CSE 127: Intro to Computer Security

WI24

Lecture 1 - Security Mindset

Slide Credit: Kirill Levchenko, Stefan Savage, Deian Stefan, Nadia Heninger, Earlence Fernandes, Imani Munyaka

Announcements

HW1 is posted

Class will start between 11:05 and 11:10am

Topics Covered

- The Security Mindset
  - Principles and threat modeling
- Systems/Software Security
  - Classic attacks and defenses on memory safety, isolation
- Web Security
  - Web architecture, web attacks, web defenses
- Network Security
  - Network protocols, network attacks, network defenses
- Cryptography
  - Public and private-key cryptography, TLS, PKI
- Privacy, Anonymity, Ethics, Legal Issues

Course Goals

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

Course Goals

- Critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits
- Technical skills
  - How to protect yourself
  - How to manage and defend systems
  - How to design and implement secure systems

Course Goals

- Critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits
- Technical skills
  - How to protect yourself
  - How to manage and defend systems
  - How to design and implement secure systems
- Learn to be a security-conscious citizen

Course Goals

- Critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits
- Technical skills
  - How to protect yourself
  - How to manage and defend systems
  - How to design and implement secure systems
- Learn to be a security-conscious citizen

  Learn to be a leet h4x0r
-

Course Goals

- Critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits
- Technical skills
  - How to protect yourself
  - How to manage and defend systems
  - How to design and implement secure systems
- Learn to be a security-conscious citizen

  Learn to be a leet h4x0r, but an ethical one!
-

Grading

40% Five programming assignments

Work in groups of two

Do your own programming and writeup

General discussion is encouraged (Piazza)

20% Midterm exam

In person unless UCSD is fully remote

Closed book with cheat sheet

40% Final exam

In person unless UCSD is fully remote

Closed book with cheat sheet

Course Policies

Late days and extensions:

- You have two late days to use as you wish
- Both you and your partner must have late days to use them

Course Policies

Late days and extensions:

- You have two late days (48hrs) to use as you wish
- Both you and your partner must have late days to use them

Regrade policy:

- Regrades should be the exception not the norm
- Incorrect regrade request ⟹ negative points

Course Policies

Late days and extensions:

- You have two late days to use as you wish
- Both you and your partner must have late days to use them

Regrade policy:

- Regrades should be the exception not the norm
- Incorrect regrade request ==⇒ negative points

Academic integrity:

- UC San Diego policy: https://academicintegrity.ucsd.edu
- We have to report suspected cases, don't make it weird
- If you are not sure if something is cheating, ask

Course Resources

- No official textbook. Optional books:
  - *Security Engineering* by Ross Anderson
  - *Hacking: The Art of Exploitation* by Jon Erikon

Course Resources

- No official textbook. Optional books:
  - *Security Engineering* by Ross Anderson
  - *Hacking: The Art of Exploitation* by Jon Erikon

  Assignments and readings on course site:
- https://cseweb.ucsd.edu/classes/wi24/cse127-a/

Course Resources

- No official textbook. Optional books:
  - *Security Engineering* by Ross Anderson
  - *Hacking: The Art of Exploitation* by Jon Erikon
- Assignments and readings on course site:

  https://cseweb.ucsd.edu/classes/wi24/cse127-a/

- Questions? Post to Piazza.

Course Resources

No official textbook. Optional books:

- *Security Engineering* by Ross Anderson
- *Hacking: The Art of Exploitation* by Jon Erikon

Assignments and readings on course site:

https://cseweb.ucsd.edu/classes/wi22/cse127-a/

Questions? Post to Piazza.

Course Resources

Lectures, office hours:

- On Zoom if UCSD is remote
- In person when UCSD is in person
- Lectures might be recorded

Discussion Session

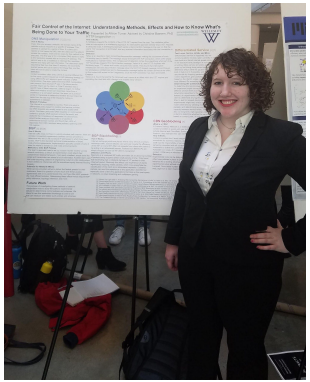
- Virtual (Zoom)
- recorded

Office Hours

- Instructors will be announced
- Piazza, Google Calendar
- Autograder (Queue?)

