EECS 388

Introduction to Computer Security

Lecture 1:

Welcome!
The Security Mindset

August 29, 2023

Prof. Halderman and Prof. Ensafi

Today's Lecture

Welcome everyone,
both in the classroom and participating remotely!

Today, we'll cover:

- Who we are
- Goals for the course
- The security mindset
  - Thinking like an attacker
  - Thinking as a defender
- Course mechanics
- Security ethics

Who Are We?

Prof. J. Alex Halderman

Web: https://jhalderm.com
Mail: jhalderm@umich.edu
Office: 4717 Beyster

Internet-wide Security Intelligence

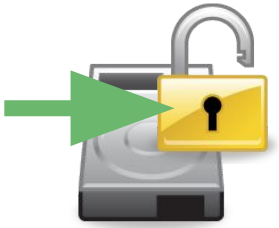
zmap

an open-source tool that can port scan the entire IPv4 address space from just one machine in minutes

Daily global scans track millions of vulnerable devices, new security threats

Our notifications increased rate of Heartbleed patching by 50% worldwide

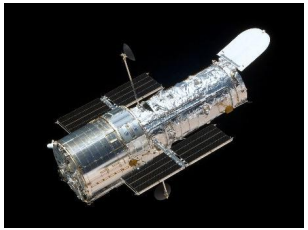
Real-world Cryptography



Cold-Boot Attack

breaks all full-disk encryption products,
inspired new subfield of crypto theory

Best Student Paper, *Usenix Security 2008*



Mining Ps and Qs

insufficient entropy compromises
RSA and DSA keys in millions of devices

Best Paper Award, *Usenix Security 2012*

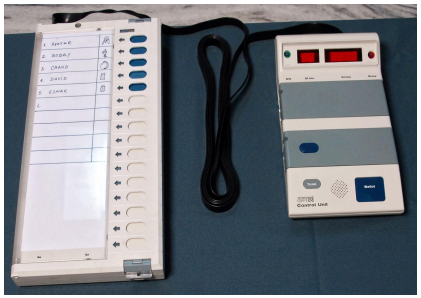
Imperfect Forward Secrecy

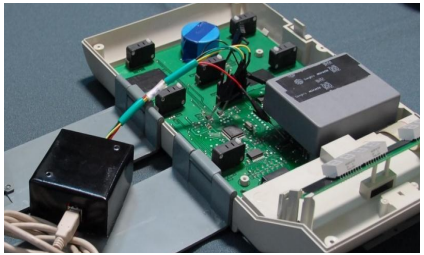
new TLS attack threatens 8% of the web,
NSA might tap 66% of VPNs using HPC

