EECS 388

Introduction to Computer Security

Welcome!
The Security Mindset

Today's Class

- Welcome!
- Goals for the course
- The Security Mindset
  - Thinking like an attacker
  - Thinking as a defender
- Course mechanics
- Ethics

Who are we?

Jeff Ringenberg

CSE Lecturer

Ph.D.

Email: jringenb@umich

Office: 2633 Beyster

Who are we?

Peter Honeyman

CSE Prof.

Princeton Ph.D.

Web: www.citi.umich.edu/u/honey/

Email: honey@umich

Office: 4777 Beyster

Twitter: @peterhoneyman

Who are we?

Kevin Fu

CSE Prof.

MIT Ph.D.

Web: web.eecs.umich.edu/~kevinfu/

Email: http://web.eecs.umich.edu/~kevinfu/contact.html

Office: 4628 Beyster

Steve Sprecher
swsprec@

Ben VanderSloot
benvds@

Alex Holland
ahollan@

Caroline Saab
ginasaab@

Rose Howell
rchowell@

Dean Robinson
dejoro@

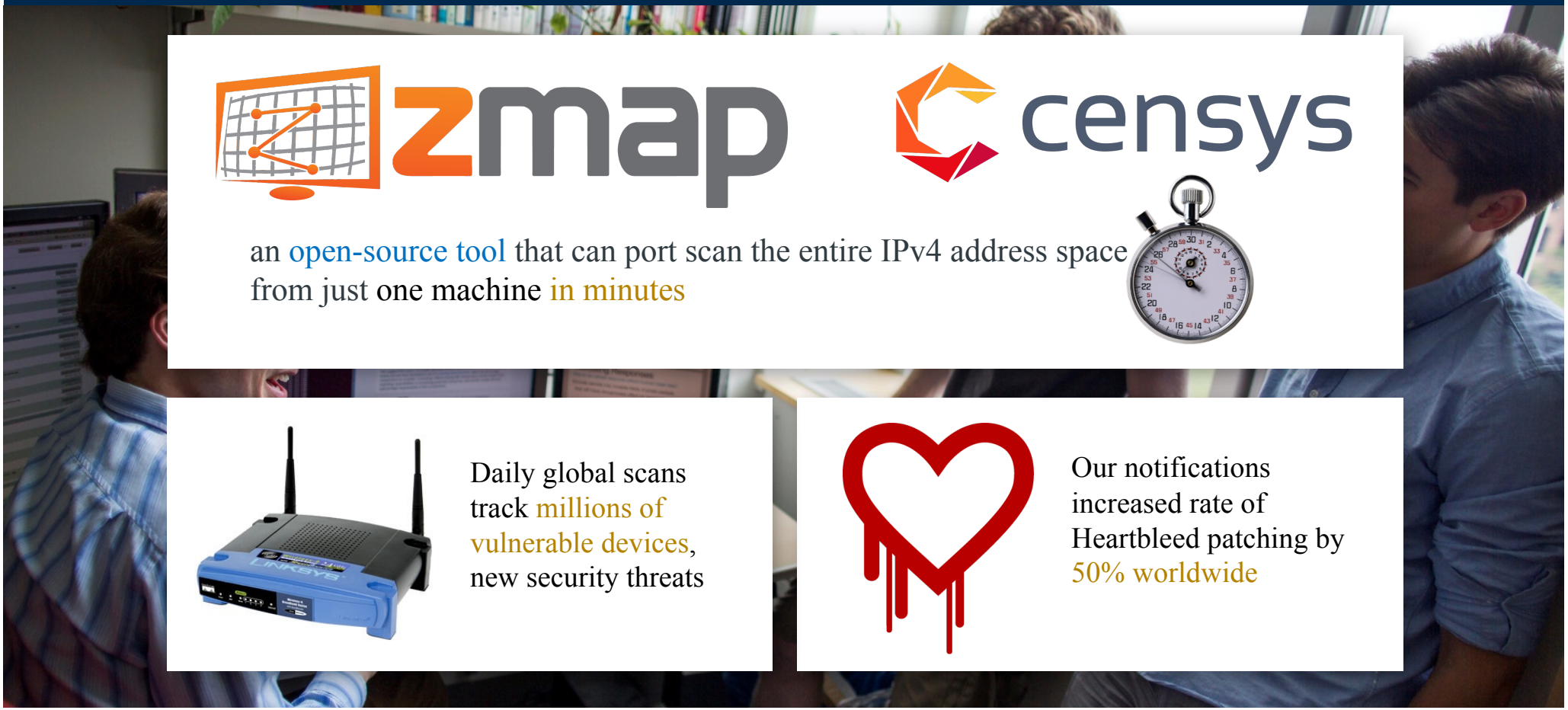
Rob Levy
roblevy@

