



EECS 388

Introduction to Computer Security

Lecture 1:

Welcome! The Security Mindset

August 27, 2024

Prof. Halderman and Prof. Chen



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



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](#)

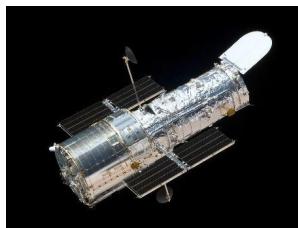
Real-world Cryptography



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



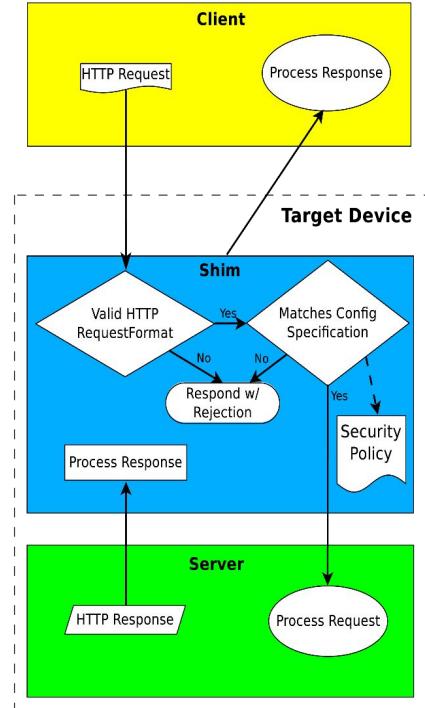
Traffic Infrastructure



Voting Machines



TSA Airport Scanners



New Defenses



Let's Encrypt

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

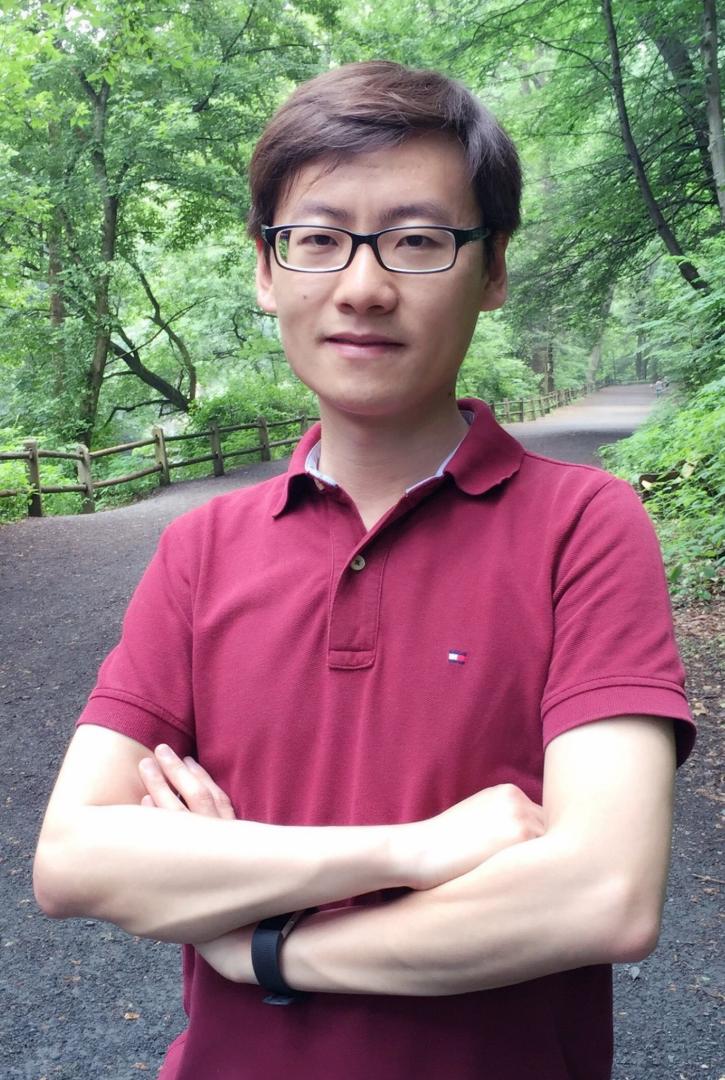
Election Cybersecurity



C-SPAN
c-span.org
@cspan



Who Are We?



Prof. Ang Chen

Web:

<https://web.eecs.umich.edu/~chenang/>

Mail: chenang@umich.edu

Office: 4753 Beyster

Research interests



Network security

- Examine latest networking hardware trends and understand security implications
- E.g., programmable switches and NICs (network interface cards)

Datacenter security

- How modern datacenters are constructed
- Modern hardware/software stacks (e.g., Remote direct memory access)
- Their security implications

Censorship circumvention

- Building anti-censorship network proxies in non-traditional locations
- Cloud, edge networks, ..

