting for?