EECS 588

Computer and Network Security

Introduction

January 12, 2016

Alex Halderman

Today's Class

- Welcome!
- Goals for the course
- Topics, what interests you?
- Introduction to security research
- Components of your grade
- Legal and ethical concerns

Who am I?

J. Alex Halderman

CSE Prof.

Web: https://jhalderm.com

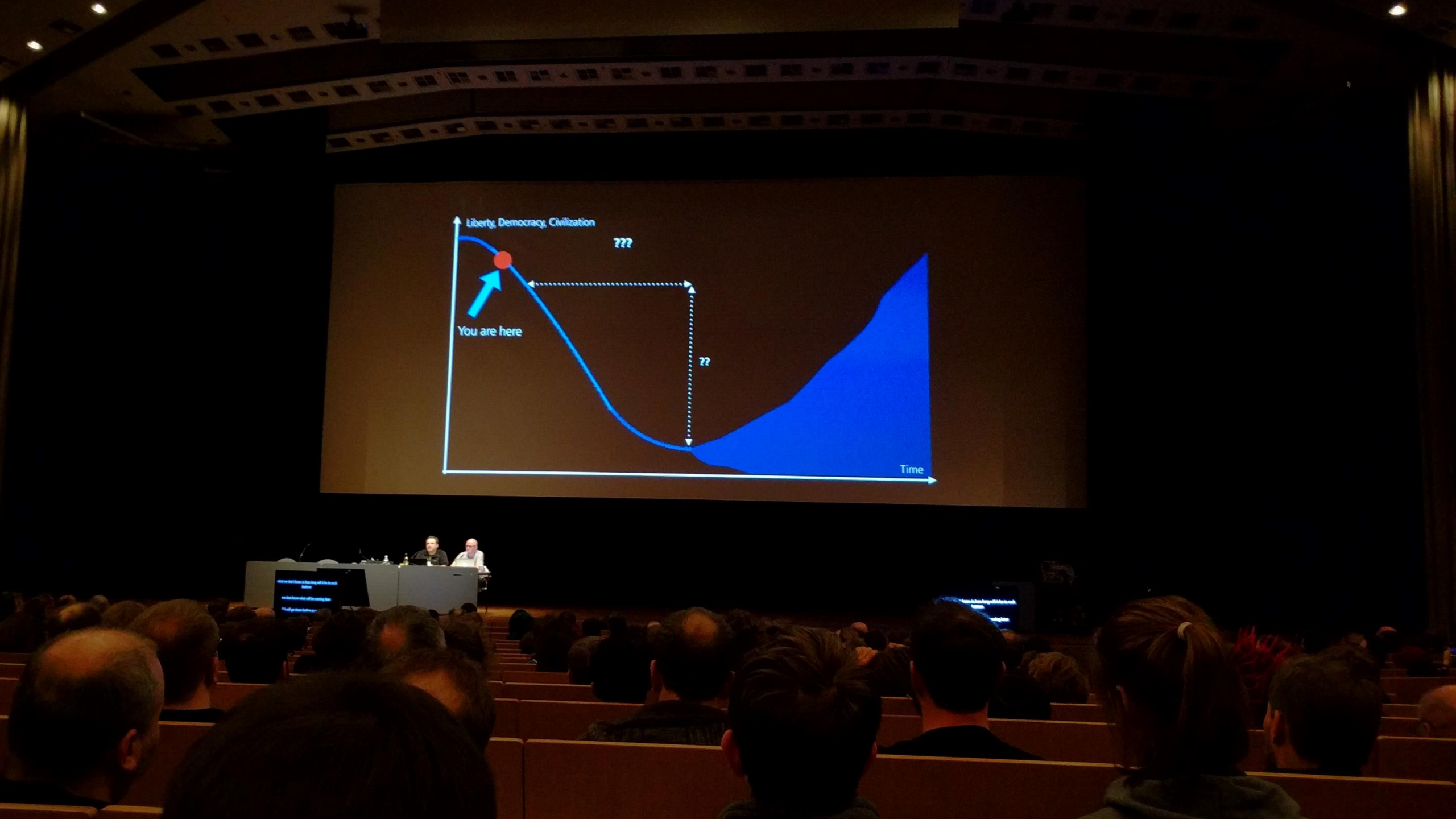
Email: jhalderm@eecs

Office: 4717 Beyster