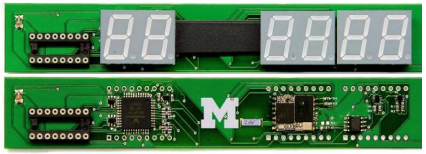
Best Paper Award, *ACM CCS 2015*

Embedded Systems Security

Traffic Infrastructure

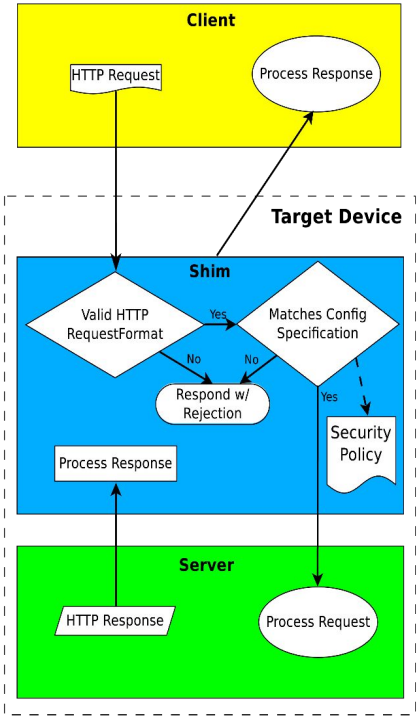






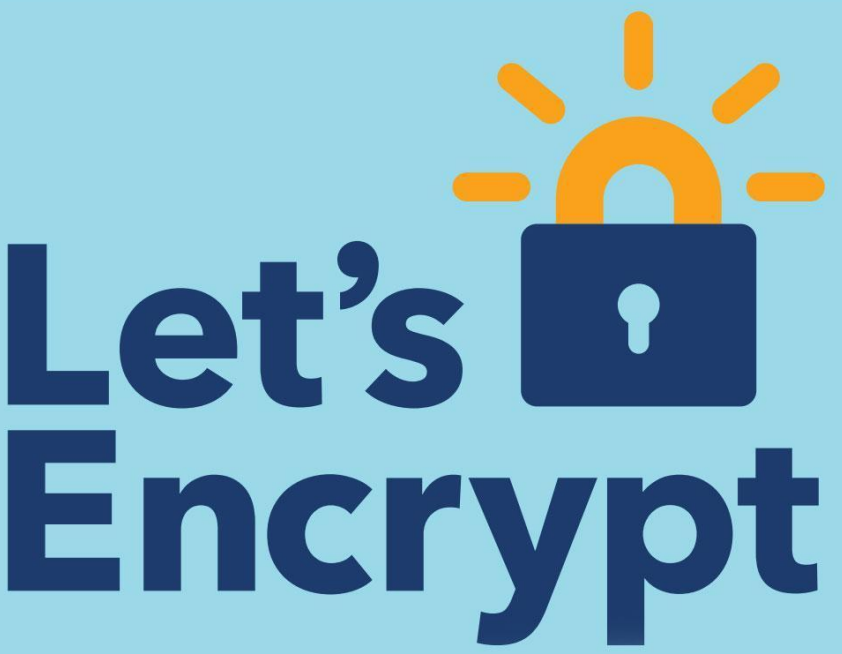
Voting Machines

TSA Airport Scanners



New Defenses

Encrypting the Entire Web



A free, automated, HTTPS certificate authority
to help encrypt the entire web

Election Cybersecurity

"Elections face real threats from nation-state attackers. And they'll be back."

Testimony to Senate Intelligence Committee

Who Are We?

Prof. Roya Ensafi

Web: https://ensa.fi
Mail: ensafi@umich.edu
Office: 4745 Beyster

Our Outstanding TAs


Isabella Allada


Hariharan Chidambaram


Lavender Li


Nina Moyski


Anirudh Ramprasad


Marshall Stone


Adam Austerberry


Aidan Delwiche


Chuang Liu


Ibrahim Musaddequr Rahman


Ben Schwartz


Jaden Sun


Edwin Chan


Christina Deng


Daniel Liu


Jai Narayanan


Robert Stanley


Sydney Zhong

Course Topics

EECS 388 teaches the **security mindset**, and the principles and practices of security. Learn foundations of building, using, and managing secure systems.

The Security Mindset	threat modeling, thinking like an attacker
Applied Cryptography	randomness, ciphers and MACs, public key cryptography, secure channels
Network Security	web security, TLS and HTTPS, authentication, network attacks and defenses
Host/Application Security	control hijacking, malware, isolation, side channels, forensics, hardware security
Security in Context	privacy and anonymity, election security, online censorship, public policy, physical security

Learning Objectives

Critical thinking:

- How to think like an attacker, anticipate threats
- How to reason about threats and risks
- How to balance security costs and benefits

Technical skills:

- Know how to better protect yourself
- Understand common vulnerabilities and defensive tools
- Basics of building and managing systems more securely

Greater understanding of concepts from all layers of the computing stack

~~Learn to be a 1337 hax0r.~~ Learn to be an ethical, security-conscious citizen with the **humility** necessary to engineer secure systems

What is computer security?

Security

Difference between these disasters?

Meet the Adversary

a.k.a. **the attacker**

Security studies how systems behave in the presence of an adversary.

An *intelligence* that actively tries to cause the system to misbehave.

Can be a person, people, or institution.

Often talked about in the abstract.

"Know your enemy." —Sun Tzu, *The Art of War*.

Movation? Capabilities? Opportunity?

The Security Mindset

The **security mindset** encourages thinking about **how attackers could cause systems to fail**, in order to head off problems before they are exploited.

Thinking like an attacker

- Understand techniques for circumventing security.
- Look for ways security can break, not excuses why it won't.

  Always ask: **"What could go wrong?"**

Thinking as a defender

- Know what you're defending, and against whom.
- Weigh benefits vs. costs: No system ever completely secure.

  Essentially "rational paranoia"

Thinking Like an Attacker

Imagine you are trying to attack the system:

- Look for **weakest links** (easiest places to attack)
- Identify **assumptions** security depends on. Are any of them false?
  example: "executing a program incorrectly and cleaning up is the same as not executing it" (led to Spectre and Meltdown)
- Think **outside the box**: Attackers not constrained by system designers' skillsets.
  example: software could be attacked via hardware vulnerabilities or physical security weaknesses

Helps to have a broad understanding of all the parts of how computer systems work.

Practice thinking like an attacker:

For every system you encounter, consider what it means for it to be secure, and image how attackers could exploit it.

Thinking like an attacker *shouldn't be* taboo… just don't follow through on your thinking!

