ECE 4095 Spring 2013
Trustable Computing Systems
Wed 11-12, Fri 10-1

Course Description: *Three Credits. Prerequisite: CSE 2300 and ECE 2001W; ECE 3401 which may be taken concurrently.* An introduction to trustable computing and hardware security. Course will include hands-on approaches to hardware security attacks. Topics include side channel attacks, differential power analysis, hardware Trojans, acoustic analysis, EM logging, and DRAM data remenance.

Instructors:

John A. Chandy	Zhijie Shi	Mohammad Tehranipoor
ITEB 437	ITEB 365	ITEB 441
(860) 486-5047	860-486-0599	860-486-3471
john.chandy@uconn.edu	zshi@engr.uconn.edu	tehrani@engr.uconn.edu

Website: HuskyCT

Grading Policy:

Project Assignments	75%
Homeworks	25%

Tentative Schedule:

Week	Date	Wednesday 11-12	Friday 10-1 (Lab)
1	1/23-25	Hardware Security Introduction, Ethics, Hacking (Chandy)	No Lab
2	1/30-2/1	Hard Disk Attacks (Chandy)	Hard Disk Attacks
3	2/6-8	Acoustic Analysis (Chandy)	Acoustic Analysis
4	2/13-15	Cryptographic Algorithm Implementations (Shi)	No Lab
5	2/20-22	Introduction to Side Channel Attacks (Shi)	Side Channel Attacks
6	2/27-3/1	No Lecture	Side Channel Attacks
7	2/6-3/8	Side Channel Attacks 2 (Shi)	Side Channel Attacks
8	3/13-15	No Lecture	Side Channel Attacks
9	3/27-29	Data Remenance (Chandy)	Data Remenance
10	4/3-5	Hardware Trojans: IC Design Flow, Hardware Trojan Examples, and Taxonomy (Tehranipoor)	Hardware Trojans
11	4/10-12	No Lecture	Hardware Trojans
12	4/17-19	Hardware Trojans: FPGA Design Flow and Trojan Insertion (Tehranipoor)	Hardware Trojans
13	4/24-26	No Lecture	Hardware Trojans
14	5/1-3	TBA	TBA

Each project module will consist of an opening lecture that gives the background science behind the project and introduces new measurement or lab techniques. The student will then work on a

a hands-on project that will focus on a particular type of hardware attack. The module will then end with a student-focused discussion session where students deliberate the ethical impacts as well as do a post-mortem analysis and brainstorm on new attack strategies as well as potential countermeasures.