Hours: TuTh 3:30-4:30
or by appointment

Mobile: 609-558-2312

How I spent my winter vacation


Liberty, Democracy, Civilization
???
You are here
??
Time

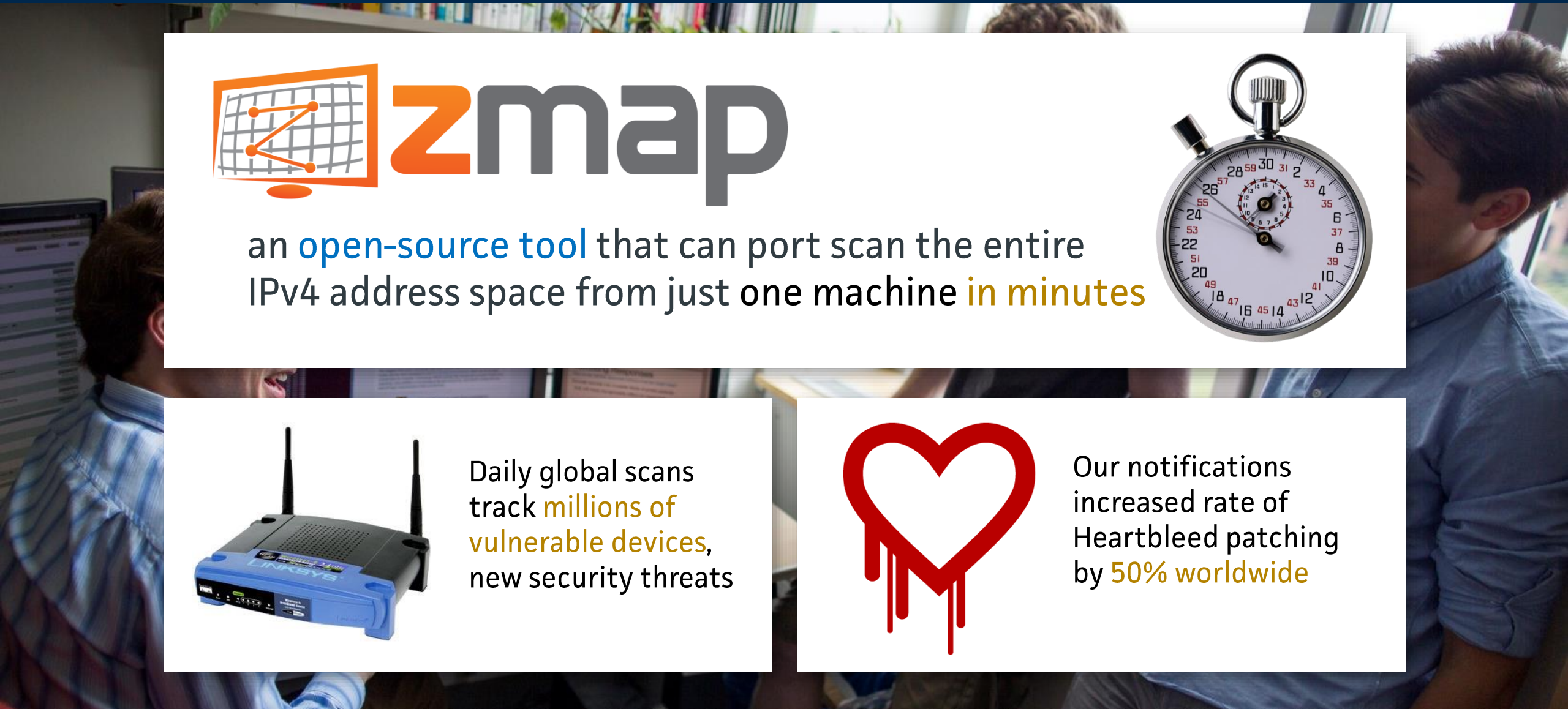
How I spent my winter vacation


JAZZ


SCHALL
RUGBY


Qualitätsfeuerwerk für zündende Begeisterung
Feuerwerk
ab dem 29. Dezember
www.pyro-partner.de
art
Gesichter des Pop
GEO EPOCHE PANORAMA
ZWEITE WELTKRIEG
FR
MONOCLE
