

Embedded Security

EECE 5698-08: Special Topics:

Cyber-Physical Security of IoT Systems in the Age of AI

Lecture 1: Introduction
Prof. Kevin Fu

September 10, 2026
<https://spqrlab1.github.io/emsec/>



Northeastern University
College of Engineering



Today

- Welcome!
- Course mechanics
- Ethics
- How to read a research paper

Course Staff



Prof. Kevin Fu
ECE/Khoury/Bioengineering
MIT PhD, MEng, BS
kevinfu.com

Primary role:
Lectures



Hui Zhuang
Khoury PhD student
[zhuang-hui.github.io](https://github.com/zhuang-hui)

Primary role:
Research and lab development



Nuntipat (Palm) Narkthong
ECE PhD student
nuntipat.me

Primary role:
Open lab hours and grading

Learning Outcomes for A-Level Students

- Model and analyze security threats to embedded systems and IoT devices based on physical principles.
- Apply principles of security and privacy to evaluate risks in AI-in-the-loop systems.
- Use oscilloscopes, function generators, and software-defined radios for security experiments.
- Evaluate MEMS, RF, acoustic, and optical components against theoretical and experimental threats.
- Design secure embedded systems involving AI/ML components with attention to hardware-software co-design.

Primary Course Activities

Lectures: This.

Labs: Three hands-on labs with pre-lab requirements, focusing on side-channel and sensor security.

Final Group Project: Teams will conduct an extended project with demonstrations. In-class midterm, lecture scribing, pop quizzes, etc.