Gabrielle Beck
becgabri@

Mel Savich
msavich@

Rebecca Lynch
lynchre@

Research on Internet-wide Security Intelligence



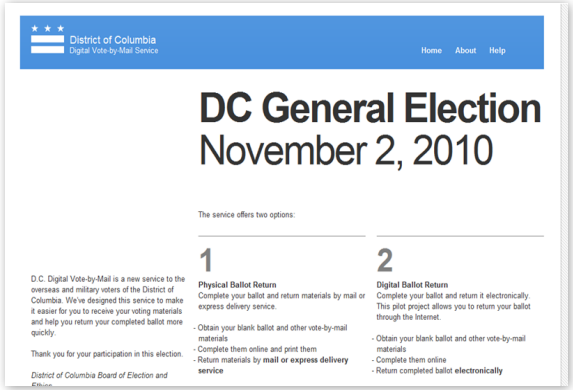
zmap censys

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

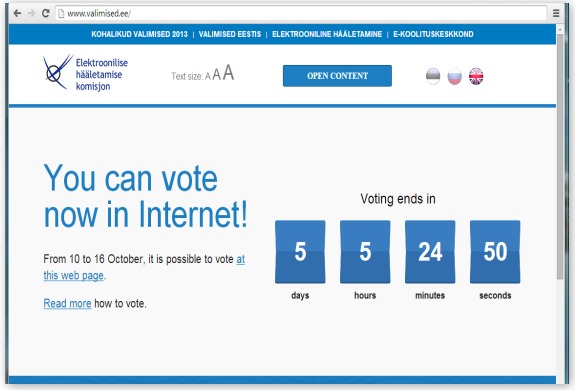
Research on Internet Voting



Washington, D.C.

First open-source online voting in U.S. general election

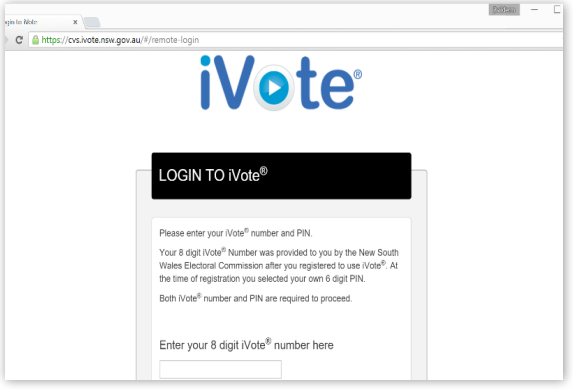
In public test, U-M team took <48 hours to change all votes



Estonia

Over 30% of Estonian voters cast their votes online

We showed that foreign powers could hack in and steal elections



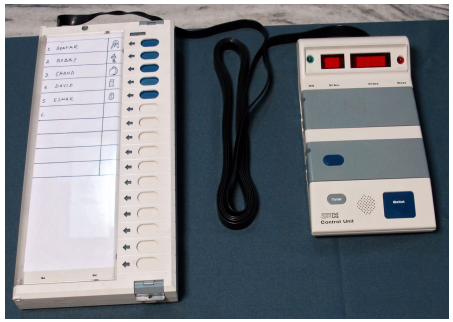
Australia

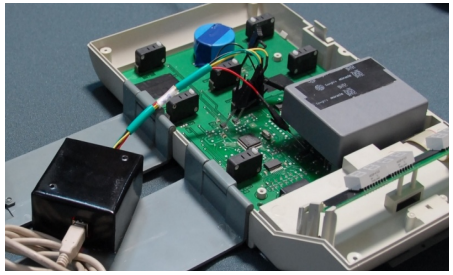
Largest-ever online election with 250,000 voters

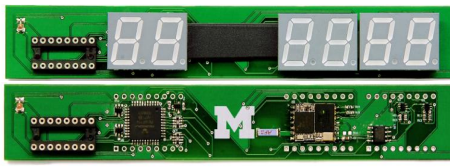
We reported flaws that could have altered the outcome

