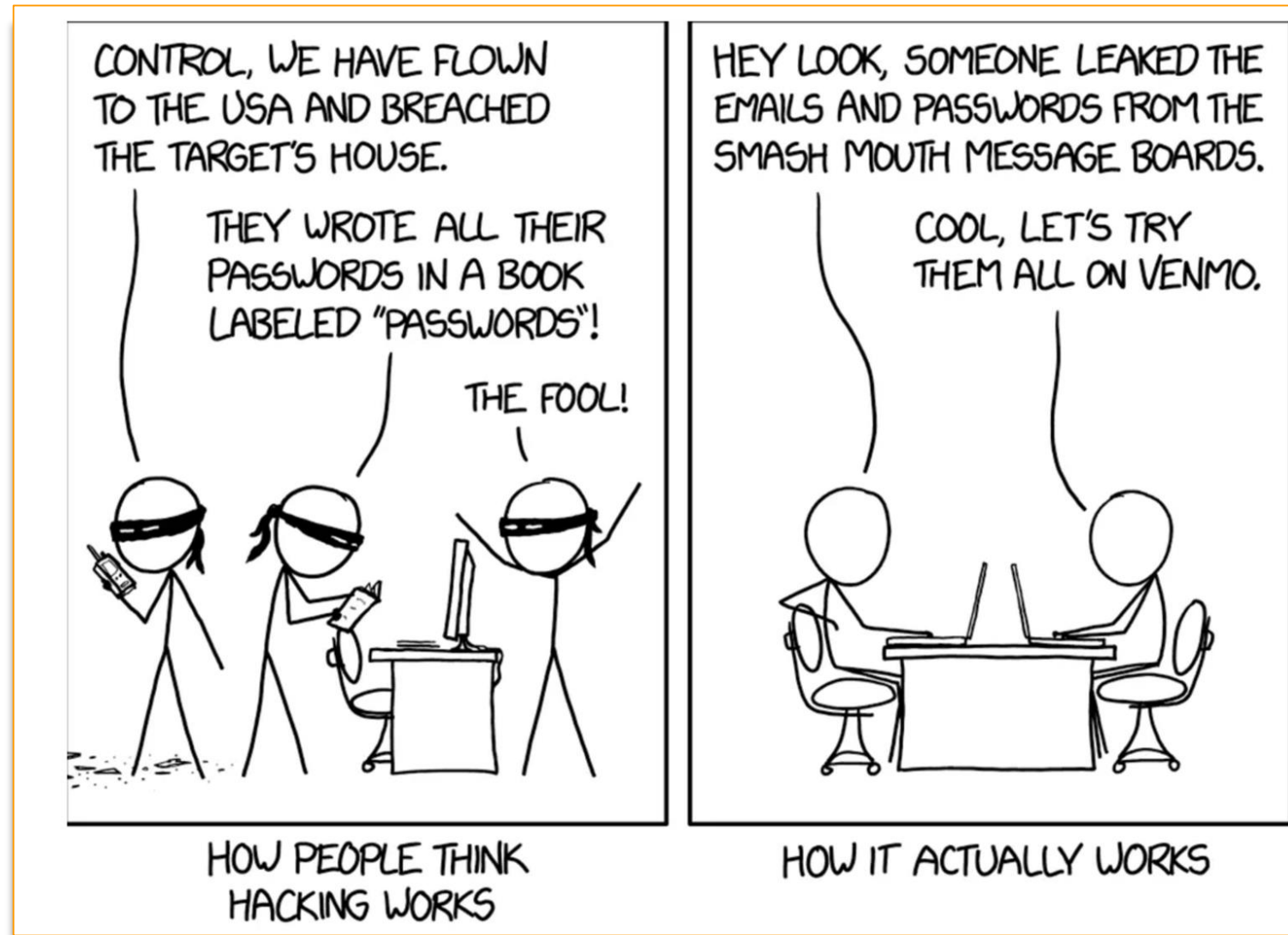


Introduction to Information Security (CS642)

Jan 21, 2020: Introduction

Earlence Fernandes
earlence@cs.wisc.edu



Source: xkcd

MOTHERBOARD

TECH BY VICE

Hackers Breach Forum Of Popular Webcomic 'XKCD'

The data breach affected 560,000 users.

