## EECS498–009/598: Embedded Security

**Instructor:** **Kevin Fu**

**Summary** This course will teach students advanced methods to model, measure, and protect the security of embedded systems and the Internet of Things (IoT). The course will have a particular focus on the interface between hardware and software and the physics of computation. Included in the IoT security topic is a deep dive on security of Operational Technology (OT) such as found in high-assurance factory floors, and Microelectrical Mechanical Systems (MEMS) technology common in IoT, automotive, medical, RFID, and satellites. Hands-on lab exercises will involve frequency-domain analysis of signals, voice recognition system integrity and authenticity, acoustics both audible and ultrasonic, radio waves and modulation, and laser fault injection of semiconductors. The semester will culminate with a group project and demonstrations. Short essays will give individual students the opportunity to explore the application of the new skills and methods to design secure implantable medical devices, automobiles, and smartphones. Students will be required to complete safety training and will gain comfort with working in a maker space. By the end of the course, students will become comfortable safely creating signals with acoustics, radios, and lasers to test the security of embedded systems.

**Credits:** **4 + ULCE MDE**

**Prerequisites:** **EECS216 and EECS370, or permission of instructor.**
**EECS373 is recommended/advisory, but not required.**

**Lectures:** **1005Dow, Mondays and Wednesdays, 10:30-12**
**(some lectures will be replaced with in-lab time and proposal presentations)**

**Lab:** **There will be 3 sections of labs with nine oscilloscopes per section. There will be some flexibility on swapping between labs unofficially, with seating priority for the officially registered students in each section. Lab times will be announced in April, and we expect enough time slots such that every student will find at least one section fitting their class schedules.**

**Calendar** **iCal feed**

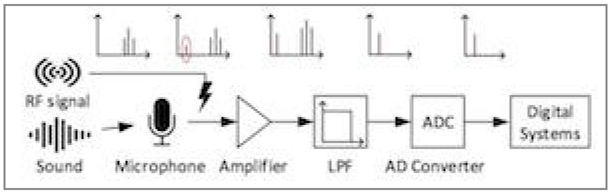
**GSI:** **Yan Long (yanlong@umich.edu)**
**Office hours:**
**Room Number: 4918 in the BBB**

**Forum:** **We use Piazza for online discussion and announcements. For administrative issues, use Piazza's private messaging function. For non-urgent matters, the course staff can be reached at TBD.**

**Resources**
**Cryptographic Hardware and Embedded Security (CHES) Workshop**
**USENIX Security**
**IEEE Security and Privacy (Oakland)**
**ACM CCS**
**Writing with Sources: A Guide for Students, 3rd Edition by Gordon Harvey**
**The Mayfield Handbook of Technical and Scientific Writing**
**Art of Electronics, 3rd Edition by Horowitz and Hill**
**AARL Handbook**

# Prereqs and Wait List

**This is a course designed primarily for upper-level undergraduates and graduate students in CE. To be considered for the wait list, please send to the emsec-staff@umich.edu email list information about your student status, degree program (e.g., CE major, CSE PhD, EE major, etc.). Having experience in computer engineering or electronics may give you a time advantage on the lab homework, but we will teach students how to use basic benchtop electronics equipment in the first weeks.**

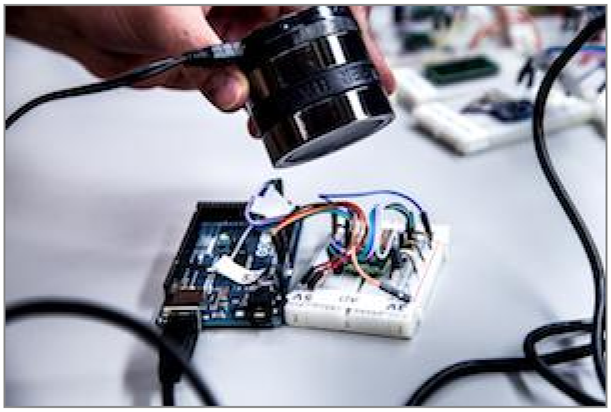


# Preliminary Topic List

**The tentative list of topics below should give you an idea of what to expect.**

**Full schedule here:**
**https://docs.google.com/document/d/1mHbZQM6rw9a_yu1NVkg2dzEXuee1m7N2wC7k6g_1ILA/edit?usp=sharing**