Research on Embedded Systems Security

Traffic Infrastructure

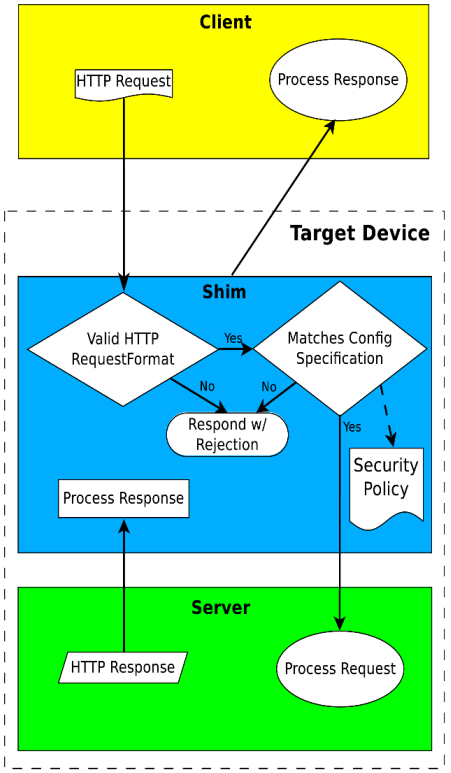






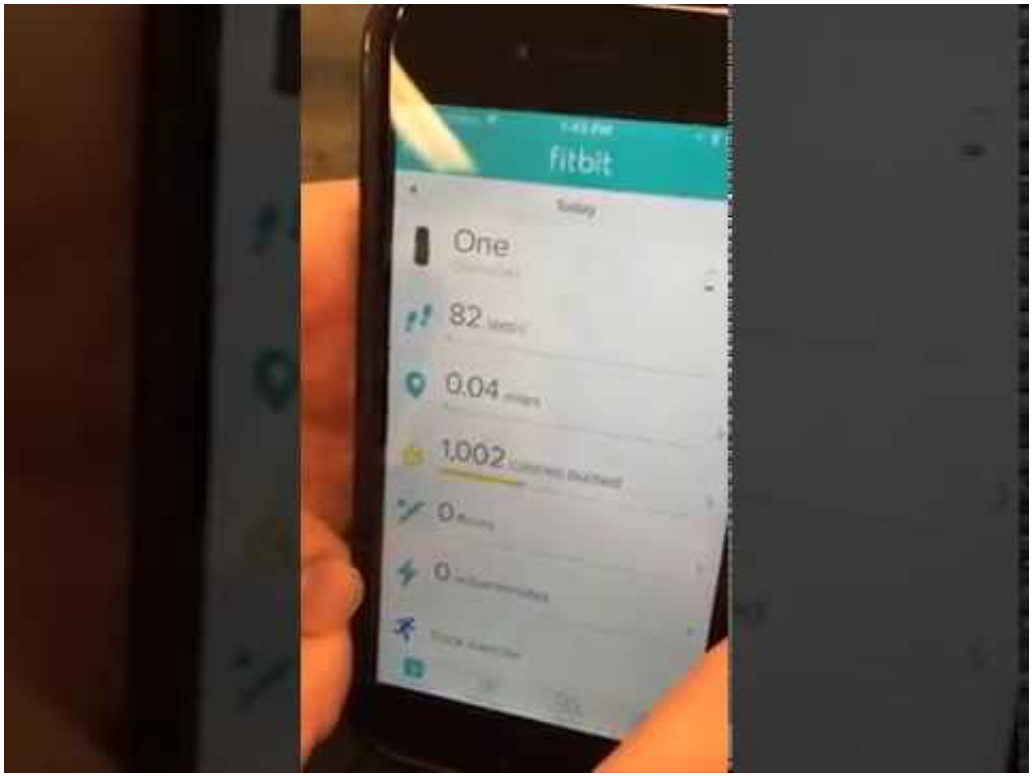
Voting Machines

TSA Airport Scanners



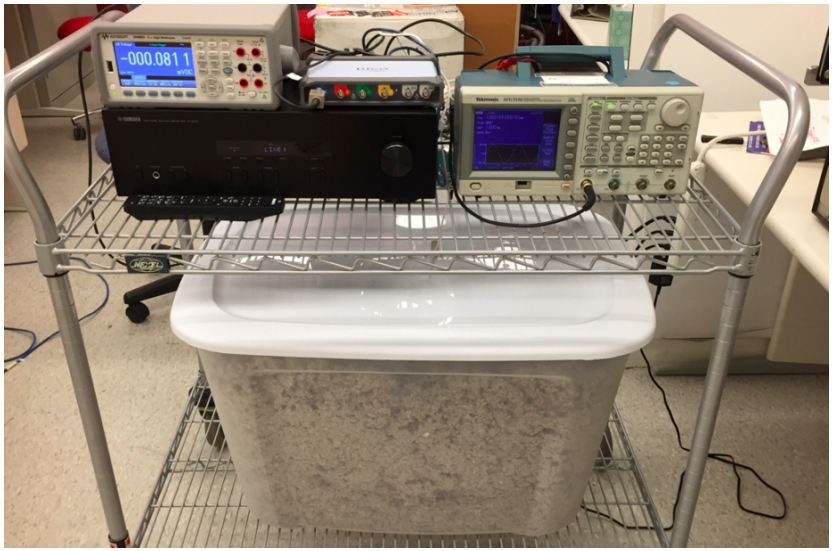
New Defenses

WALNUT: Acoustic Attacks on MEMS accelerometers



spqr.eecs.umich.edu/walnut

https://youtu.be/i_vvqELgBxk



Course Topics

The Security Mindset	Principles, threat modeling ...
Applied Cryptography	Public and private-key cryptography, digital signatures and authentication, hash functions, secure channels …
Internet Security	IP, TCP, routing, network protocols, web architecture, web attacks, Firewalls, intrusion detection
Application Security	Defensive programming, memory protection, sandboxing, virtual machines, buffer overflows, malware
