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 4, 2025

https://spqrlab1.github.io/emsec/

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

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.
- Essays: Short writing assignments applying embedded security principles to real-world scenarios.
- Final Group Project: Teams will conduct an extended project with demonstrations.
- In-class midterm, lecture scribing, pop quizzes, etc.

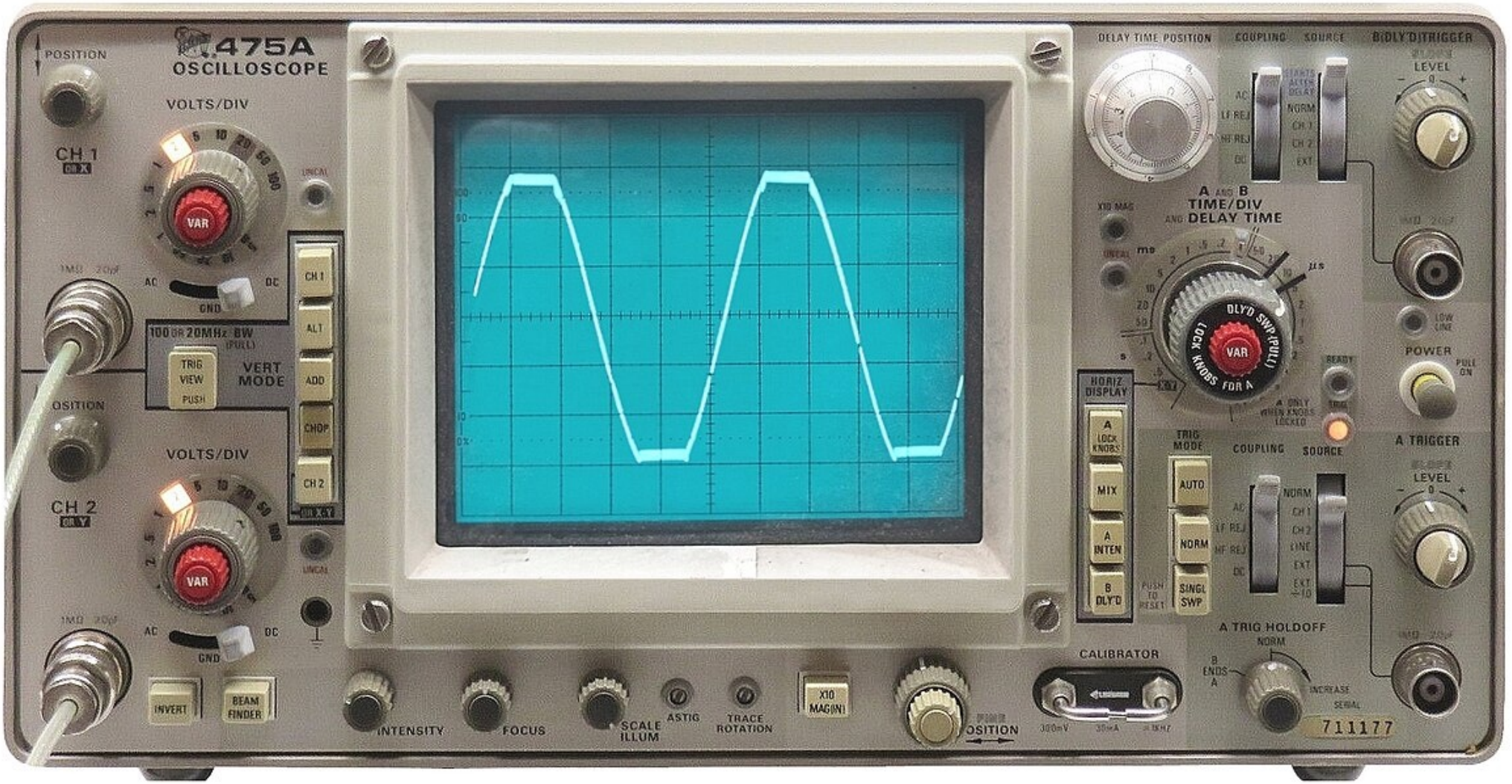

After Sales Service:
support@kungber.com
29.34
V
C.V
0.000
A
C.C
0.000
W
Kungber
—COARSE—
5V/2A
—FINE—