Thinking Like an Attacker

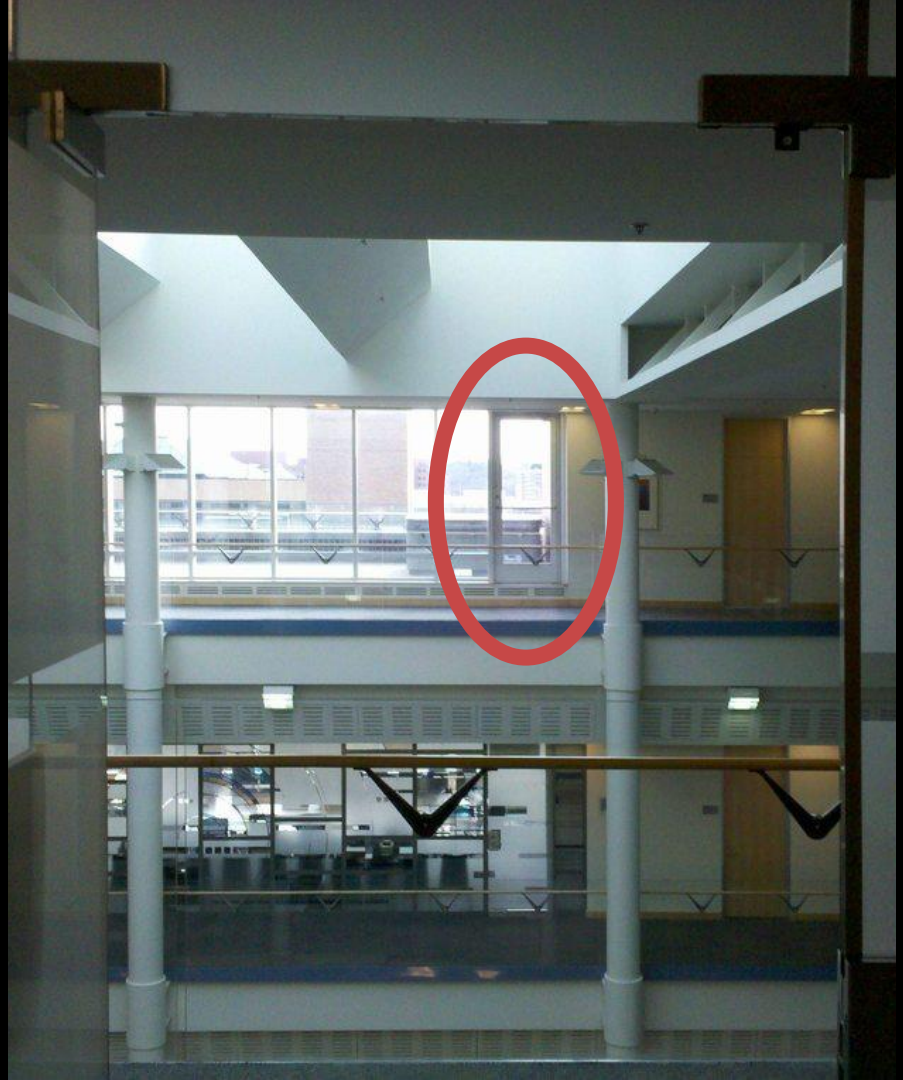
Thought exercise:

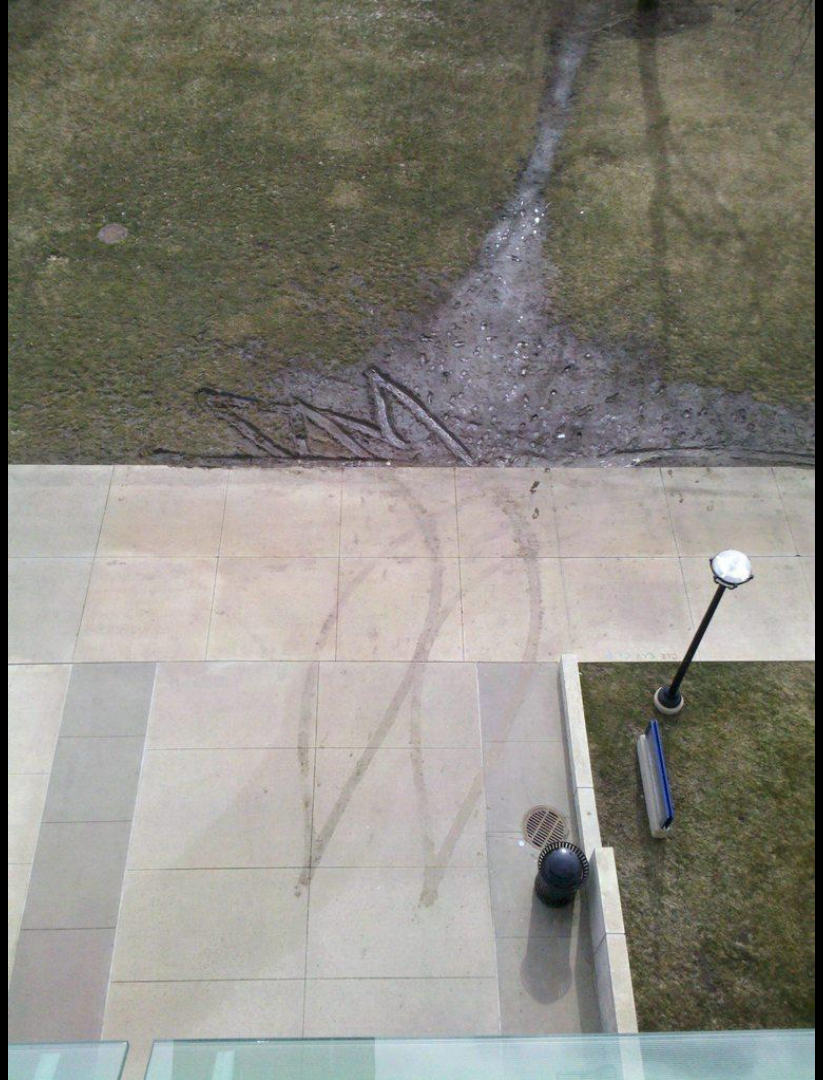
The Beyster Building was designed with locks so that only those with a valid key (MCard) can enter.