Culture, Law, and Politics	Privacy, security and the law, digital rights management, voting, ethics...

Goals for this Course

- 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 program secure systems
- Learn to be a security-conscious citizen
- Learn to be a `1337 hax0r`, but an ethical one!

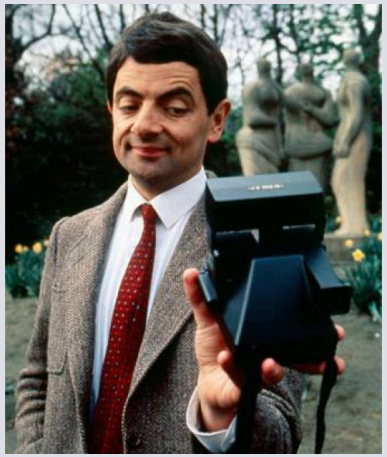
Getting to Know You

1. Meet two new people and learn their names.

2. Take a selfie and email it to us. Follow directions:

To: **eecs388-photos@umich.edu**

Subject: ***<your_uniqname>***



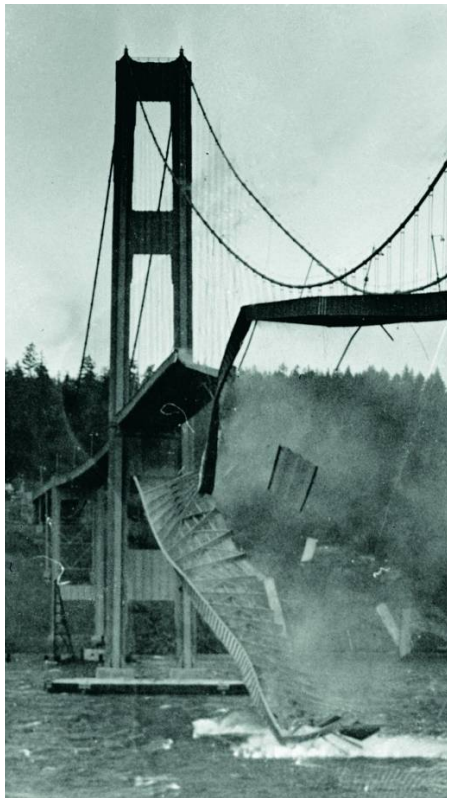
```
> What name should we call you?
> What's your year and major?
> Can you program in Python?
> In x86 asm?
> What would you like to learn in 388?
```

5 minutes. **Go!**

What is Computer *Security*?

- Math?
- Engineering?
- Philosophy?
- Natural Sciences?

What's the Difference?