By Lorenzo Franceschi-Bicchierai

Sep 3 2019, 10:35am



Share



Tweet

Team

Instructor

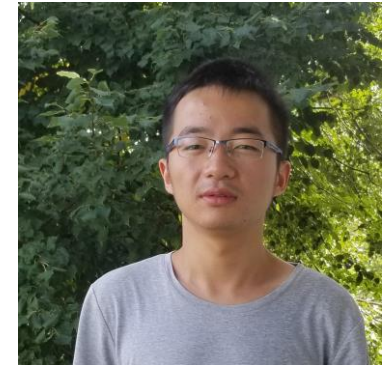


Earlence Fernandes

Teaching Assistants



Suleman Ahmad



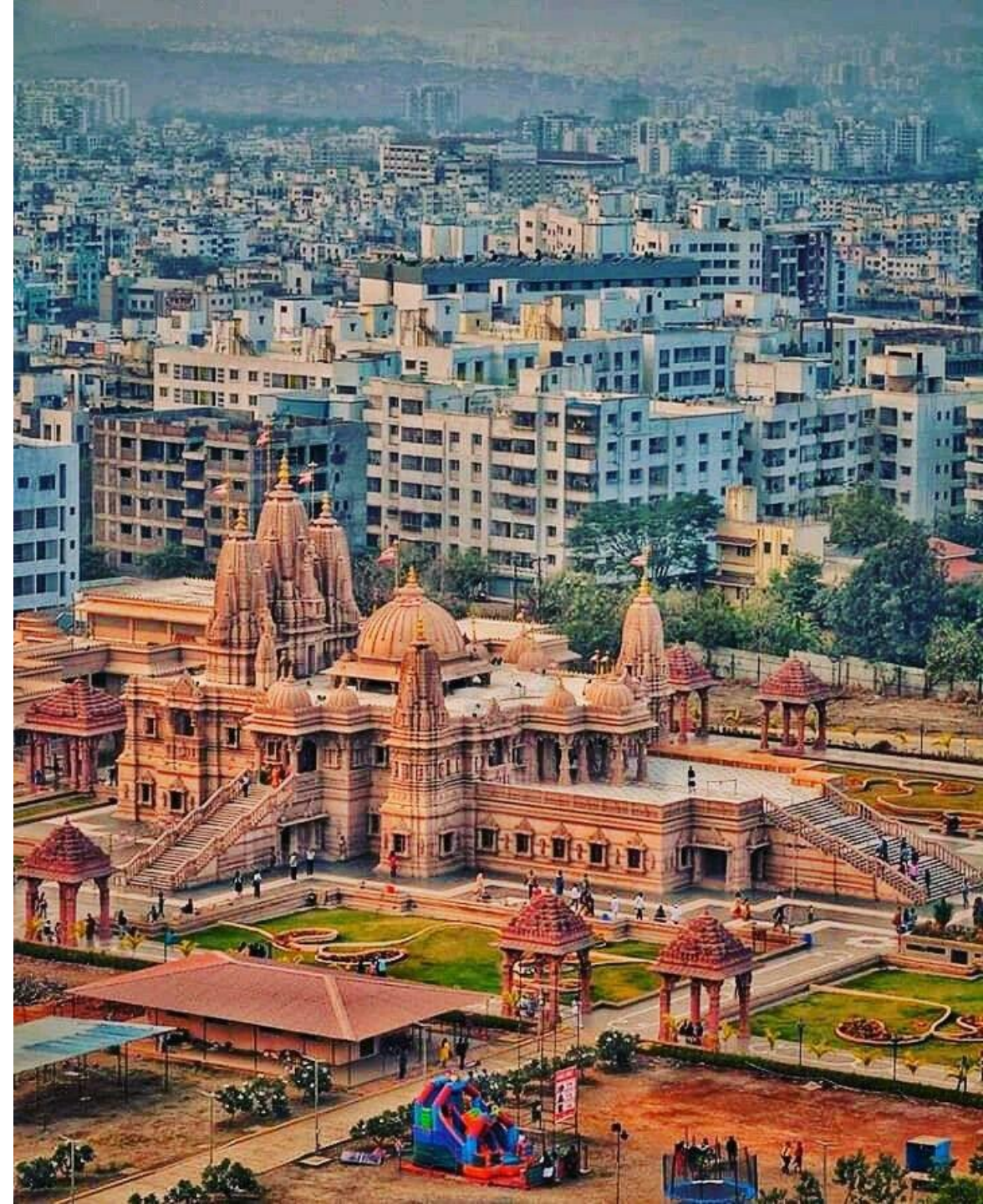
Zijun Ma

My background in pictures

Undergrad in CS



University of Pune



My background in pictures



Scientific Programmer



My background in pictures



PhD from

M UNIVERSITY OF
MICHIGAN

My background in pictures



Researcher at

W
UNIVERSITY *of*
WASHINGTON

My background in pictures



Assistant Professor



Research in computer security
for the physical world: homes,
cars, drones, planes, ...

Anything physical that
computers control

Today's Session

- Course goals and structure
- Logistics
- Areas of computer security: systems, networks, privacy, ...
- Some recent events in the security world

Goals for the Course

- Provide you with foundations in computer security and privacy
 - The security mindset
- Gain experience:
 - Evaluating the security of real systems
 - Building defenses
- Become a 1337 h4x0r, but an ethical one!



How the course is structured: Topics

Basic cryptography	Randomness, Symmetric Encryption, Modes of Operation, Public Key Crypto, Hashing
Software security	Buffer Overflows (and other memory corruption vulnerabilities), Fuzzing, Secure Coding
OS Security	Access Control, Process Isolation Model, Privilege Escalation, Confused Deputy Attacks