How to break in to the Beyster Building?

(Remember: Weakest links? Security assumptions? Thinking outside the box?)


THE BOB AND BETTY BEYSTER BUBBLER
A SPECIAL GIFT FOR THE STUDENTS OF MICHGAN CSE





Thinking Like an Attacker

Thought exercise:

Other security systems you interact with in everyday life?

What could go wrong?

Get in the habit of practicing adversarial thinking.
For every system you encounter, ask yourself how attackers could exploit it.

Thinking as a Defender

Security policies

- What **assets** are we trying to protect?
- What **properties** are we trying to enforce?
  e.g.: **confidentiality**, **integrity**, **availability**, **authenticity**

Challenge is to think rationally and rigorously about potential risks.

Rational paranoia

Threat modeling

- Who are we defending against? Attacker motivations?
- Which threats should we disregard? ("Outside our threat model")

Assessing risk

- What would breaches cost us? Money, safety, reputation, … How likely? How to recover?

Selecting countermeasures

- Costs vs. benefits? No security mechanism is free.
  Indirect costs include added complexity, false positives, lost productivity …
- Technical or nontechnical approaches e.g., law enforcement, procedures, training

Thinking as a Defender

Thought exercise:

Defending your apartment or dorm room?

Think in terms of:

- Assets?
- Adversaries?
- Likelihood?
- Countermeasures?
- Costs/benefits?

Thinking as a Defender

Thought exercise (later, on your own):

Using a credit card safely, as a consumer?

Think in terms of:

- Assets?
- Adversaries?
- Likelihood?
- Countermeasures?
- Costs/benefits?

Security Design and Assessment

Secure design is a **process**, not a product

- Not easily retrofitted
- Must be practiced continuously

Good design strives for **defense-in-depth**, requiring multiple failures for attacks to succeed

Common analyst mistake: Trying to convince yourself that the system is secure
Better approach: Identify weaknesses of your design and work to correct them

Places to focus security scrutiny:

- **Attack surface** (parts of the system exposed to attackers)
- **Trusted components** (parts that must function correctly for system to be secure)

Recall Our Learning Objectives ...

Critical thinking:

- How to think like an attacker, anticipate threats
- How to reason about threats and risks
- How to balance security costs and benefits

Technical skills:

- Know how to better protect yourself
- Understand common vulnerabilities and defensive tools
- Basics of building and managing systems more securely

Greater understanding of concepts from all layers of the computing stack

~~Learn to be a 1337 hax0r.~~ Learn to be an ethical, security-conscious citizen with the **humility** necessary to engineer secure systems

Lectures and Labs

Lectures cover core security concepts and applications

Prof. Halderman, Prof. Ensafi, and a few distinguished guests
Slides posted to Piazza before each lecture
Video recordings available on Canvas shortly after each lecture
Everyone is welcome to attend in-person if there are open seats

Labs cover vital tools and techniques for completing the projects

Detailed reviews of assignments and solutions
Hands-on tutorials of tools used for projects
Pre-recorded video will be posted each week
You may attend any lab section if there are open seats

We encourage coming to class. It's more fun, and you can ask questions!

Attendance

Choose the mode of learning that works best for you

Keep up with the material by attending in person and/or reviewing materials online

Default policy: We encourage coming to class, but we won't make you

Optional policy: Strict attendance with penalties (a Ulysses pact)

If you think you'd benefit from lecture but *know* you won't show up unless we make you, you can **opt-in** to this strict attendance policy. Email eecs388-staff@umich.edu to sign up.