Beyond computer security



Cloud computing

- Infrastructure-as-code

Industrial digitalization

- Modernization of industrial infras, such as power grids

OS mechanisms

- Rust-based kernel development
- eBPF ecosystem

Our Outstanding TAs



Edwin Chan



Santiago Guiza



Lani Quach



Ben Schwartz



Sydney Zhong



Hariharan
Chidambaram



Leonardo
Lindemberg



Ibrahim Musaddequr
Rahman



Robert Stanley



Aidan Delwiche



Jai Narayanan



Josh Roy



Alan Zhang

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?

Difference between these disasters?



Meet the Adversary



a.k.a. the attacker

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

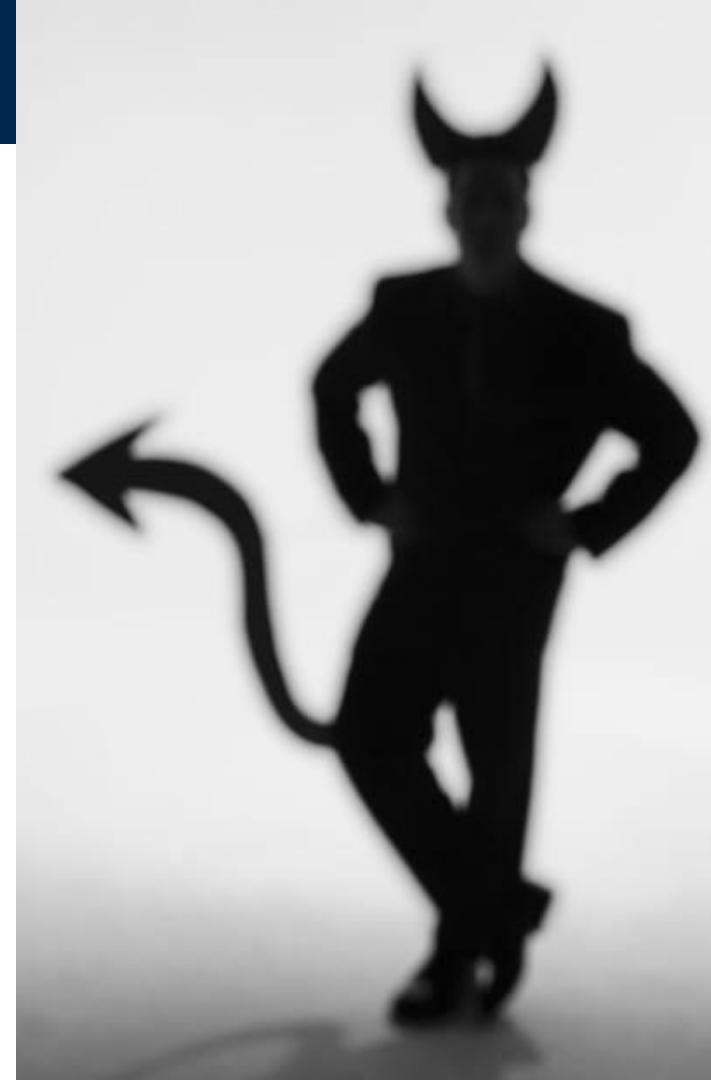
An *intelligence* that actively tries to cause
the system to misbehave.

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!



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?)

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.

Interlude: Great “Hacks” of Michigan



The Bob and Betty Beyster Bubbler (2012)

<https://cse.engin.umich.edu/stories/hackers-install-bubbler-as-a-salute-to-beysters>



Interlude: Great “Hacks” of Michigan



BBB Blinkenlights (2012-present)

<https://blinken.org>

<https://cse.engin.umich.edu/stories/hackers-brighten-beyster-building-with-a-puzzle-of-programmable-lights>

The screenshot shows a web browser window with the URL blinken.org/gallery/. The page title is "BBB Blinken Bulbs". There are three navigation links: "Status", "Gallery", and "Example". Below the title, there is a heading "BBB Blinken Bulbs Gallery" and a link "Next >>".
The main content area displays two light patterns:

- Out of phase:** A pattern where lights are lit in a staggered sequence, appearing to move across the building's facade.
- Maize & Blue:** A pattern where lights are lit in a repeating sequence of yellow and blue dots along the building's edge.

Each pattern has a "Running" button and links for "comments" and "code".



Bob and Betty Beyster Blinkenlights

Welcome to the Bob and Betty Beyster Blinkenlights, the individually addressable, student controlled Christmas lights of the BBB. Checkout [@bbb_blinken](#) or ask around and surely someone will share the API such that you too can learn how to hack the blinkenlights.