Network Security, Anonymity	TLS, Firewalls, Intrusion Detection, Tor
Web Security	SQL Injection, CSRF, XSS, HTTPS
Usability	How HCI matters in computer systems, how it matters for security and safety critical systems, user studies
Authentication	Passwords, Biometrics, Attacks on such systems
Mobile Security	Android security model, Permissions
Emerging Topics	IoT/CPS, Adversarial Machine Learning, Dare-I-Say Blockchain??

Pre-requisites

- Be comfortable with systems concepts: Operating Systems, microprocessor architecture, etc.
- Be comfortable with data structures and algorithms
- Be comfortable with a variety of programming languages: should be able to pick up new languages quickly
- Willingness to work hard

https://

CS 642: Intro to Information Security (Computer Security and Privacy, Spring 2020)

Time: Tuesdays and Thursdays, 11:00 am - 12:15 pm

Location: [Science Hall](#) 180

Instructor: [Earlence Fernandes](#) <earlence AT cs.wisc.edu>

Office Hours: CS 7387, Th 1:30 pm - 2:30 pm

Teaching Assistant: Suleman Ahmad < suleman.ahmad AT wisc.edu >

Office Hours: Mondays 1pm to 2pm, CS 4291

Teaching Assistant: Zijun Ma < zma96 AT wisc.edu>

Office Hours: Fridays 2pm to 3pm, CS 4XXX

Credits: 3.00 units

Canvas: <https://canvas.wisc.edu/courses/190368>

Mailing List: compsci642-1-s20@lists.wisc.edu

Prerequisites: Operating Systems, Data Structures and Algorithms, Experience with JS, Python, C/C++ (willingness to learn and work hard).