TA: Kunj Champaneri

TA: Allison Turner



Tutor: Andrei Secor

Tutor: Ruinan Ma

Purpose of Each Instructor

Instructor/Prof

- Lecture
- Office Hours
- Exam Grading

TAs

- Lecture (Review of Material)
- Homework Grading
- Office Hours

Tutors

- Office Hours

Purpose of Each Instructor

Instructor/prof

- Anything

Instructor/Prof or TAs

- Specific question about homework or reading

Tutors

- Questions about concepts
- A little refresher on background stuff (maybe)

Use your resources!

Other Resources

- View prior recordings from previous iterations on ucsd podcast website
- MIT Security Course on Youtube (Computer Systems **Security)**
- **Coursera (Software Security, Univ Maryland ?)**
- Books listed in syllabus
- Readings in syllabus
- Slides

(TAs and Tutors are not substitutes for missed lectures)

Participation

- Raise hand
  - Sound my not make it to my ear
- Anonymous Q&A
  - Q&A break to answer
  - Piazza post with questions and answer
  - Use slides numbers
- Community Notes

Accomodations

Subject: CSE 127 - [Name] Accommodation Request

Dear Prof. Munyaka,

Due to [thing] I need the following accommodation : [enter] .

I do[not] have an official letter coming your way.

Note - Provide the level of detail you believe is necessary and are comfortable sharing. I will ask for more details if needed. You are welcome to CC whoever you need to. However, keep in mind that the instructor rules reign supreme.

Missing Class

- You are not graded based on attendance
- Do not come to class sick
- If legitimately absent or need to miss exam, email instructor.
- This rule may change if the situation warrants it

How to email instructor…

Subject: CSE 127 - [Name] Experiencing Illness for Exam on [date]

Dear Prof. Munyaka,

I missed [event] on [date] due to [enter] and need the following accommodation : [enter]

Note - Provided the level of detail you believe is necessary. I will ask for more details if needed. You are welcome to CC whoever you need to. However, keep in mind that the instructor rules reign supreme.

Letters of Recommendation

- A or B in class
- No letter but a form to fill out or short paragraph
- I should know you beyond your performance in class if you want a full letter
- You are always welcome to ask me for it or strategize with me

Afterclass Questions

Due to time constraints, I can not answer questions right before or after class. Please use office hours, email, or other methods.

- Assistant Professor
  - Teach courses (x2)
  - Mentor students (x10)
  - Research
  - Manage research students
  - Participate in university committee
  - Conference duties
  - Outside service

