ECE 5960 - Hardware and Embedded System Security
(Syllabus adapted from Dr. Ryan M. Gerdes' Course)

Spring 2017

Class:	ENGR 104 MWF 11:30 am - 12:20 pm
Instructor:	Nathanael Weidler nweidler@gmail.com
Office Hours:	Please email me or speak to me after class
Teaching Assistant:	Danny Froerer dkfroerer@gmail.com (In charge of all homeworks)
Course Website:	Canvas

Text: Introduction to Hardware Security and Trust, Tehranipoor, Mohammad; Wang, Cliff (Eds.), ISBN 1441980792 (available online).

Requisites: (Pre-) ECE 3710 – Microcontrollers and (Co-) ECE 3410 – Microelectronics I; permission from instructor

Course Description: A senior/graduate-level course that focuses on the application of security thinking to analyse threats to embedded systems originating from, and solutions based on, hardware and the physical layer. Topics to be covered include hardware trojans (creation and detection); cryptographic hashing (optimized hardware and software implementations); stack-based attacks against embedded systems (code injection and return-oriented programming); side-channel attacks; physically unclonable functions (authentication and true random number generators); identification of devices based on physical characteristics; and fault-injection attacks.

Course Objectives: At the conclusion of this course, students are expected to be able to
• apply fundamental security tools, processes, ideas, and thinking to the analysis and design of systems;
• build and debug software and hardware implementations of various hashing and crypto systems;
• explain and carry out stack-based attacks and be knowledgeable of hardware techniques to frustrate such attacks;
• be familiar with common side-channel analysis techniques and carry out such attacks on embedded system/special-purpose crypto devices;
• make use of physical properties of devices/systems and the physical layer for such purposes as identification, authentication, and true random number generation; and
• create malicious logic/hardware trojans and be familiar with their detection.

IDEA Objectives: The instructor has selected the following objectives for the students end-of-the
semester, online assessment
• Learning to analyze and critically evaluate ideas, arguments, and points of view;
• Learning to apply course material (to improve thinking, problem solving, and decisions); and
• Learning fundamental principles, generalizations, or theories.
Lectures: Lectures will cover the most important and difficult parts of the course material. Students are expected to read relevant papers/chapters prior to lecture; readings will be provided in preceding lectures. As this is an upper-level course in a new area, most material can not be found
in textbooks. It is expected that most students will not have been exposed to research literature or used it to acquire new knowledge. Thus, the lecture will attempt to bridge the gap between the
pedagogical material the students are used to and the papers they are expected to read. There may be any number of unannounced quizzes during the semester.

Lectures: Lectures will cover the most important and difficult parts of the course material. Students are expected to read relevant papers/chapters prior to lecture; readings will be provided in preceding lectures. As this is an upper-level course in a new area, most material can not be found in textbooks. It is expected that most students will not have been exposed to research literature or used it to acquire new knowledge. Thus, the lecture will attempt to bridge the gap between the pedagogical material the students are used to and the papers they are expected to read. There may be any number of unannounced quizzes during the semester.

Each Student will have an opportunity, with their partner, to present materials from at least one paper to the class.

Grading:

Paper Presentations	10%
Final Presentations	10%
Projects	80%

Projects: Students must complete five projects of equal weight over the course of the semester. Each project will involve some combination of coding, mathematics, data analysis, and demonstration. In addition, each student will be required to give a class presentation summarising their project solution at least once in the semester (likely for the final project.) The projects will be selected from
• a software and hardware implementation of MD5 (ECE 5760) or SHA-1 (ECE 6760);
• the recovery of an encryption key through side-channel analysis of ASIC/FPGA implementations of DES (ECE 5760) or AES (ECE 6760);
• the demonstration of a stack-based attack against Cortex-M3/4-based (or similar) microcontroller without stack protection (ECE 5760) and with stack protection (ECE 6760);
• an implementation of PUF-based system for authentication or true random number generation

(ECE 5760) or secret key generation (ECE 6760);
• the design and implementation of a hardware trojan for malicious processor/microcontroller/system
(ECE 6760 students will need to implement the trojan in a fully functioning system).

Project requirements: Students will work individually or in groups of two—though they are encouraged to engage in discussion and problem solving in larger numbers. Work is to be submitted
on Canvas by the date specified. Project reports should have an introduction, body, and conclusion,
with references if necessary. Code must be commented and can be attached as a separate file. The
report must
• be typed on 8.5 × 11 inch paper (LATEXrecommended);
• be neat and easily followed;
• include appropriate derivations or steps taken to arrive at the answers;
• include your name, project number, and course number on the first page;

Additional requirements for ECE 6760 Students taking the course as ECE 6760 will analyse/implement more sophisticated/modern algorithms and techniques, as noted in the Projects section, and their reports will need to be of conference quality.

Grades: Your grade will be calculated using the following scale.

90–100	A
87–89	B+
83–86	B
80–82	B-
77–79	C+
73–76	C
70–72	C-
67–69	D+
63–66	D
60–62	D-
0–59	F

Note that students are independently evaluated and do not compete against each other.

Honor Pledge: Students will be held accountable to the Honor Pledge which they have agreed to: I pledge, on my honor, to conduct myself with the foremost level of academic integrity.
Academic Dishonesty: The Instructor of this course will take appropriate actions in response to Academic Dishonesty, as defined the University's Student Code. Acts of academic dishonesty include but are not limited to
1. Cheating:

(a) using or attempting to use or providing others with any unauthorized assistance in taking quizzes, tests, examinations, or in any other academic exercise or activity, including working in a group when the instructor has designated that the quiz, test, examination, or any other academic exercise or activity be done individually;
(b) depending on the aid of sources beyond those authorized by the instructor in writing papers, preparing reports, solving problems, or carrying out other assignments;
(c) substituting for another student, or permitting another student to substitute for oneself, in taking an examination or preparing academic work;
(d) acquiring tests or other academic material belonging to a faculty member, staff member, or another student without express permission;
(e) continuing to write after time has been called on a quiz, test, examination, or any other academic exercise or activity;
(f) submitting substantially the same work for credit in more than one class, except with prior approval of the instructor; or
(g) engaging in any form of research fraud.

2. Falsification: altering or fabricating any information or citation in an academic exercise or Activity.

3. Plagiarism: representing, by paraphrase or direct quotation, the published or unpublished work of another person as one's own in any academic exercise or activity without full and clear acknowledgment. It also includes using materials prepared by another person or by an agency engaged in the sale of term papers or other academic materials.

Outside Help: The College of Engineering has an Engineering Tutoring Center. Tutoring services are available free of charge to all College of Engineering students. You can find help for any engineering required courses, i.e. math, chemistry, physics, and all engineering classes. The Tutoring Center is located in ENGR 322 and 324. Hours are Monday through Friday 8:00 AM to 5:00 PM with extended hours on Tuesday and Thursday until 7:00 PM.

Students with Disabilities: Students with ADA-documented physical, sensory, emotional or medical impairments may be eligible for reasonable accommodations. Veterans may also be eligible for services. All accommodations are coordinated through the Disability Resource Center (DRC) in Room 101 of the University Inn, (435)797-2444 voice, (435)797-0740 TTY, (435)797-2444 VP, or toll free at 1-800-259-2966. Please contact the DRC as early in the semester as possible. Alternate format materials (Braille, large print or digital) are available with advanced notice.