For more information, please use the navigation bar at the top of the page.

Logistics

Logistics

- Website + Canvas + Piazza
- Grades
 - Curved/Relative: no cap on number of grades
 - Grads, undergrads graded separately
- Graded Items
 - 5 Homeworks (10 points each): 50 points
 - 2 in-class midterms (20 points each): 40 points
 - Class participation (10 points)

Participate in discussion during session, or

Participate in online discussion on Piazza, or

Short presentation on Apr 28/30 on security topic of your choice

Timeline (tentative: for updates, see website)

Homework/Exam	Week	Release date	Due date
HW1	Week-2	Jan 30	Feb 13
HW2	Week-4	Feb 13	Feb 25
In-class Midterm-1	Week-8	Mar 10	
HW3	Week-8	Mar 12	Mar 24
HW4	Week-11	Apr 2	Apr 16
In-class Midterm-2	Week-13	Apr 23	
HW5	week-13	Apr 16	Apr 30* (last day of class)

* = this homework cannot be late

Office hours (Posted on Website)

Th 1:30 to 2:30 pm (to start with, then I'll experiment with a floating session)

Also I will use hangout (if you don't want to walk to the CS building)

- I will post the link on the website (once I figure out how to get a permalink in hangout)
- Email to schedule another time if the given time slots don't work

TA office hours: Suleman (CS 4291, Mondays 1-2), Zijun (CS 4XXX, Fridays 2-3)

Class discussions: Piazza

piazza.com/wisc/spring2020/sp20compsci642001

- Discuss current security incidents (extra credit)
- Get class participation points by participating in Piazza/Canvas
- Option to do class presentation to ensure full points in class participation
 - Talk to me if you are interested

Participate in class. Ask questions

Communication

- Class-wide announcements will come from
 - compsci642-1-s20@lists.wisc.edu
- Use my email for confidential issues
- Office hours

Meet the **ADVERSARY**

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

An intelligence that actively
tries to cause a system to
misbehave



Who does Computer Security?

- Academia
- Industry
- Military
- Hobbyists
- Bad Guys...