OUR GLOBAL ADVENT ADVENTURE
Cicero
29,

My Work: 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

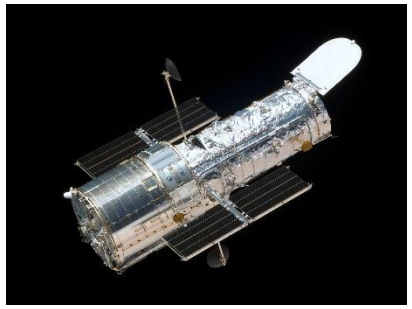
Our notifications increased rate of Heartbleed patching by 50% worldwide

My Work: 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 Security

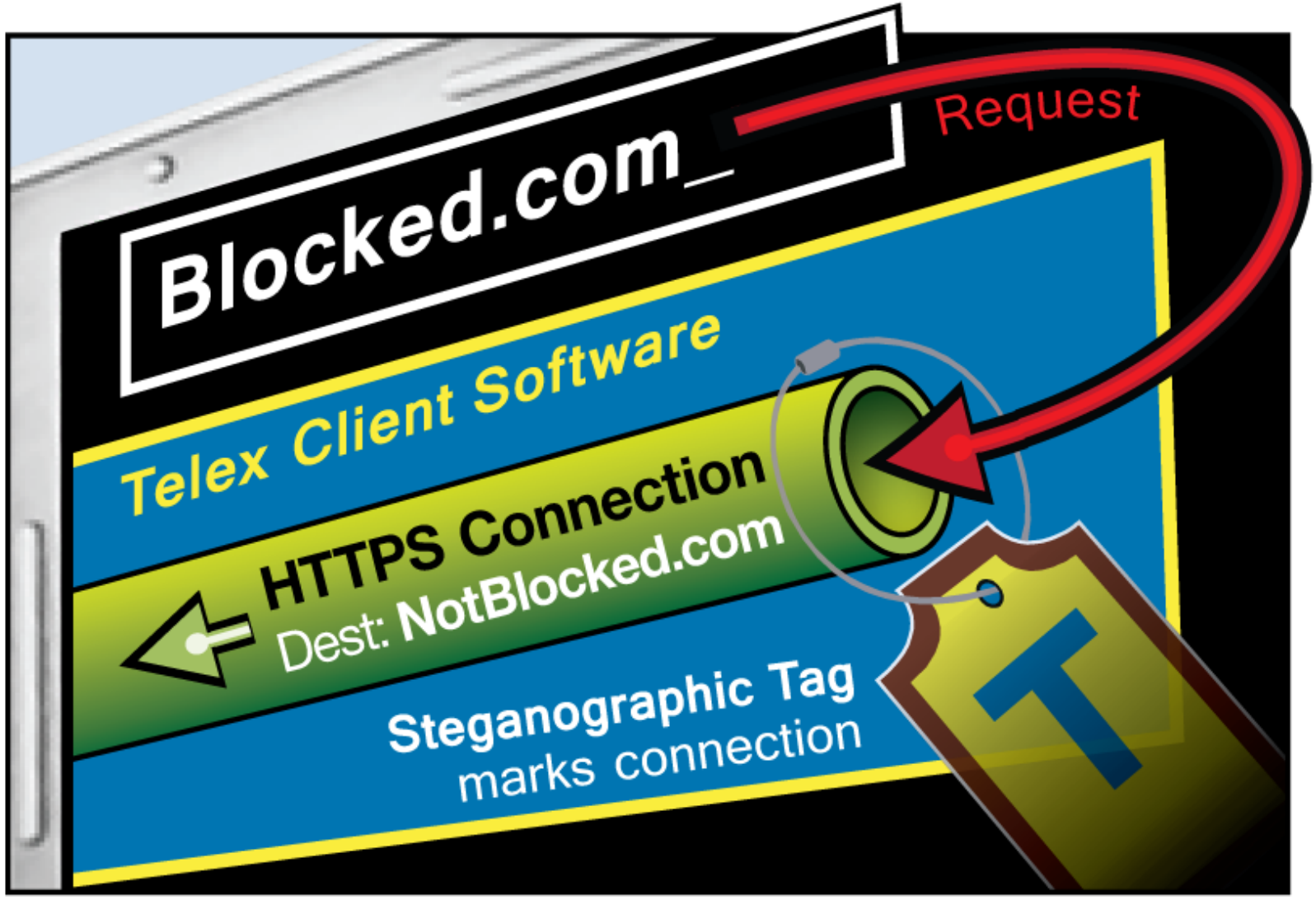
new TLS attack threatens 8% of the web,
NSA might tap 66% of VPNs using HPC