$

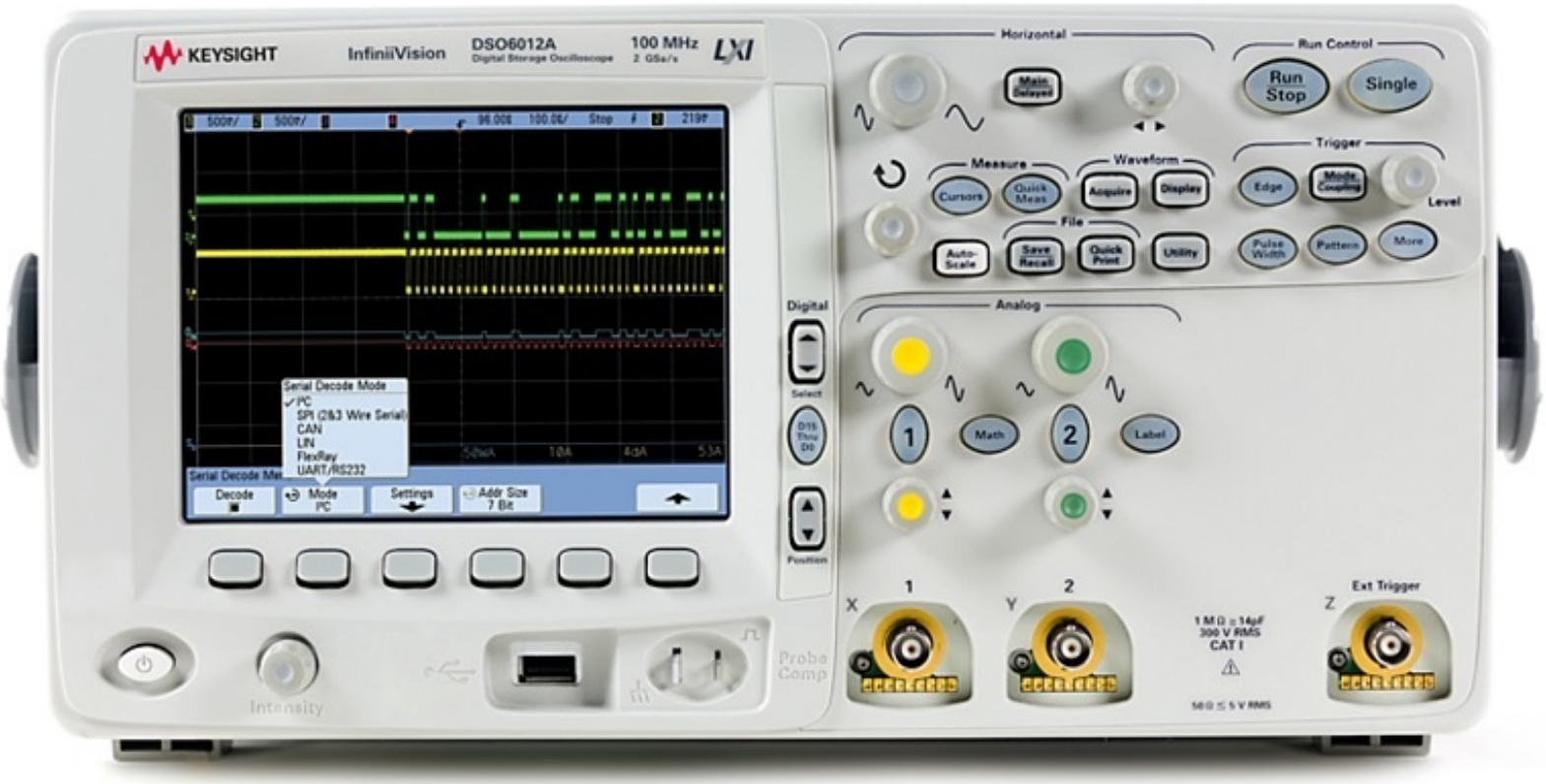

Agilent
LXI

$900


WARNING: NO OPERATOR SERVICEABLE PARTS INSIDE. REFER SERVICING TO SERVICE TRAINED PERSONNEL.
10 MHz In
± 5V
10 MHz Out
0 dBm
42Vpk
Modulation In
± 5V
Ext Trig / FSK / Burst
TTL
42Vpk
C US
168520
N10149
ICES/NMB-001
ISM 1-A
33220A
Made in Malaysia
100-240V 50-60Hz
100-127V 400Hz
50VA Max
LXI Class C
Non Auto-MDIX
GPIB
USB
LAN
WARNING: FOR CONTINUED FIRE PROTECTION, USE SPECIFIED ~ LINE FUSE.


475A
OSCILLOSCOPE
POSITION
VOLTS/DIV
CH 1
OR X
VAR
AC
GND
DC
CH 1
ALT
ADD
CHOP
CH 2
100 OR 20MHz BW
TRIG VIEW
PUSH
VERT MODE
CH 2
OR Y
INVERT
BEAM FINDER
INTENSITY
FOCUS
SCALE ILLUM
ASTIG
TRACE ROTATION
X10 MAG(IN)
POSITION
DELAY TIME POSITION
COUPLING
SOURCE
B DLY'D TRIGGER
LEVEL
A AND B TIME/DIV AND DELAY TIME
X10 MAG
DLY'D SWP (PULL) LOCK KNOBS FOR A
READY
POWER
HORIZ DISPLAY
A LOCK KNOBS
MIX
A INTEN
B DLY'D
TRIG MODE
AUTO
NORM
SINGL SWP
A TRIGGER
A TRIG HOLDOFF
CALIBRATOR
711177