A Common Approach to Security

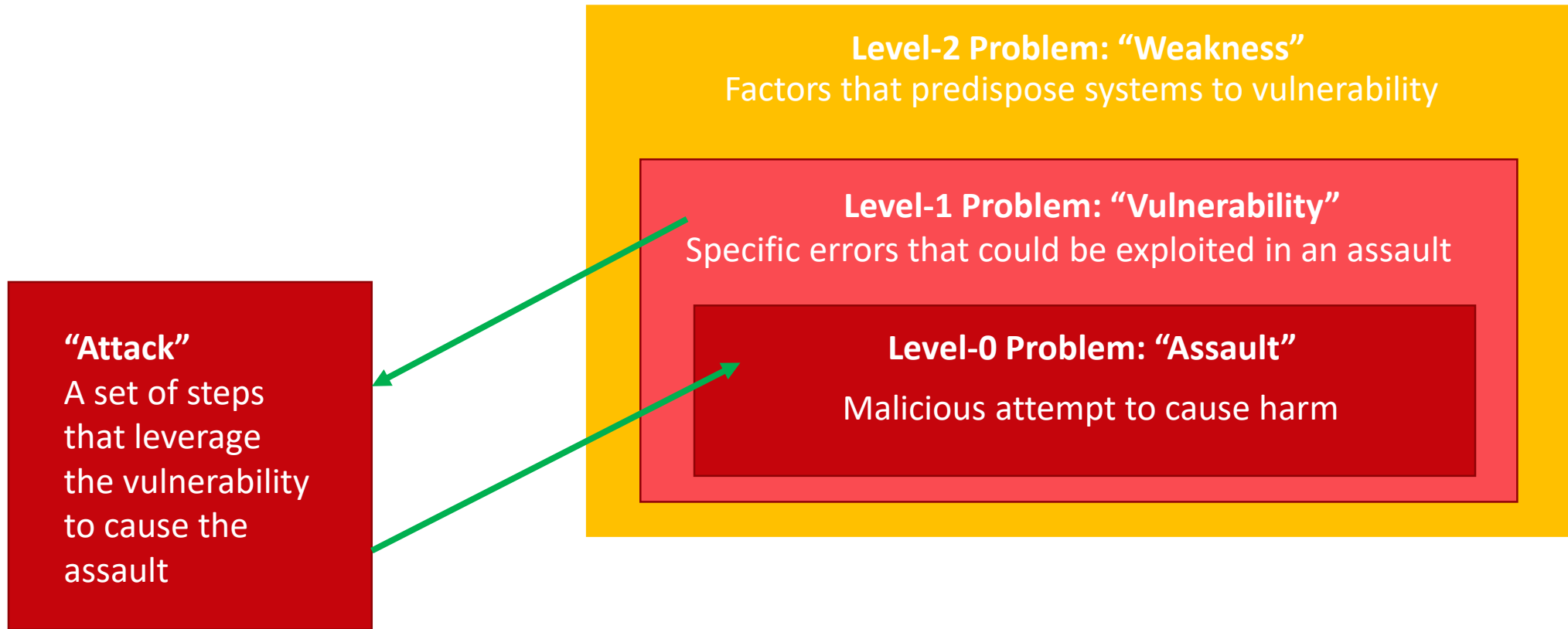


Is this a cat and mouse game?



What are ways to break this cycle?

Anatomy of an Attack



Why Study Attacks?

- Identify vulnerabilities so they can be fixed
- Create incentives for vendors to be careful
- Learn about new classes of threats (in new areas as well)
- Determine what we need to defend against
- Help designers build stronger systems
- Help users more accurately evaluate risk

What are attackers attacking?

The “CIA” Properties

- Confidentiality
- Integrity
- Availability

What are attackers attacking?

The “CIA” Properties

- Confidentiality

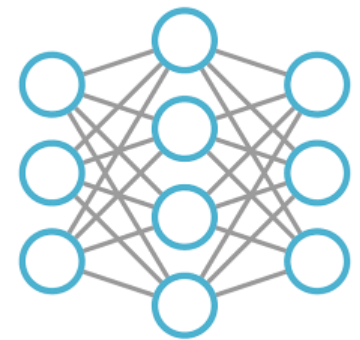
Protecting information from being accessed by unauthorized parties.

Once confidentiality is breached, it cannot be undone. Why?

Examples?

- Integrity

- Availability



Model Extraction Attacks, Training-set recovery

What are attackers attacking?

The “CIA” Properties

- Confidentiality

Protecting information from being accessed by unauthorized parties.

Once confidentiality is breached, it cannot be undone. Why?

- Integrity

- Availability

Privacy?

Use/disclose personal data according to some rules

Use my location, but ONLY for navigation

Anonymity?

Keep identity of participant hidden

Tor, Bitcoin, ...

Not the same as confidentiality

What are attackers attacking?

The “CIA” Properties

- Confidentiality
- Integrity
- Availability

Protecting information from being altered by unauthorized parties.



← → ↻ 🔒 amazon.com

ONLY protecting information alteration? Nothing else?



If it is 9pm, then close the door

Attacker steals credential, and opens door whenever they want!

What are attackers attacking?

The “CIA” Properties

- Confidentiality
- Integrity
- Availability

Information remains accessible to authorized users

Denial of Service Attacks



Are there other effects of availability attacks?



If 45 mins have elapsed, then turn off the oven

What does this look like in real life?

- Software bugs or design issues
- Hardware bugs or design issues
- Humans (social engineering)
- Unintended characteristics
 - (e.g., side channels, poor sources of randomness, ...)

Everything can be compromised.

There is no such thing as complete security.

Only degrees of security.