Highest-rated Submission, *ACM CCS 2015*

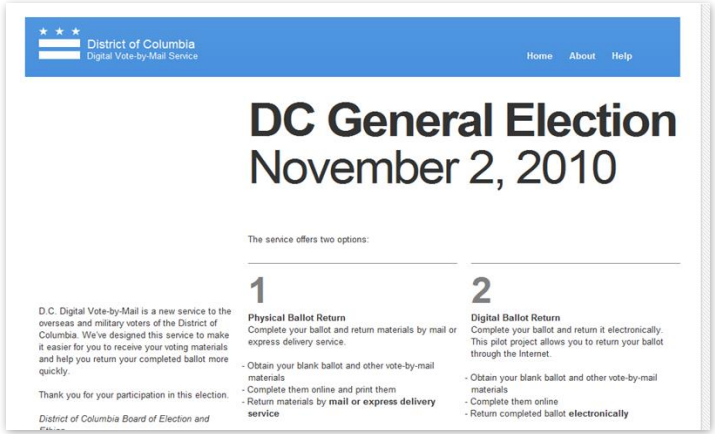
My Work: Encrypting the Entire Web

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

My Work: Censorship Resistance



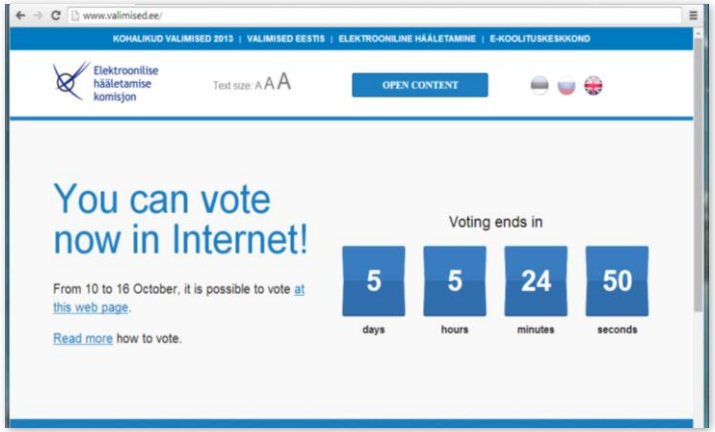
My Work: Internet Voting



Washington, D.C.