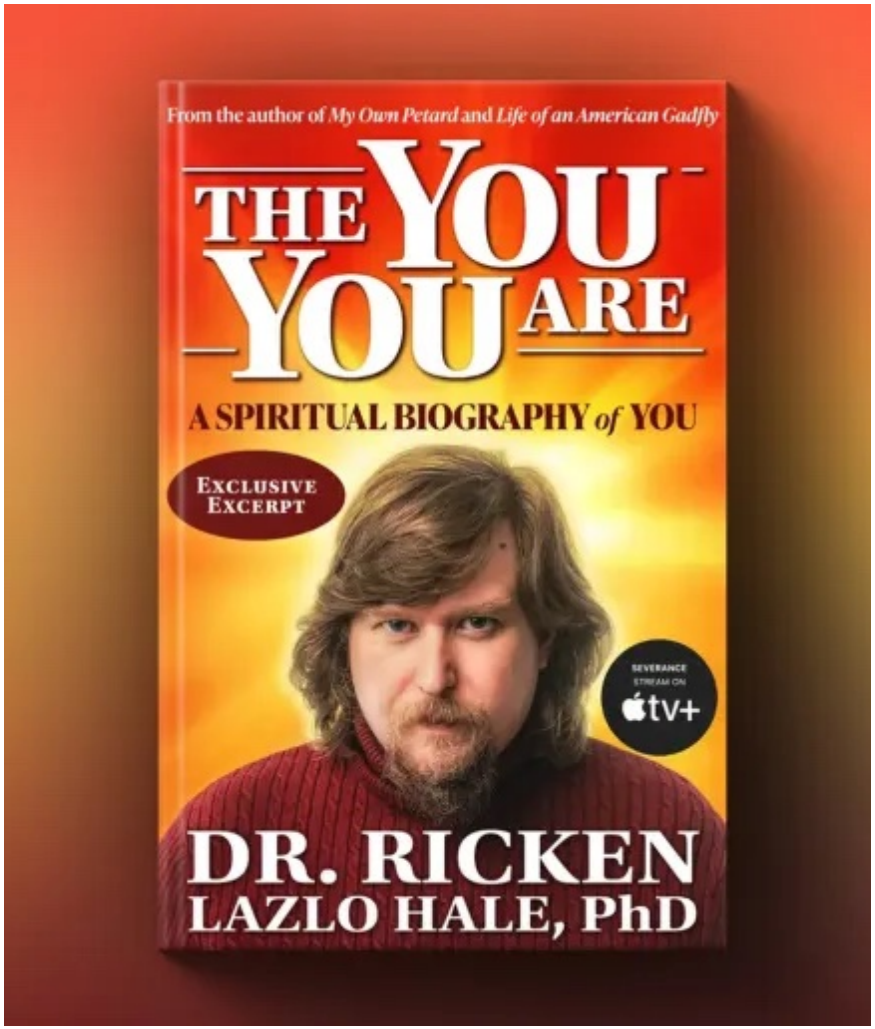
$3,200


KEYSIGHT
InfiniiVision
DSO6012A
Digital Storage Oscilloscope
100 MHz
2 GSa/s
LXI
Horizontal
Run Control
Run Stop
Single
Trigger
Measure
Waveform
File
Cursors
Acquire
Display
Edge
Level
Auto-Scale
Utility
Pulse Width
Pattern
More
Digital
Analog
Math
Label
Serial Decode Mode
I²C
SPI (2&3 Wire Serial)
CAN
LIN
FlexRay
UART/RS232
Decode
Mode
I²C
Settings
Addr Size
7 Bit
Select
Position
Intensity
Probe Comp
Ext Trigger
CAT I

Thu$, 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?



Midterm

- In-class Exam
- One double-sized, **hand written**, 8.5”x11” cheat sheet allowed
- No final exam; we have final projects

Course Mechanics

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%
- Essays - 15%
- Hands-on Labs - 30%
- 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.
- To accommodate for absences, being busy with graduate paper deadlines, football games, and minor illness where you are unable to get a doctor's note: we will drop the lowest score of one essay. However, we will not drop the scores of the first essay. I.e., you get one freebie essay. Use wisely!
- Doctor's note required for special circumstances (e.g., hospitalized, COVID); reach out privately to staff on Piazza ASAP
- Religious holidays: speak to course staff by 9/11 for accommodation.
- 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

Homework and Next

- Go to lab safety open house this week for checkoff (2336 EECS today at 4-5:30pm or Tuesday 9-10:30AM, next Tuesday, or by appointment with lab GSI Yan Long)
- For Wednesday: Read “On the Importance of Checking Cryptographic Protocols for Faults” by Boneh et al., EuroCrypt 1997
  - Discuss the topic freely on Piazza
  - Be prepared for a short in-lecture quiz as part of class participation
- Next lecture: Threat modeling for security
- Next->Next: Refresher on signals and systems

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/fall2025/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/fall2025/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