The Security Mindset

https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html

Schneier on Security



[Blog](#) [Newsletter](#) [Books](#) [Essays](#) [News](#) [Talks](#) [Academic](#) [About Me](#)

[Blog](#) >

The Security Mindset

Uncle Milton Industries has been selling ant farms to children since 1956. Some years ago, I remember opening one up with a friend. There were no actual ants included in the box. Instead, there was a card that you filled in with your address, and the company would mail you some ants. My friend expressed surprise that you could get ants sent to you in the mail.

I replied: "What's really interesting is that these people will send a tube of live ants to anyone you tell them to."

Search

Powered by *DuckDuckGo*

Go

☒ blog ☐ essays ☐ whole site

Subscribe



The Security Mindset

- Look for weakest links – easiest to attack
- Identify assumptions that security depends on. Are they false?
- Think outside the box: Not constrained by system designer's worldview. Practice thinking like an attacker:
 - For every system you interact with, think about what it means for it to be secure, and image how it could be exploited by an adversary

RATIONAL PARANOIA

Thinking like an attacker

- Breaking into the CS building
- Stealing my password
- Getting free beer on the terrace
- What are some security systems that you interact with in everyday life?



Thinking as a defender

- Security Policy

- What are we trying to protect? (i.e., assets)
- What properties are we trying to enforce? (CIA properties)

- Threat Model and Risk Assessment

- Who are the attackers? Capabilities? Motivations?
- What kind of attack are we trying to prevent?

- Countermeasures

- Cost vs. Benefit
- Technical vs. Non-technical

Threat Model

- Set of assumptions about the attacks that a security system is trying to protect against
- Important to consider before starting work on a defense
- Must be straightforward and reasonable. No “attackers will only attack on Tuesdays and Thursdays, after I kick my cat and spit on the ground”

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

BLAST! OUR
EVIL PLAN
IS FOILED!

NO GOOD! IT'S
4096-BIT RSA!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



This World of Ours

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)	<ul style="list-style-type: none">◆ Magical amulets?◆ Fake your own death, move into a submarine?◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON



James Mickens
Professor, Authority On All Things
Computer Science
Harvard School of Engineering & Applied Sciences



[Research](#) [Teaching](#) [Publications](#) [Wisdom](#)

[HOME](#) /

The Wisdom of James Mickens

James Mickens offers his timeless insights for free, because he loves you and he wants you to succeed. Please enjoy the undeniable masterpieces which are collected below.

Secure Design

- Common mistake:
 - Convincing yourself that the system is secure
- Better approach:
 - Identify the weaknesses of your system and focus on correcting them
- It's a process:
 - Must be practiced continuously; shouldn't be retrofitted

Where to Focus Defenses

- Trusted Components

- Parts that must function correctly for the system to be secure
- All security guarantees are rooted in the TCB

- Attack Surface

- Parts of the system exposed to the attacker (comes from threat modeling)

- Complexity and Obscurity

- Try to minimize moving pieces
- Common logic: complex systems with many moving pieces are more prone to failure