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

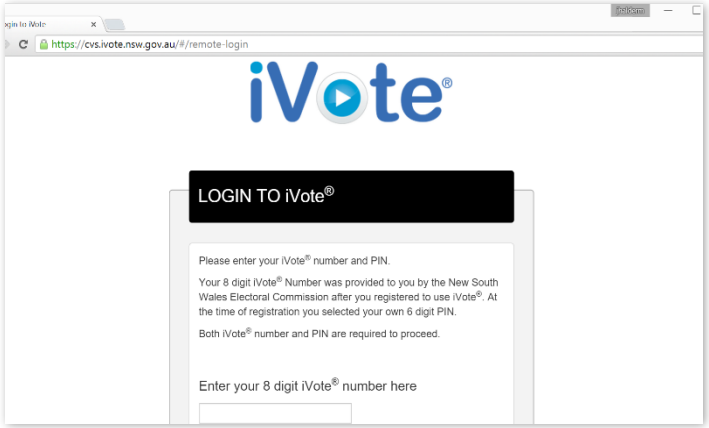
In public test, U-M team took <48 hours to change all votes



Estonia

Over 30% of Estonian voters cast their votes online

We showed that foreign powers could hack in and steal elections



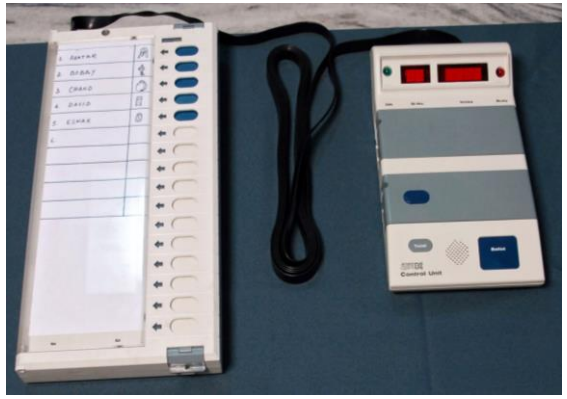
Australia

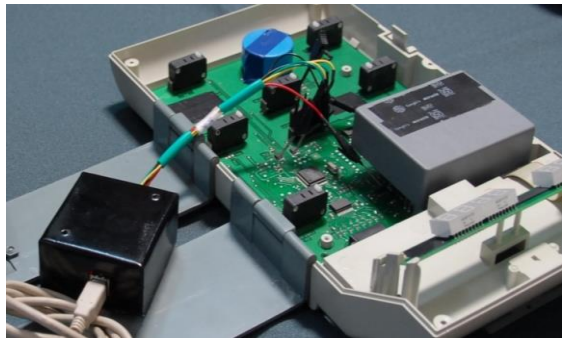
Largest-ever online election with 250,000 voters

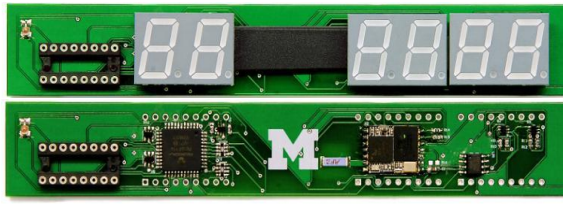
We reported flaws that could have altered the outcome