Happy Holidays!

- The Bob and Beyster Brigade

Interlude: Great “Hacks” of Michigan

M

Chez Betty (2013-2020)

<https://www.michigandaily.com/news/chez-betty-stays-open/>



Interlude: Great “Hacks” of Michigan



GG Brown LED Wall Hack (2015)

<https://youtu.be/ifUW-KOMSAg>





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. Chen, 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

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

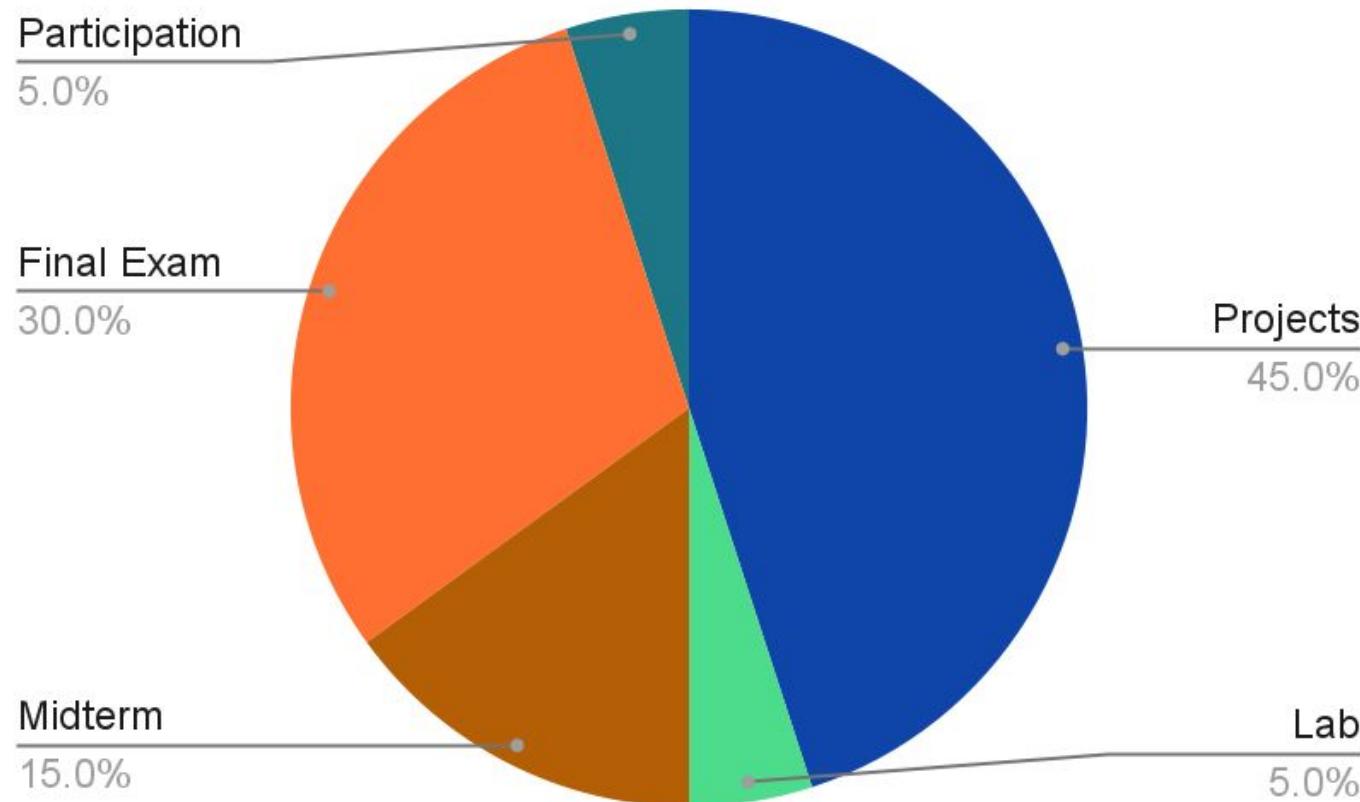
May attend any section, but seats only reserved for your registered lab section

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 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 a high signal-to-noise ratio.



Participation and Quizzes (5%)



2.5%

+

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 a high signal-to-noise ratio.

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

Projects (45%)



Five technical projects

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

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

Project 1: Cryptography

Available Thursday

Part 1 due **Sept. 12** at 6 p.m.

Part 2 due **Sept. 19** 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.

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. 5** 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 work in promptly so we can move on and review solutions together.

Labs and Projects:

- 3 late days* for all routine illness, tech problems, scheduling conflicts, etc.