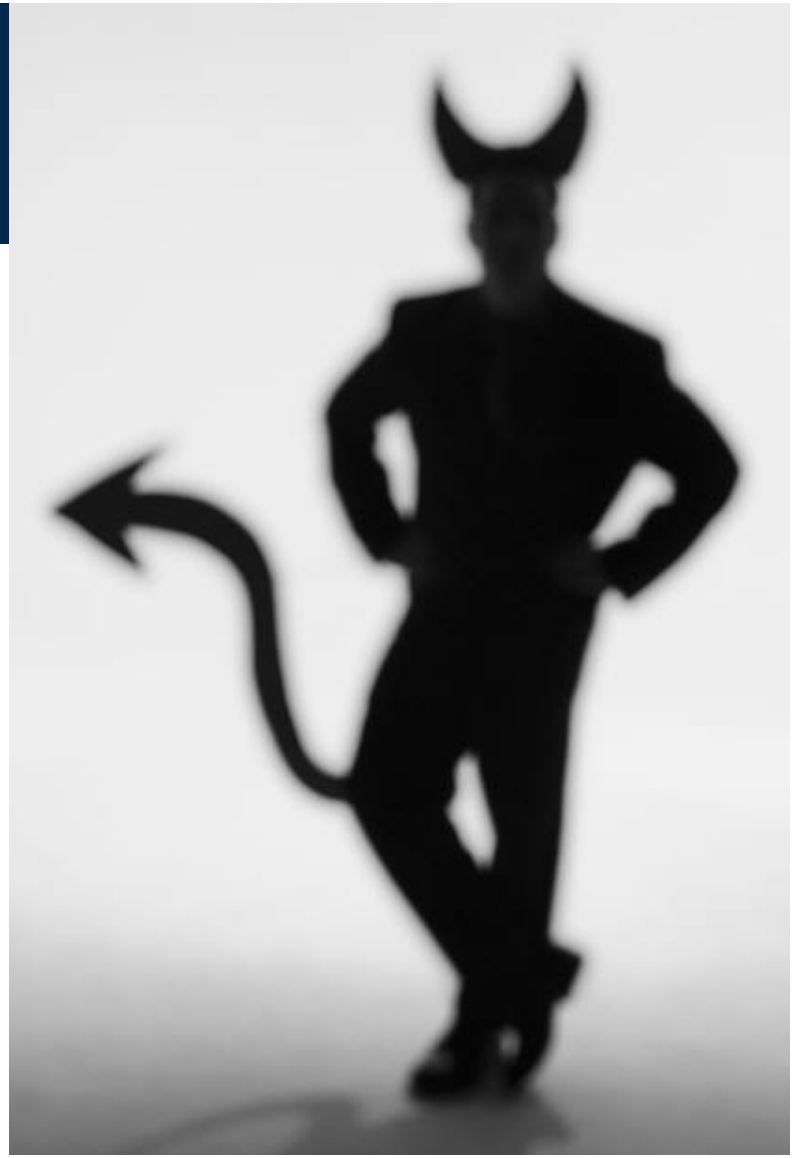


Meet the Adversary

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

The adversary
a.k.a. the attacker
a.k.a. the bad guy

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



“Know your enemy.”

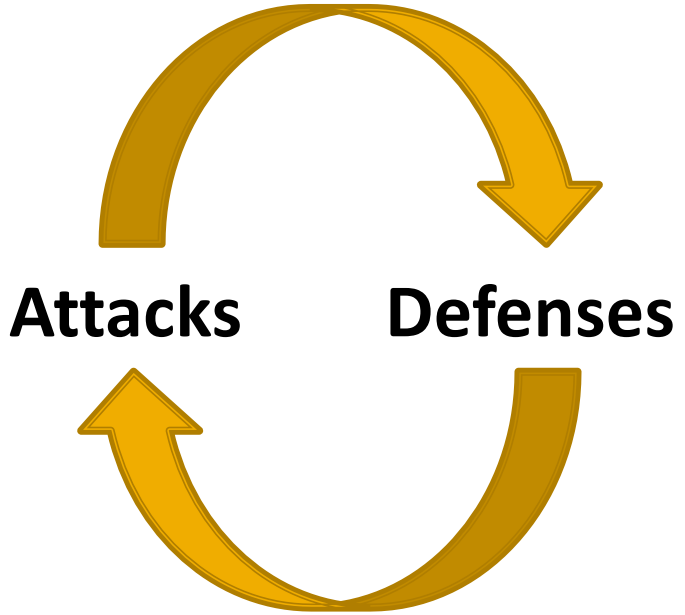
- Motives?
- Capabilities?
- Degrees of access?