Some Recent Events in Computer Security

Attacks on DNA Sequencers



Attacks on Machine Learning Models

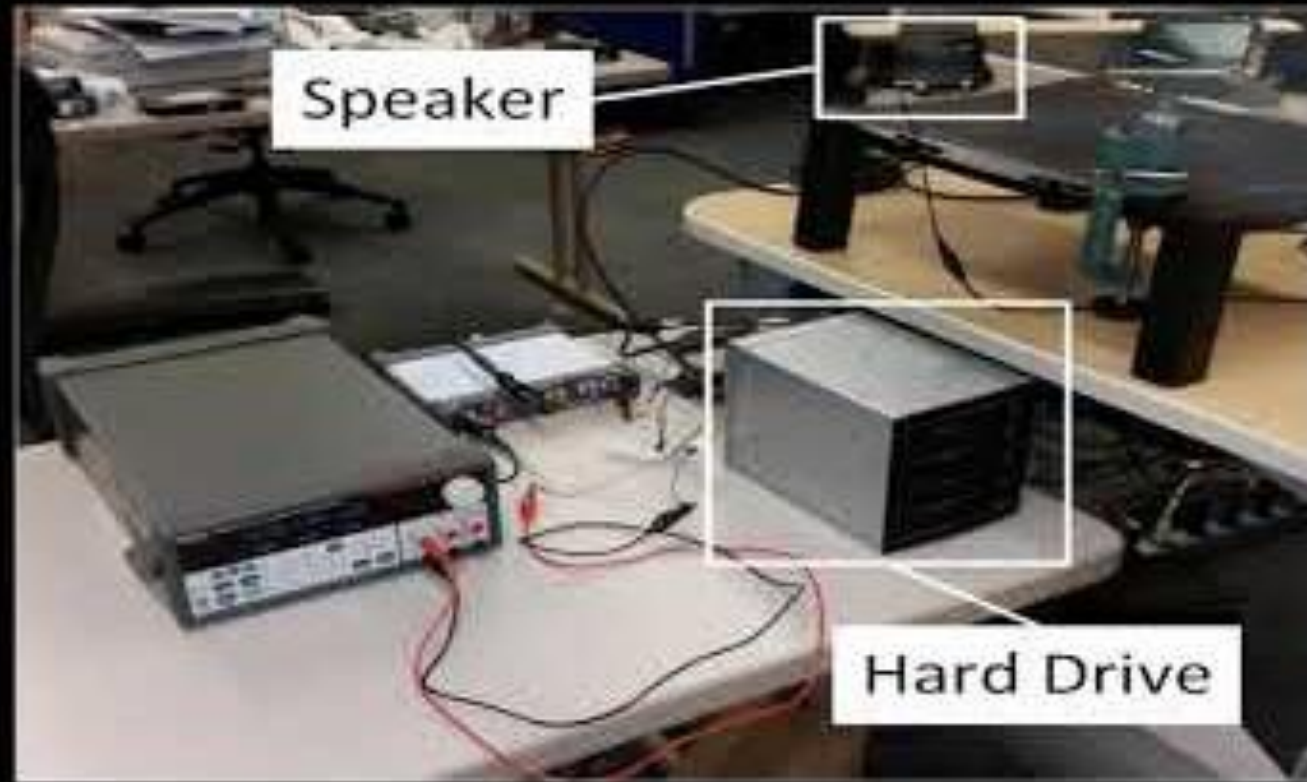


Attacks on Voice Assistants (Alexa, G-Home)



Attacks on Hard Drives

<https://www.youtube.com/watch?v=2EHQCuWI2jg>




speech through the hard drive. We evaluated this side-channel

Attacks on Kitchen Sinks?

SMART HOME

Kohler smart faucet brings voice commands to the kitchen sink

Ask your Kohler Sensate faucet to turn on the water, dispense 1 cup or fill your coffee pot. The kitchen sink just got smarter.

BY MOLLY PRICE  | AUGUST 6, 2019 4:30 AM PDT



Chris Monroe/CNET

Next class (Jan 23)

Basic cryptography

- Randomness, Historical Ciphers, Alice-Bob Setting

Law and Ethics

- Don't be evil!
 - Ethics requires you to refrain from doing harm
 - Always respect privacy and property rights
 - Otherwise you will fail this course!
- Federal/state law criminalize computer intrusion/wiretapping
 - E.g., Computer Fraud and Abuse Act (CFAA)
 - You can be sued or end up in jail
- University policies prohibit tampering with campus systems
 - You can be disciplined, even expelled
- Talk to me if you have questions

Introduction to Information Security (CS642)

Jan 21, 2020: Introduction

Earlence Fernandes
earlence@cs.wisc.edu

I don't like this title. It's wrong.

Modern computer security is more
than just "information security."

I'll try to get this course renamed.