Quizzes:

- Half credit if in before final exam day

Exceptions only for **extreme** medical or personal emergencies, with documentation

*See policy details on <https://eecs388.org>

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. 18, 7–8:30 p.m. IN PERSON

Covers first half of the course

Final Exam

Tuesday, Dec. 17, 7–9 p.m. IN PERSON

Covers the entire course

Exams are IN PERSON only. Plan travel accordingly.

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

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

If you require testing accommodations, upload SSD form via umich-accommodate.symplicity.com.



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

The screenshot shows the EECS 388 course website (eecs388.org) in a web browser. The page title is "EECS 388: Intro to Computer Security". The main content area includes:

- Introduction to Computer Security** (Fall 2024)
- A brief course description: "This course teaches the security mindset and introduces the principles and practices of computer security as applied to software, host systems, and networks. It covers the foundations of building, using, and managing secure systems. Topics include standard cryptographic functions and protocols, threats and defenses for real-world systems, incident response, and computer forensics. See the [schedule](#) for details."
- Professors**: J. Alex Halderman and Ang Chen.
- TAs**: Edwin Chan, Hariharan Chidambaram, Leonardo Lindenberg, Santiago Guiza, Jai Narayanan, Lani Quach, Ibrahim Musaddequr Rahman, Ben Schwartz, Robert Stanley, Sydney Zhong, and Josh Roy.
- Lectures**: Tue./Thu. Noon–1:20, 1670 Beyster. A note states: "We encourage you to attend the lectures in person, but you may also review the slides and videos asynchronously. Students registered for the hybrid lecture section are welcome to attend the in-person"

EECS 388 - Course Schedule			
EECS 388		Overview	Schedule
		Assignments	Slides
		Piazza	
 EECS 388 Course Schedule		Fall 2024	
<h2>Course Schedule</h2> <h3>Part 1. Security Fundamentals</h3>			
Lectures		Lab	
Tuesday, Aug. 27 1. The Security Mindset Threat models, vulnerabilities, attacks; how to think like an attacker and a defender	HALDERMAN/CHEN	Thursday, Aug. 29 2. Message Integrity Alice and Bob, crypto games, Kerckhoffs's principle, hashes and MACs Crypto Project available Lab 1 available	HALDERMAN Aug. 30/Sep. 2 Only pre-recorded video Introduce project Python tutorial
Tuesday, Sep. 3 3. Randomness and Pseudorandomness Generating randomness, PRGs, one-time pads	HALDERMAN	Thursday, Sep. 5 4. Confidentiality Simple ciphers, AES, block cipher modes Lab 1 due 6 p.m.	HALDERMAN Sep. 6/Sep. 9 Length extension Hash collisions
Tuesday, Sep. 10 5. Combining Confidentiality and Integrity Confidentiality attacks, authenticated encryption	HALDERMAN	Thursday, Sep. 12 6. Key Exchange, Public-Key Cryptography Diffie-Hellman, RSA encryption, digital signatures	HALDERMAN Sep. 13/Sep. 16 Review Part 1 Padding oracles

EECS 388 - Assignments x +

eeecs388.org/assignments.html

EECS 388 Overview Schedule **Assignments** Slides Piazza 

Assignments

Fall 2024

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. 29) – Part 1 due Thursday, Sep. 12 at 6 p.m.; Part 2 due Thursday, Sep. 19 at 6 p.m.
2. **Web Project** (available Thursday, Sep. 19) – due Thursday, Oct. 3 at 6 p.m.
3. **Networking Project** (available Thursday, Oct. 3) – due Thursday, Oct. 24 at 6 p.m.
4. **AppSec Project** (available Thursday, Oct. 24) – due Thursday, Nov. 14 at 6 p.m.
5. **Forensics Project** (available Thursday, Nov. 14) – due Thursday, Dec. 5 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 Thursday, Aug. 29) – due Thursday, Sep. 5 at 6 p.m.
- **Lab 2: Browser DevTools** (available Thursday, Sep. 19) – due Thursday, Sep. 26 at 6 p.m.
- **Lab 3: Python Sockets** (available Thursday, Oct. 3) – due Thursday, Oct. 10 at 6 p.m.
- **Lab 4: GDB** (available Thursday, Oct. 24) – due Thursday, Oct. 31 at 6 p.m.
- **Lab 5: Autopsy** (available Thursday, Nov. 14) – due Thursday, Nov. 21 at 6 p.m.

Lecture Quizzes



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 at right)

Due before next lecture

New Message - X

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 A U C S ⋮ trash icon

Coming Up



Reminders:

Send selfie email before next lecture

**Complete the Quiz on Canvas after every lecture,
due before the day 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