The Security Mindset

- Thinking like an attacker
  - Understand techniques for circumventing security.
  - Look for ways security can break,
    not reasons why it won't.
- Thinking like a defender
  - Know what you're defending, and against whom.
  - Weigh benefits vs. costs:
    No system is ever completely secure.
  - "Rational paranoia!"

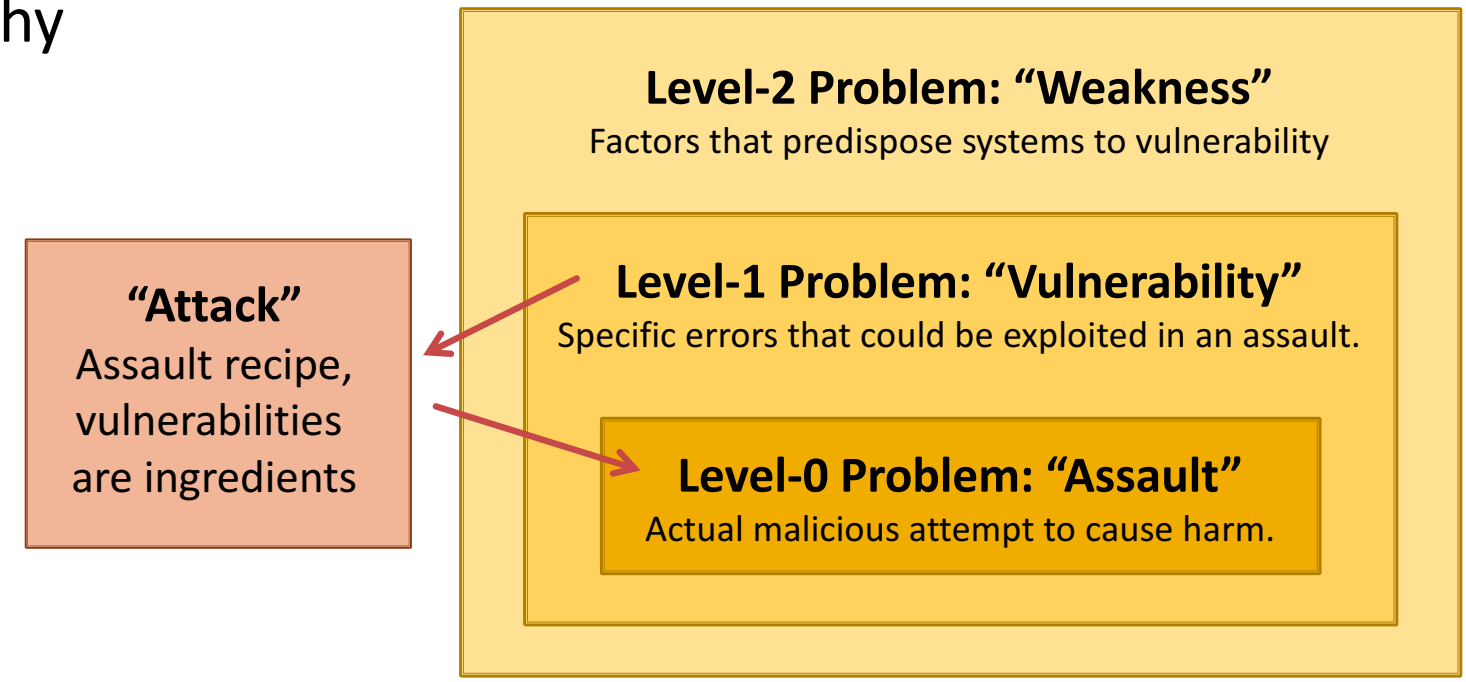
Why Study Attacks?

- Identify vulnerabilities to fix and determine a (new) defense.
- Create incentives for vendors to be careful in the future.
- Learn about new classes of threats.
- Help designers build stronger systems.
- Help users more accurately evaluate risk.



“Insecurity”?

Hierarchy



Thinking Like an Attacker

- 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.