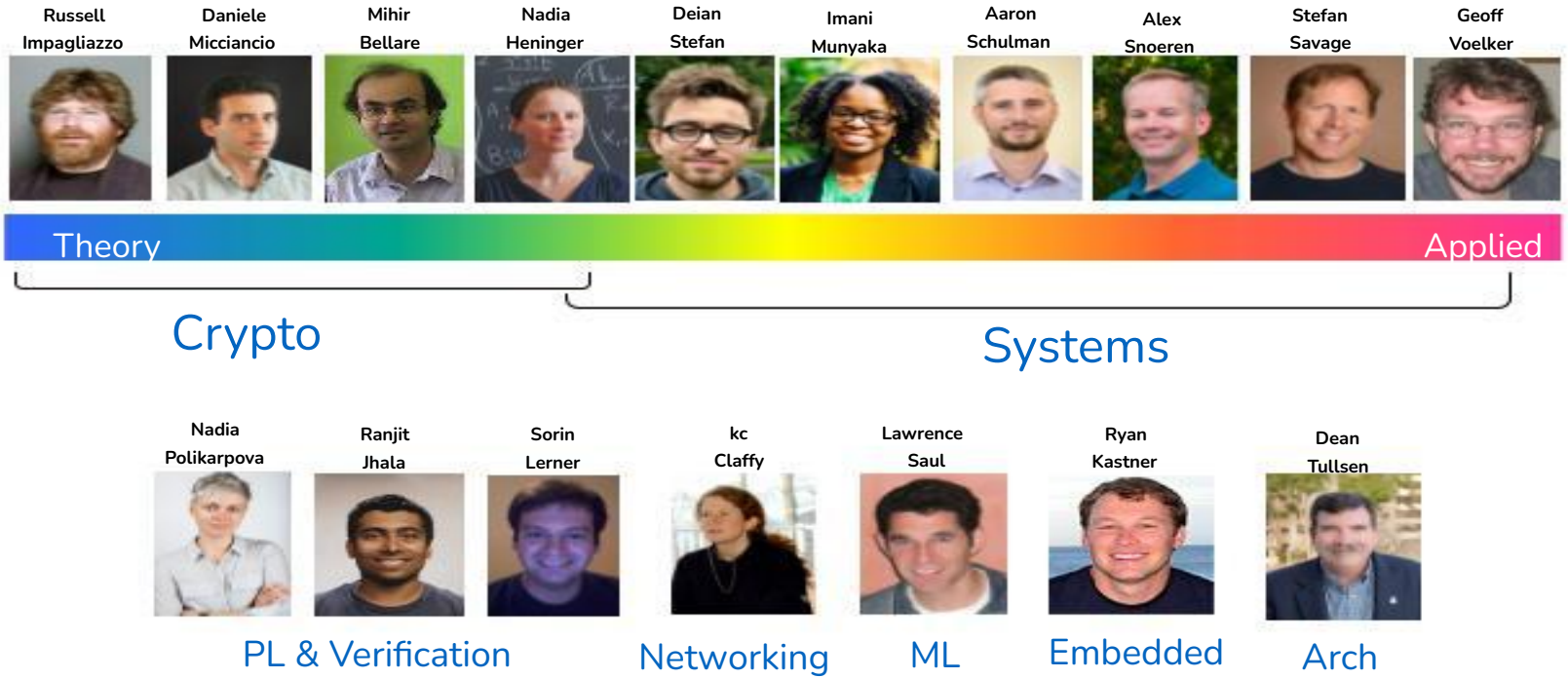
Instructor: Imani Munyaka

Email: drmunyaka@ucsd.edu

Office Hours: BRC and by appointment

- Office Hours Means…
  - My office is open
  - Time to network with instructor
  - Ask questions or get clarification
  - Open to everyone
  - Easy question: what habits would you suggests I adopt in order to do well in your class?what common mistakes do student make when approaching your class?

Many amazing folks at UCSD working on security



Ethics of Security

Ethics

We will be discussing and implementing real-world attacks.

Using some of these these techniques in the real world may be unethical, a violation of university policies, or a violation of federal law.

This includes the course assignment infrastructure (e.g., grading system).

Ethics

Be an ethical hacker

- Ethics requires you to refrain from doing harm
- Always respect human, privacy, property rights
- There are many legitimate hacking capture-the-flag competitions

Computer Fraud and Abuse Act

Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer…

Title 18 U.S. CODE § 1030 - FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS

Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer...

The punishment for an offense...

- a fine under this title or imprisonment for not more than one year, or both...,

- a fine under this title or imprisonment for not more than 5 years, or both... if—
  - (i) the offense was committed for purposes of commercial advantage or private financial gain;
  - (ii) the offense was committed in furtherance of any criminal or tortious act...; or
  - (iii) the value of the information obtained exceeds $5,000

CFAA Cases

- In 2011, FBI prosecuted weev for exposing data of 114K AT&T iPad users
  - Criminal CFAA charge
  - Found guilty and sent to prison; appeals court overturned ruling in 2014 on venue grounds

- In 2011, Sony sued George Hotz for jailbreaking PlayStation 3
  - Civil CFAA and DMCA complaints
  - Settled out of court

- In 2011, FBI prosecuted Aaron Swartz for downloading academic articles on MIT network from JSTOR
  - Indicted for wire fraud and CFAA
  - Prosecution continued until his death in 2013

- In 2021, Van Buren was charged with exceeding authorized access under CFAA
  - Police officer misused license plate database
  - Supreme court ruling (6-3) ruled that authorized access for improper purposes is not “exceeding authorized access”

What is security?

Menti.com use code 9791 9790

What is security

Protection of an asset

What makes it different from robustness?