- If you opt for strict attendance, your decision will be irrevocable
- We'll track your attendance with a sign-in sheet at the front of the lecture room
- You'll be allowed to miss up to two lectures without penalty
- After that, we'll reduce your overall course grade by 0.5% for every time you fail to sign the sheet, up to a maximum of 5%
- Absences will be excused only under extraordinary circumstances with documentation

Lecture and Lab Mechanics

Lecture: In-person and hybrid options

Encouraged: Attend lectures in person

Everyone is welcome, but seats only reserved for those in Section 001

Permitted: Watch lecture video asynchronously

Either way: Complete a **brief quiz** on Canvas before the next lecture day

Lab: In-person and hybrid options

Encouraged: Attend lab in person

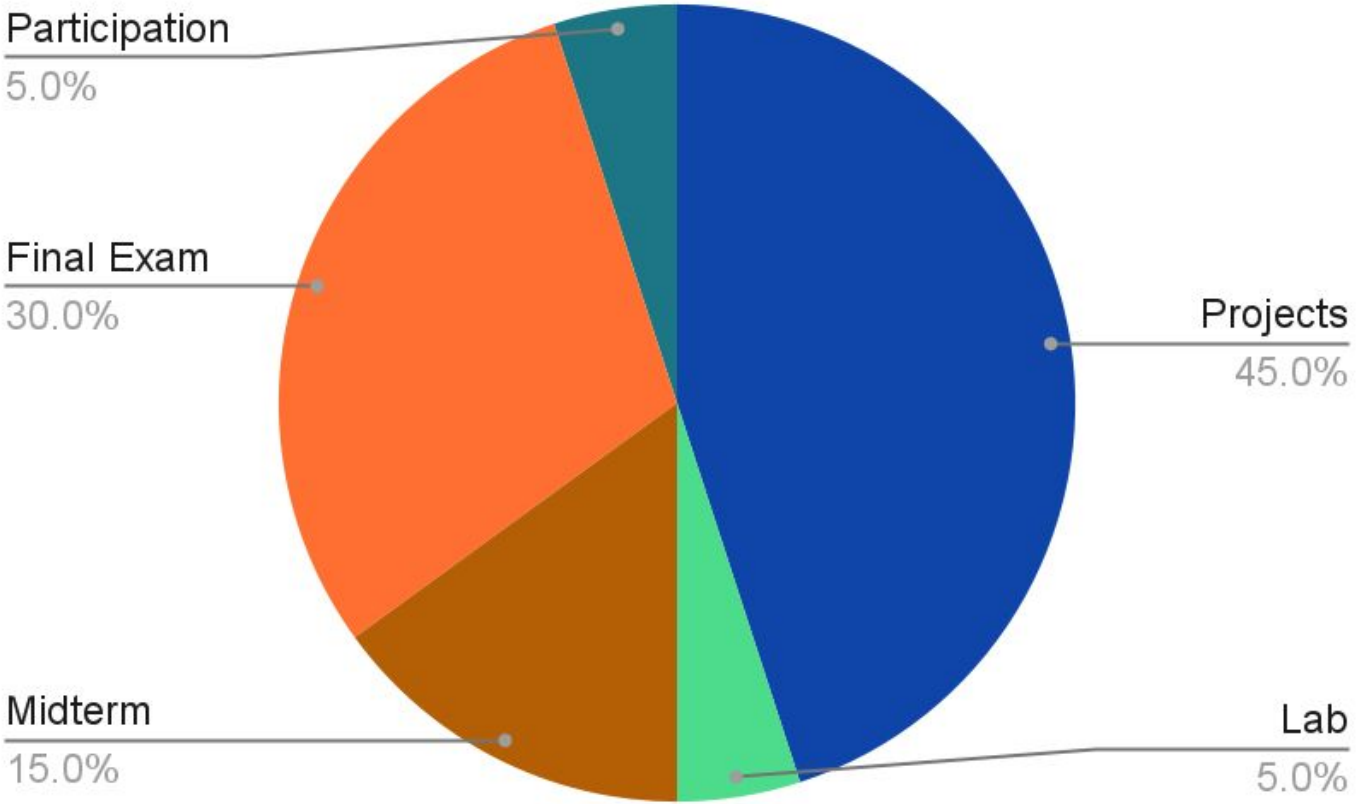
May attend any section, but seats only reserved for your registered lab section

Permitted: Watch lab video asynchronously

First labs meet Friday/Monday after Labor Day. Videos will be posted each week

No capacity limit: Everyone eligible has permission to enroll

Grading


Participation
5.0%
Final Exam
30.0%
Projects
45.0%
Midterm
15.0%
Lab
5.0%

Participation and Quizzes (5%)

2.5%

Intellectual Contributions

in class, OH, or Piazza

Goal: Encourage you to be a positive part of the learning experience. E.g.:

- asking good questions
- making thoughtful comments
- helping others appropriately

We look for quality over quantity and encourage maintaining a high signal-to-noise ratio.