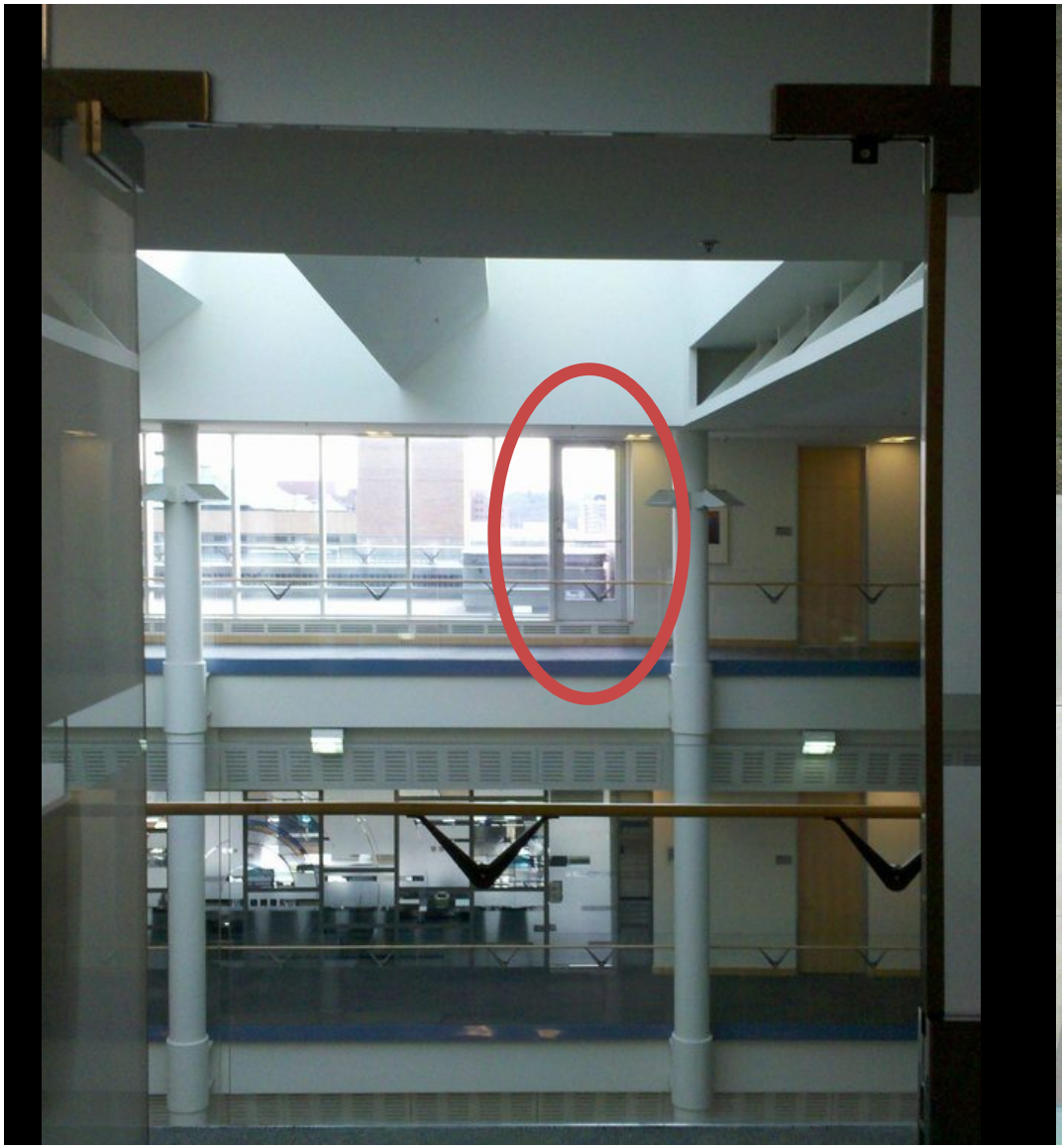
Practice thinking like an attacker:

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 attacker.

Exercises

- Breaking into the Beyster building?


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



Exercises

- What are some security systems that you interact with in everyday life?

Thinking as a Defender

- Security policy
  - What are we trying to protect?
  - What properties are we trying to enforce?
- Threat model
  - Who are the attackers? Capabilities? Motivations?
  - 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?

Challenge is to think rationally and rigorously about risk.

Rational paranoia.

Security Policies

- What *assets* are we trying to protect?
- 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: Kinds of attacks we should ignore?

Assessing Risk

Remember: *Rational* 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.

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

Exercises

- Should you lock your door?
  - Assets?
  - Adversaries?
  - Risk assessment?
  - Countermeasures?
  - Costs/benefits?

Exercises

- Using a credit card safely?
  - Assets?
  - Adversaries?
  - Risk assessment?
  - Countermeasures?
  - Costs/benefits?