What makes it different from robustness?

“Computer security studies how systems behave in the presence of *an adversary*.”

**Actively tries to cause the system to misbehave.*

The Security Mindset

- Thinking like an attacker
  - Understand techniques for circumventing security
  - Look for ways security can break, not why it won't

The Security Mindset

Thinking like an attacker

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

Thinking like a defender

- Know what you're defending, and against whom.
- Weigh benefits vs. costs:
- Rational paranoia

No system is ever completely secure.

Don't build bridges to sustain bombings

Thinking like an Attacker

- Look for weakest links
- Identify assumptions that security depends on
- Are they false?

Thinking like an Attacker

- Look for weakest links
- Identify assumptions that security depends on
- Are they false?
- Think outside the box

Thinking like an Attacker

- Look for weakest links
- Identify assumptions that security depends on

  Are they false?
- Think outside the box

  Not constrained by system designer’s worldview!

Thinking like an Attacker

- Look for weakest links
- Identify assumptions that security depends on
  Are they false?
- Think outside the box
  Not constrained by system designer's worldview!

Start practicing: When you interact with a system, think about what it means to be secure, and how it might be exploited.


1
2
3
4
5
6
7
8
9
*
0

Exercise

How would you break into the CSE building?

Exercise

How would you identify who was at a protest?

Exercise

How would you steal the email password of the dean?

Exercise

What security systems do you interact with?

Thinking like a Defender

- Security policy
  - What are we trying to protect?
  - What properties are we trying to enforce?
- Threat model
  - Who are the attackers? Capabilities? Motivation?
  - What kind of attack are we trying to prevent?
- Risk assessment
  - What are the weaknesses of the system?
  - What will successful attacks cost us?
  - How likely?
- Countermeasures
  - Costs vs. benefits?
  - Technical vs. nontechnical?

Security Policies

- What *assets* are we trying to protect?
  - Password (hashes)
  - Emails
  - Browsing history
- What properties are we trying to enforce?
  - Confidentiality
  - Integrity
  - Availability
  - Privacy
  - Authenticity

Threat Models

- Who are our adversaries?
  - Motives?
  - Capabilities?
- What kinds of attacks do we need to prevent?

  (Think like the attacker!)
- Limits: What kinds of attacks we should ignore?