My Work: Embedded Systems Security

Traffic Infrastructure

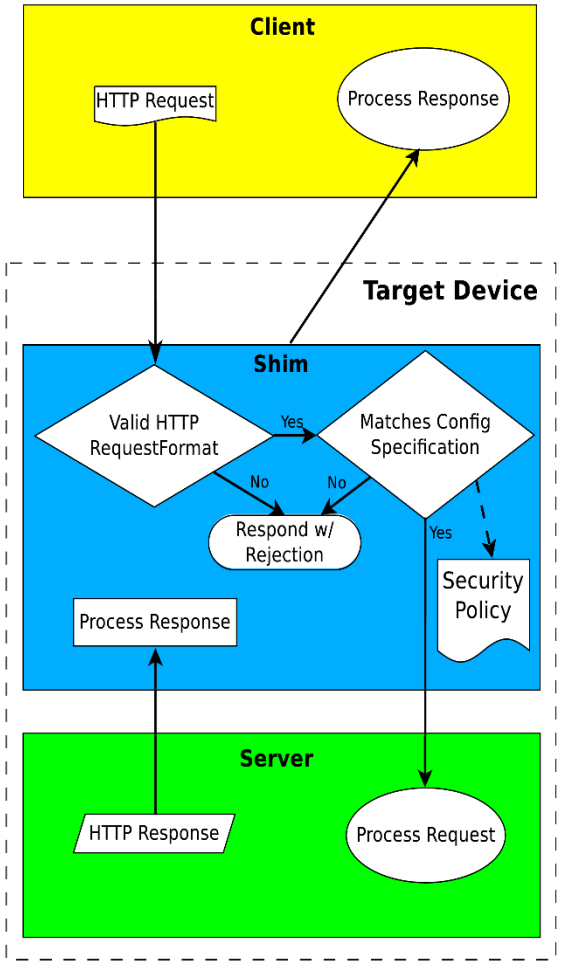






Voting Machines

TSA Airport Scanners



New Defenses

Goals for this Course

- Gain hands-on experience
  - Building secure systems
  - Evaluating system security
- Prepare for research
  - Computer security subfield
  - Security-related issues in other areas
- Generally, improve research, writing, and presentation skills
- Learn to be a `1337` `hax0r`, but an ethical one!

Getting In, Getting an A

Waitlist?

Prereqs:

EECS482 or EECS489 or grad standing

We'll grant everybody overrides, but can't guarantee hard work will bring success, unless you have the prerequisites.

EECS 588: Computer and N ×

https://www.eecs.umich.edu/courses/eecs588/

Computer & Network Security

EECS 588 – Winter 2016

Professor: J. Alex Halderman
Office hours: TuTh 3:30–4:30, 4717 Beyster, or by appointment

Credits: 4. This course counts towards meeting software quals requirements.

Prerequisites: EECS 482 Operating Systems, EECS 489 Networking (recommended), or grad standing. Success in this course requires a mature understanding of software systems.

Lectures: TuTh 1:30–3:30, 1690 Beyster

GSI: Travis Finkenauer (4828 Beyster, meetings by appointment)

Forum: We'll use Piazza for online discussion and announcements.
For administrative issues, email eecs588@umich.edu.

Resources
Security Research at Michigan
Security Reading Group
CSE CTF Club

This intensive research seminar covers foundational work and current topics in computer systems security. We will read research papers and discuss attacks and defenses against operating systems, client-side software, web applications, and IP networks. Students will be prepared for research in computer security and for security-related research in other subareas, and they will gain hands-on experience designing and evaluating secure systems.

Building Blocks
The security mindset, thinking like an attacker, reasoning about risk, research ethics
Symmetric ciphers, hash functions, message authentication codes, pseudorandom generators
Key exchange, public-key cryptography, key management, the SSL protocol

Software Security
Exploitable bugs: buffer overflows and other common vulnerabilities – attacks and defenses
Malware: viruses, spyware, rootkits – operation and detection
Automated security testing and tools for writing secure code
Virtualization, sandboxing, and OS-level defenses

Web Security
The browser security model
Web site attacks and defenses: cross-site scripting, SQL injection, cross-site reference forgery
Internet crime: spam, phishing, botnets – technical and nontechnical responses

Network Security
Network protocols security: TCP and DNS – attacks and defenses
Policing packets: Firewalls, VPNs, intrusion detection
Denial of service attacks and defenses
Data privacy, anonymity, censorship, surveillance

Advanced Topics
Hardware security – attacks and defenses
Trusted computing and digital rights management
Electronic voting – vulnerabilities, cryptographic voting protocols

Getting to Know You

- Who are you?
- What topics interest you?
- What would you like to learn in this course?

What is Computer *Security*?

Math?

Engineering?