Participation and Quizzes (5%)

2.5%

Intellectual Contributions

in class, OH, or Piazza

Goal: Encourage you to be a positive part of the learning experience. E.g.:

- asking good questions
- making thoughtful comments
- helping others appropriately

We look for quality over quantity and encourage maintaining a high signal-to-noise ratio.

+

2.5%

Brief Quizzes on Canvas

after each lecture

(due before day of next lecture)

Goal: Encourage you to keep up with the lectures

First Lecture Quiz

Available today

~~Due by **midnight tomorrow**~~

Extension: Due by **11:59pm Monday**

Projects (45%)

Five technical projects

1. Cryptography
2. Web security
3. Network security
4. Application security
5. Computer forensics

Project 1: Cryptography
Available Thursday

Part 1 due **Sept. 14** at 6 p.m.
Part 2 due **Sept. 21** at 6 p.m.

May work individually or with a partner for Projects 1–4; **must** work with a partner for Project 5

Upper-level course projects often require learning on your own, building on what we cover in class. Make sure you follow lecture and lab, and start early

Projects will be distributed on EECS388.org and submitted via Autograder.io

Lab Assignments (5%)

Simple labs accompanying the projects

Interactive introductions to languages or tools

Must be completed individually

Lab 1: Docker and Python
Available Thursday

Due **Sept. 7** at 6 p.m

Upper-level course projects often require learning on your own, building on what we cover in class. Make sure you follow lecture and lab, and start early

Lab assignments will be distributed on EECS388.org and submitted via Autograder.io

Assignment Policies

Lateness

We want to return graded work promptly and review solutions in your next lab, so:

Lateness policy:

- 10% penalty for being late
- Lose additional 10% every 4 hours
- Late work cannot be accepted after start of following lab (of any section)

Professors may grant exceptions under extraordinary circumstances. Talk to us.

Please start assigned work early.

Collaboration

We encourage you to learn together by discussing course **concepts**

No cheating policy:

- Don't give or accept **hints/solutions**, including from AI
- Don't copy others' work
- Don't share or post your solutions

Questions? Ask us.

We have **booby traps** in place to catch cheaters. We'll report you to the Honor Council after the final exam.

Midterm (15%) and Final (30%)

Midterm Exam

Friday, Oct. 20, 7–8:30 p.m. **IN PERSON**
Covers first half of the course

Final Exam

Thursday, Dec. 14, 7–9 p.m. **IN PERSON**
Covers the entire course

Exams will test concepts and techniques that you learn *from the lectures and the projects.*

We'll provide practice exams and hold review sessions prior to each test.

Communication and Resources

Website: eecs388.org
overview, schedule, assignments

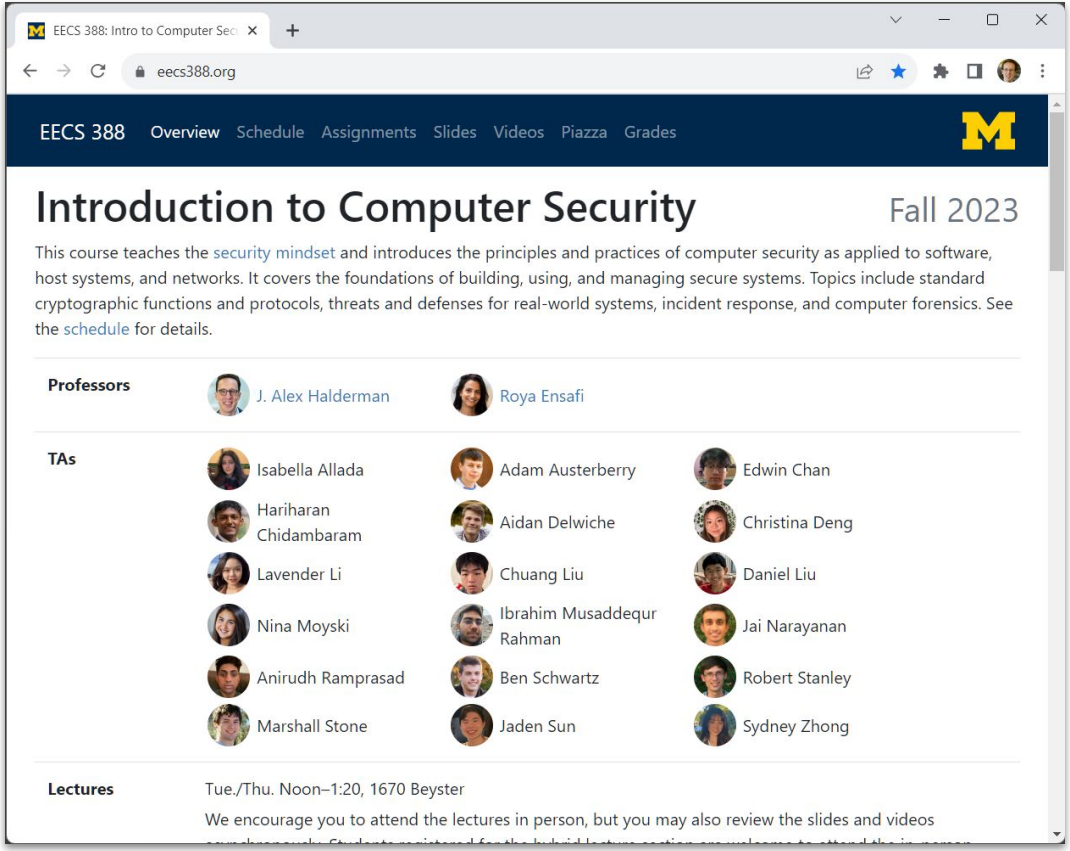
Piazza
questions, discussion, slides, announcements