Secure Design

- Common mistake:
  Trying to convince yourself that the system is secure
- Better approach:
  Identify the *weaknesses* of your design and focus on correcting them

- Secure design is a ***process***, not a product
  Must be practiced continuously; can't be retrofitted
- Try to provide ***defense-in-depth***

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

- Complexity vs. security?

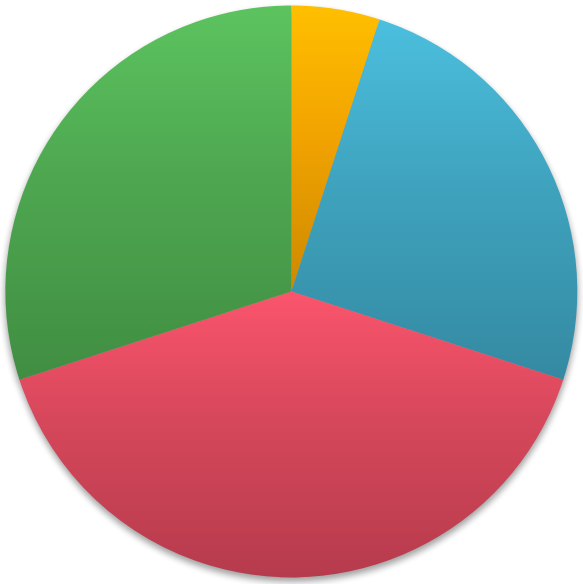
Security Testing

- Testing against requirements?
  - What are the right requirements?
- Adversarial testing
  - **Black box testing**
  - **White box testing**

Recall Goals for this Course

- 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 program secure systems
- Learn to be a security-conscious citizen
- Learn to be a `1337 hax0r`, but an ethical one!

Grading



- Class Participation (5%)
- Homework Exercises (25%)
- Programming Projects (40%)
- Final (30%)

Class Participation (5%)

Get points for:

- Coming to class and lab, speaking up, posting on Piazza
- Asking and/or answering questions
- Taking part in discussions
- Making intellectual contributions

Lose for:

- Being completely silent, frequently missing class, browsing the web, etc.

Homework Exercises (25%)

Five sets of exercises, done individually.
Problems or short written analysis.
Will be posted on course site.
Submit everything via Canvas (unless otherwise noted).

- Homework 1 available now, due September 14th, 6pm

Programming Projects (40%)

Five programming projects, working in pairs:

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

- Will be posted on course site
- May involve material ***not covered in lecture*** (but covered in lab)***.***
- Focus on learning techniques ***on your own*** which is important in security.
- Start early! Go to labs!

- Crypto Project available next week, due September 28th, 6pm

Lateness Policy

Our constraints:

Return graded work promptly.

Go over solutions in next day's discussion.

→ Strict lateness policy:

- 10% penalty for being late.
- Lose additional 10% every 5 hours.
- Can't accept work after 19.5 hours.
- Extensions in *extraordinary* circumstances only.

Please start early!

Collaboration Policy

- Encourage you to help each other learn. You may give or receive help on *concepts.* However, all work/code must be done by you/your team.
- Cheating is when you **give** or **receive** an unfair advantage.
  e.g., don't copy work from others
  e.g., don't post your solutions publicly
- Questions? Ask us.

- **No cheating!**
  (If we catch you cheating, we won't tell you until after the exam.)

Final Exam (30%)

Covers the entire course.

Review session earlier that week.

Practice exam will be released.

- The final exam is **Thursday, December 14th, 7-9pm**

Lectures

Come to lecture.

Take notes!

Slides will be posted to Canvas,
but videos available only in cases of excused absence.

Interrupt, ask questions, share stories.

Lab Sections

Go to lab.

Learn secure programming techniques,
vital information for completing projects,
detailed reviews of completed assignments.

- First labs this week

Communication

https://**eecs388.org** ..... *overview, schedule, assignments*

Piazza ..... *questions, discussion, announcements*

Canvas/Gradescope ..... *assignment submission and grading*

eecs388-staff@umich.edu ..... *administrative issues*

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 the course.
- Federal/state laws criminalize computer intrusion, wiretapping.
  - e.g., Computer Fraud and Abuse Act (CFAA)
  - You can be sued or go to jail.
- University policies prohibit tampering with campus systems.
  - You can be disciplined, even expelled.

Coming Up

Next Lecture …

Intro to Crypto
Alice and Bob,
Kerckhoffs's principle,
hashes and MACs

Next two weeks …

Applied Crypto
randomness, encryption,
key exchange, secure channels