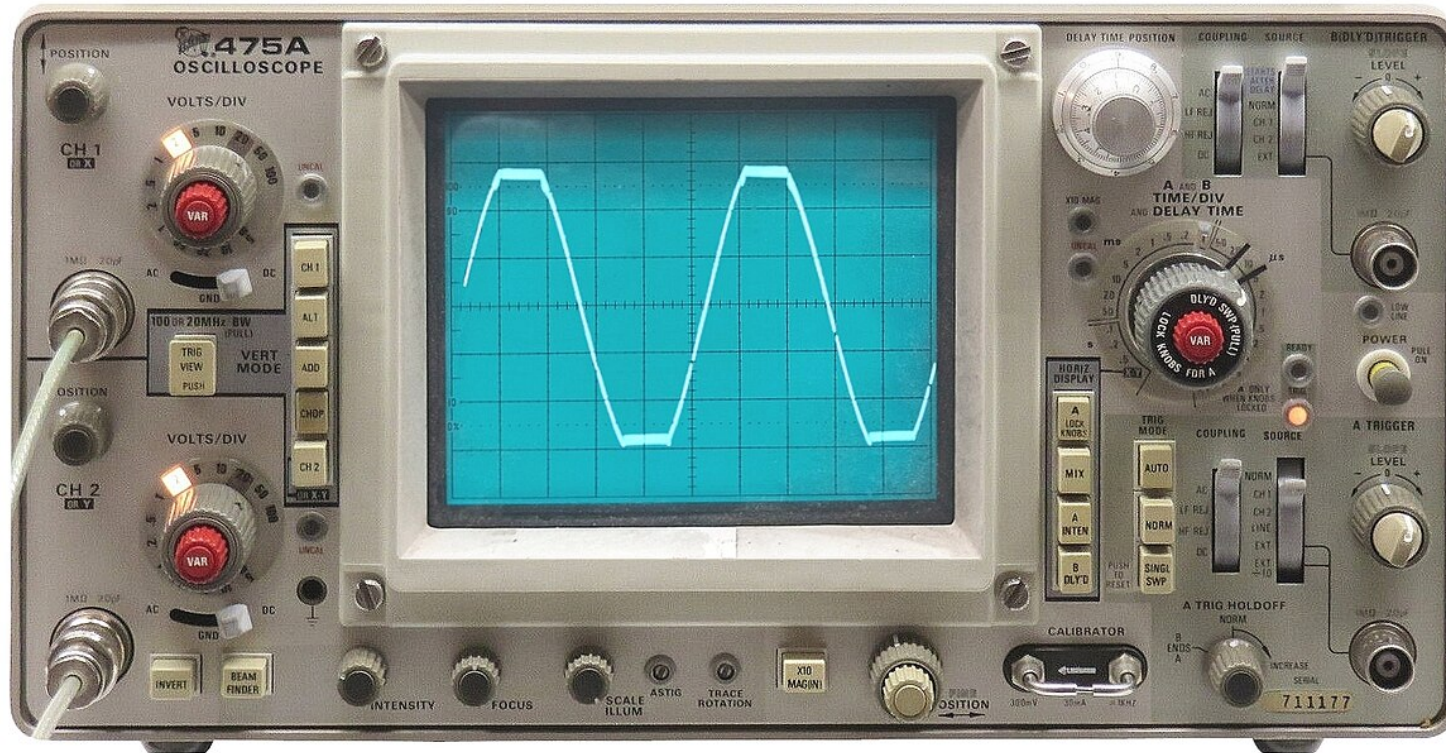


\$

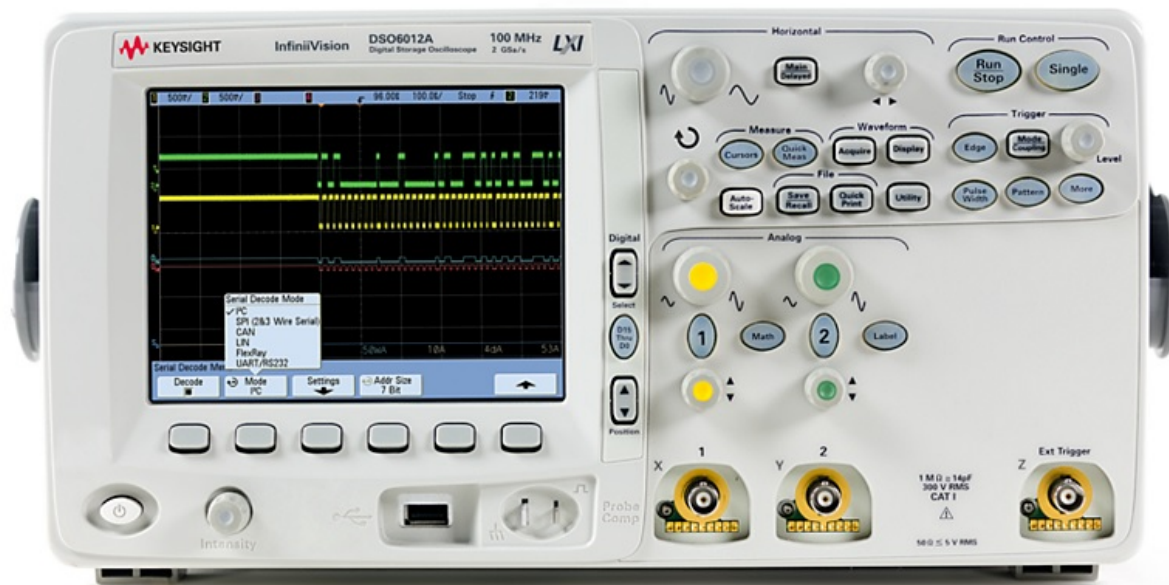


\$900





\$3,200



Thus, No Food or Drink in Lab



Let's Get to Know You

Who are you?

What do you hope to learn from class?

What's a fun fact that people might not know about you?

Course Mechanics

Northeastern University
College of Engineering



Course Topics

- Part 1: Building Blocks: Threat modeling based on physics, principles of information security and privacy, risk, research ethics
- Part 2: Embedded Security: Side channels, spectral analysis, timing attacks, power analysis, data remanence
- Part 3: Sensor Security: Physics of security, transducers, MEMS, audible and ultrasonic acoustics, RF, optics
- Part 4: Internet of Things (IoT) & Operational Technology (OT): Factory floors, robotics, advanced manufacturing, medical devices, smart homes
- Part 5: Machine Learning (ML) and Artificial Intelligence (AI): Embedded security for ML and AI

Course Prerequisites

At least one of the following courses, or permission of instructor:

- EECE 2160 (Embedded Design: Enabling Robotics)
- EECE 2412 (Fundamentals of Electronics)
- EECE 4534 (Microprocessor-Based Design)
- EECS 5515 (Wireless Sensor Networks and the Internet of Things)
- EECE 5666 (Digital Signal Processing)

Grading

- Class Participation and Presentation - 5%
- Hands-on Labs - 45%
- Midterm - 15%
- Final Group Project - 35%

Academic Integrity

- Students must uphold the highest standards of academic honesty. Violations (cheating, plagiarism, unauthorized collaboration, etc.) will be reported.
- Consequences include zeroes on assignments and potential failure in the course.
- See NU's full policy:
<https://osccr.sites.northeastern.edu/academic-integrity-policy/>

Generative AI

- Absolutely!
- Encouraged Uses: You may use AI tools for refining writing, grammar, and clarity. Occasionally, assignments will require use of generative AI.
- You must disclose your generative AI prompts as a form of “showing work” so we can assess that the original ideas are your own.
- Prohibited Uses: Do not rely on AI to generate ideas or references. Any hallucinated references, fabricated facts, or AI-style filler text (e.g., cliches such as “keen insight,” “absolutely essential,” or honorific fluff) will result in a zero for the assignment and may lead to failure in the course.
- Rule of Thumb: If AI use is invisible to us, you are likely safe. If we detect hallucinations or obvious AI artifacts, penalties will apply.

Hacking Ethics

To defend a system, you must think like an attacker, but testing real-world systems without permission is prohibited. Any unauthorized probing or compromise attempts may result in failure of the course, disciplinary action, and possible legal consequences. Please respect the privacy and property of others at all times.

Late Policy

- Submit homework/essays and labs before the start of class. Late means zero.
- Religious holidays: speak to course staff by tomorrow for accommodation.
- Doctor's note required for health-related absences; reach out privately to staff on Piazza ASAP for special cases.
- Personal time away, weddings, etc. would require early submission of work.
- Projects and labs: if late, docked a full letter grade per 24 hours late. Late starts one minute after the deadline. E.g., A->B, B->C

Security is a Negative Property of a System

- Confidentiality
- Integrity
- Availability
- Authentication
- Non-repudiation
- What isn't a security property?
 - Encryption: mechanism to provide confidentiality and sometimes, but not always, integrity and authentication
 - Hashing and blockchains (they are mechanisms, not properties, often misused)
 - Digital signatures and message authentication codes: mechanisms to provide authentication
- Not orthogonal! :-)

How to Contact Staff

<https://piazza.com/northeastern/fall2026/eece569808>



**Be wicked smaht; use Piazza.
That's where course updates and Q&A live.
Don't be a chowdahead and miss out!**



Photo credits: Boston Globe, Boston Herald

Next Steps

- Log into Piazza and post a hello about what you're looking to learn from the course
<https://piazza.com/northeastern/fall2026/eece569808>
- Read Adam Shostack's webpage on threat modeling:
<https://shostack.org/resources/threat-modeling>
- Prepare for a pop quiz; normally no warning given
- Next lecture: Threat Modeling