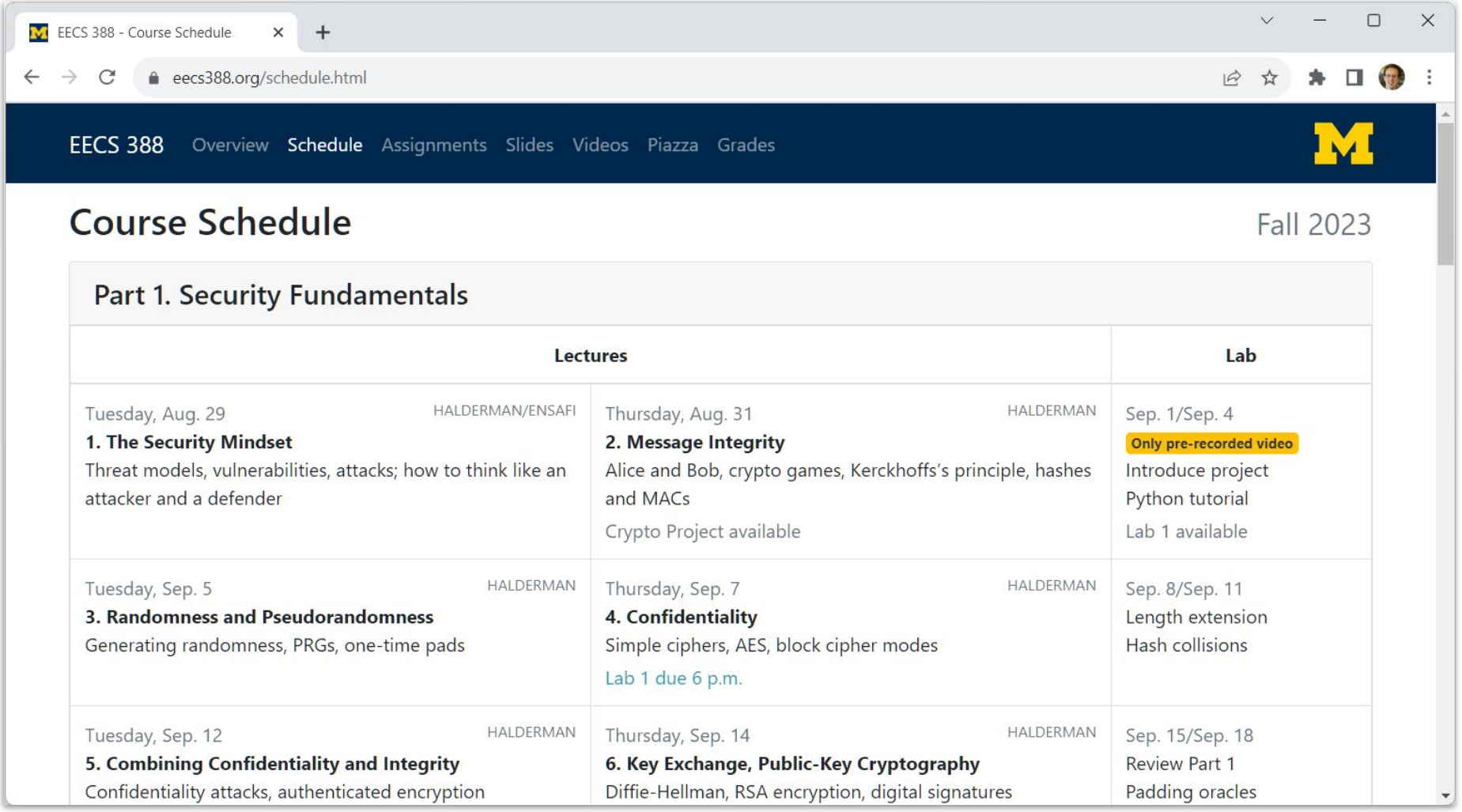
Canvas
gradebook, lecture videos

Autograder.io
assignment submission/grading

Office Hours
(see calendar on course website)