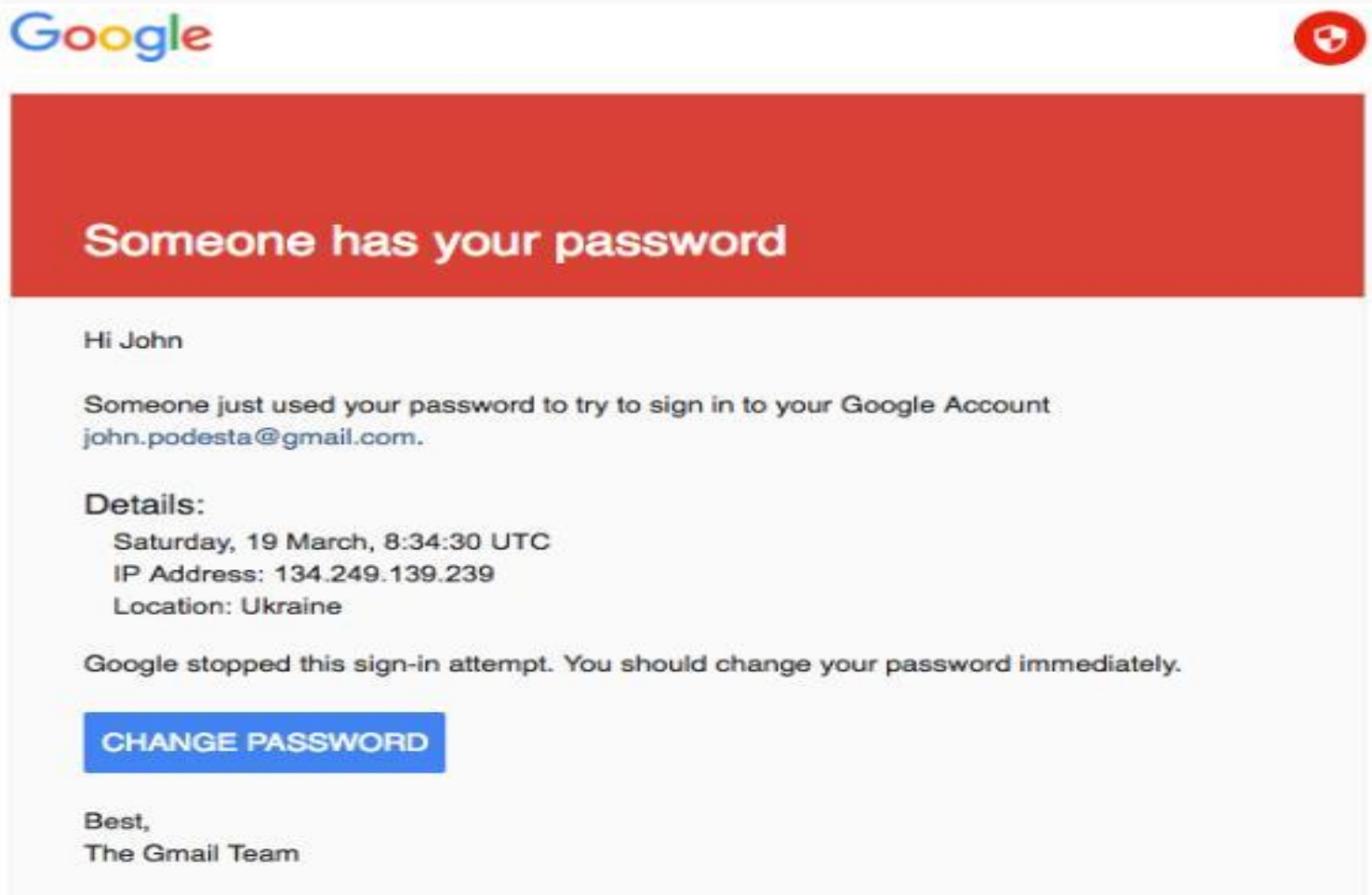
Example of Threat Modeling

Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	Magical amulets? Fake your own death, move into a submarine? YOU'RE STILL GONNA BE MOSSAD'ED UPON

Figure 1: Threat models

James Mickens "This World of Ours"

Example of Threat Modeling



Who is John Podesta?

Assessing Risk

Remember: *Controlled paranoia*

- What would security breaches cost us?
  - Direct costs: Money, property, safety, …
  - Indirect costs: Reputation, future business, well being, …
- How likely are these costs?
  - Probability of attacks?
  - Probability of success?

Countermeasures

- Technical countermeasures
- Nontechnical countermeasures
  Law, policy (government, institutional), procedures, training, auditing, incentives, etc.

How do we protect classified satellites?

Security Costs

No security mechanism is free

- Direct costs:
  Design, implementation, enforcement, false positives
- Indirect costs:
  Lost productivity, added complexity

Challenge is to rationally weigh costs vs. risk

- Human psychology makes reasoning about high cost/low probability events hard

Exercise

Should you lock your door?

- Assets?
- Adversaries?
- Risk assessment?
- Countermeasures?
- Costs/benefits?

Exercise

Should you use automatic software updates?

- Assets?
- Adversaries?
- Risk assessment?
- Countermeasures?
- Costs/benefits?

Exercise

Should we protect the CSE bear?

- Assets?
- Adversaries?
- Risk assessment?
- Countermeasures?
- Costs/benefits?

Secure Design

- Common mistake:
  Convince yourself that the system is secure

  Better approach:
- Identify *weaknesses* of design, focus on correcting them

  Formally prove that design is secure (soon)
- Secure design is a **process**

  Must be practiced continuously

  Retrofitting security is super hard

Where to focus defenses

- *Trusted components*

  Parts that must function correctly for the system to be secure.

  Attack surface
- Parts of the system exposed to the attacker

Security Principles

- Simplicity, open design, and maintainability
- Privilege separation and least privilege
- Defense-in-depth and diversity
- Complete mediation and fail-safe

Exercise

Preventing cheating on an online exam?

Exercise

Preventing you from stealing my password?

Next lecture: Buffer overflows!