## Part 1: Building Blocks



**Threat modeling based on physics, principles of information security and privacy, risk, research ethics**
**Foundations: Science of Security**
**Lab: Intro to oscilloscopes, Fourier transforms, function generators, software radios**

## Part 2: Embedded Security

**Side channels, spectral analysis, timing attacks, power analysis, data remanence**
**Applications: Smartcards, RFID, IoT**
**Lab: Side channel analysis of cryptographic hardware**

## Part 3: Sensor Security

**Physics of security, transducers, MEMS, audible and ultrasonic acoustics, RF, optics**
**Applications: Medical devices, autonomous vehicles, satellites**
**Lab: Fault injection attacks and intentional interference against analog sensors**

## Part 4: Internet of Things (IoT) & Operational Technology (OT)

**Factory floors, robotics, advanced manufacturing, medical devices, smart homes**

**Applications: How to protect the security of factory floors, how to secure a pacemaker**
**Lab: Group projects**

## Part 5: Machine Learning (ML)

**Embedded security for machine learning, voice recognition systems**
**Applications: Designing secure digital voice assistants, voice fingerprinting, secure object recognition**
**Lab: Group projects**

# Grading

**Your grade will be based on the following (tentative, subject to change until first day of class):**

Class Participation and Presentation (5%) — Each week, we will suggest supplementary technical reading associated with the core material. Each student will have the opportunity to sign up for either making one five-minute presentation on the reading during lecture, or writing up lecture notes on the instructor's lecture. The supplementary reading will often be timely or fun, with exciting avenues of embedded security curiosity. Students will also have the opportunity to participate in discussion in class and piazza.

Essays (15%) — We expect to issue four one-page writing assignments that apply principles of embedded security in complex real-world scenarios. The top essay will be specially recognized with commendation. For example, one essay will pertain to role playing as a federal regulator to issue a warning about a cancer radiation therapy device that is globally knocked offline by ransomware at all hospitals simultaneously.

Midterm (15%) — One midterm will take place during class in lieu of lecture.

Hands-on Labs (30%) — Working mostly in small teams, students will carry out three lab assignments pertaining to reproducing embedded security experiments that are linked with the reading assignments. Homeworks range from learning how to use an oscilloscope to simple power analysis to extracting cryptographic keys from a microcontroller to using sound waves to take control of an accelerometer. The first lab will be individual. All labs have an individual pre-lab component required before the in-person lab component may begin. The team sizes will depend on enrollment due to a limited number of electronic kits. Some labs will span multiple weeks divided into milestones.

Final Group Project (35%) — You will conduct an extended group project during the semester, with the goal of producing a demonstration on embedded security to protect a notional embedded system against one of three kinds of sensor attacks: acoustics, radio waves, or lasers. This work must be done in a small group of 3-4 students per MDE rules. Example projects: protecting a robot from laser control of its voice commands, protecting a car airbag from detonating from malicious acoustic injection, protecting a nano satellite magnetorquer from RF injection on the inertial measurement units for inclination control, protecting a laptop lithium-ion battery from RF interference on thermocouples causing a sudden thermal runaway. Final group project grading is broken down as follows:

3% draft proposal  
12% proposal  
5% milestone 1  
5% milestone 2  
60% final project status (works, etc.)  
15% final report and documentation

There is no final exam, instead there is a final project and demonstration

# Ethics, Law, and University Policies

To defend a system, you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy in EECS 588 is that you must respect the privacy and property rights of others at all times, or else you will fail the course.

Acting lawfully and ethically is your responsibility. Carefully read the Computer Fraud and Abuse Act(CFAA), a federal statute that broadly criminalizes computer intrusion. This is one of several laws that govern "hacking." Understand what the law prohibits — you don't want to end up like this guy. The EFF provides helpful advice on vulnerability reporting and other legal matters. If in doubt, we can refer you to an attorney.  
Please review ITS's policies on responsible use of technology resources and CAEN's policy documentsfor guidelines concerning proper use of information technology at U-M, as well as the Engineering Honor Code. As members of the university, you are required to abide by these policies.