eecs388-staff@umich.edu
administrative issues




EECS 388 - Course Schedule
eecs388.org/schedule.html
EECS 388 Overview Schedule Assignments Slides Videos Piazza Grades
Course Schedule
Fall 2023
Part 1. Security Fundamentals
Lectures
Lab
Tuesday, Aug. 29 HALDERMAN/ENSAFI
1. The Security Mindset
Threat models, vulnerabilities, attacks; how to think like an attacker and a defender
Thursday, Aug. 31 HALDERMAN
2. Message Integrity
Alice and Bob, crypto games, Kerckhoffs's principle, hashes and MACs
Crypto Project available
Sep. 1/Sep. 4
Only pre-recorded video
Introduce project
Python tutorial
Lab 1 available
Tuesday, Sep. 5 HALDERMAN
3. Randomness and Pseudorandomness
Generating randomness, PRGs, one-time pads
Thursday, Sep. 7 HALDERMAN
4. Confidentiality
Simple ciphers, AES, block cipher modes
Lab 1 due 6 p.m.
Sep. 8/Sep. 11
Length extension
Hash collisions
Tuesday, Sep. 12 HALDERMAN
5. Combining Confidentiality and Integrity
Confidentiality attacks, authenticated encryption
Thursday, Sep. 14 HALDERMAN
6. Key Exchange, Public-Key Cryptography
Diffie-Hellman, RSA encryption, digital signatures
Sep. 15/Sep. 18
Review Part 1
Padding oracles

Assignments

Fall 2023

Projects

There will be five projects, which will count for a total of 45% of your course grade. You may work individually or with a partner for Projects 1–4, but you **must** work with a partner for Project 5. You may switch partners between projects.

1. **Crypto Project** (available Thursday, Aug. 31) – Part 1 due Thursday, Sep. 14 at 6 p.m.; Part 2 due Thursday, Sep. 21 at 6 p.m.
2. **Web Project** (available Thursday, Sep. 21) – due Thursday, Oct. 5 at 6 p.m.
3. **Networking Project** (available Thursday, Oct. 5) – due Thursday, Oct. 26 at 6 p.m.
4. **AppSec Project** (available Thursday, Oct. 26) – due Thursday, Nov. 16 at 6 p.m.
5. **Forensics Project** (available Thursday, Nov. 16) – due Thursday, Dec. 7 at 6 p.m.

Lab Assignments

Accompanying each project, we'll ask you to complete a simple assignment that provides an interactive introduction to relevant programming languages or tools. We'll go over how to complete these during lab. You must complete them individually, and they will count for a total of 5% of your grade.

- **Lab 1: Docker and Python** (available Friday, Sep. 1) – due Thursday, Sep. 7 at 6 p.m.
- **Lab 2: Browser DevTools** (available Friday, Sep. 22) – due Thursday, Sep. 28 at 6 p.m.
- **Lab 3: Python Sockets** (available Friday, Oct. 6) – due Thursday, Oct. 12 at 6 p.m.
- **Lab 4: GDB** (available Friday, Oct. 27) – due Thursday, Nov. 2 at 6 p.m.
- **Lab 5: Autopsy** (available Friday, Nov. 17) – due Thursday, Nov. 30 at 6 p.m.

Ethics, Law, and University Policies

Don't be evil!

- Learn to use your security skills responsibly and for good.
- **388 ethics policy:** Respect privacy and property rights **or else you fail.**
- Stay safe: practice attacks **only on systems we give you to test.**

Warning

Federal and state laws criminalize computer intrusion, wiretapping.

- Example: *Computer Fraud and Abuse Act* (CFAA)
- You can be sued or go to prison.

University policies prohibit tampering with campus systems.

- You can be disciplined, even expelled.

Homework: Getting to Know You

Assignment:

Take a selfie and mail it to us
(follow the template shown here)

Due before next lecture

New Message

Recipients eecs388-photos@umich.edu

Subject *[Your Uniqname]*

> What name should we call you?

> What's your year and major?

> What would you like to learn in 388?

> Selfie!

Send

Coming Up

Reminders:

Send selfie email before next lecture

Complete the Quiz on Canvas after every lecture, due (normally) before the date of the next lecture

Thursday

Intro to Cryptography

Alice and Bob
Kerckhoffs's principle
Hashes and MACs

Coming Weeks

Applied Cryptography

Pseudorandomness
Integrity and confidentiality
Public key cryptography