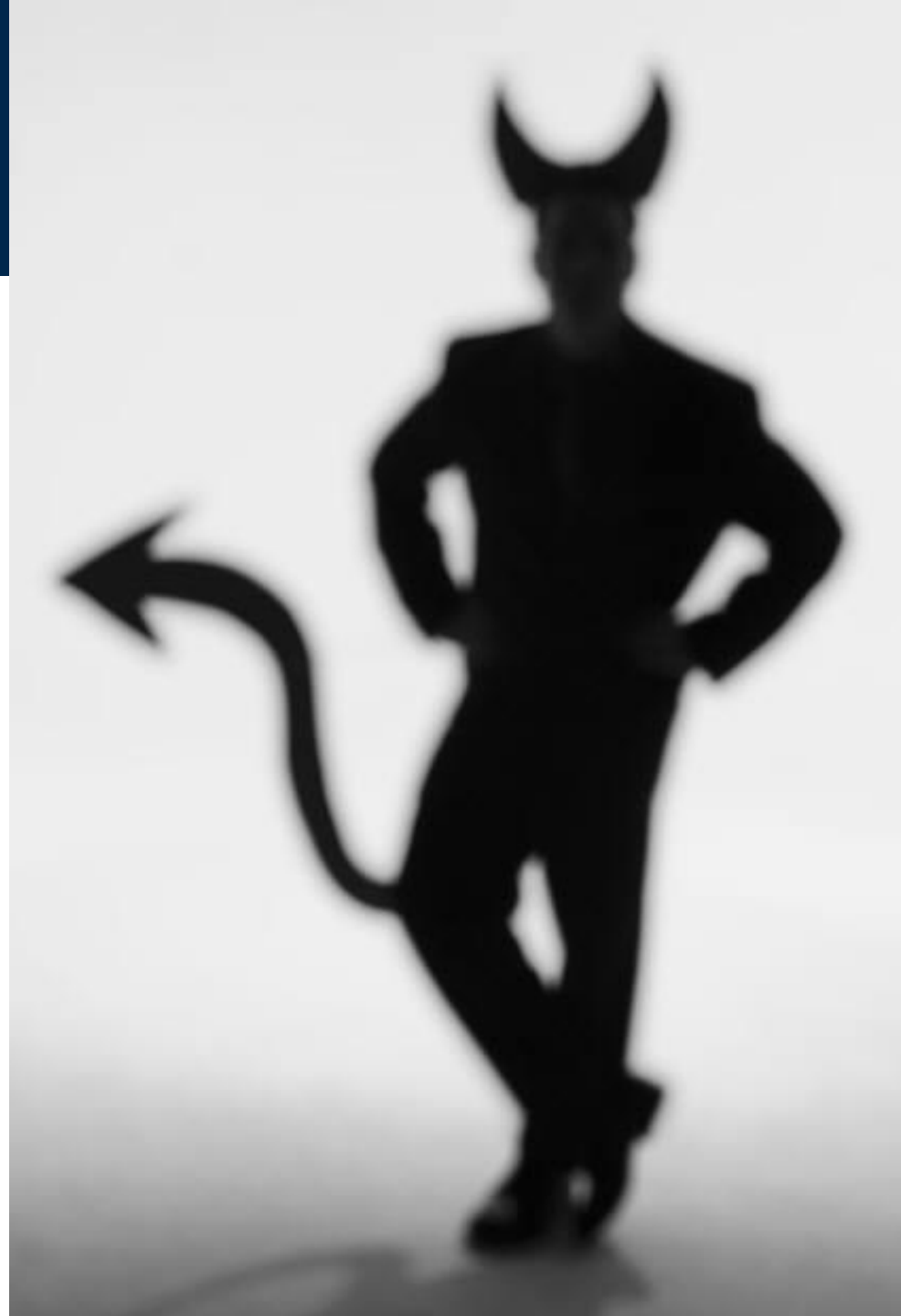
Philosophy?

Natural Sciences?

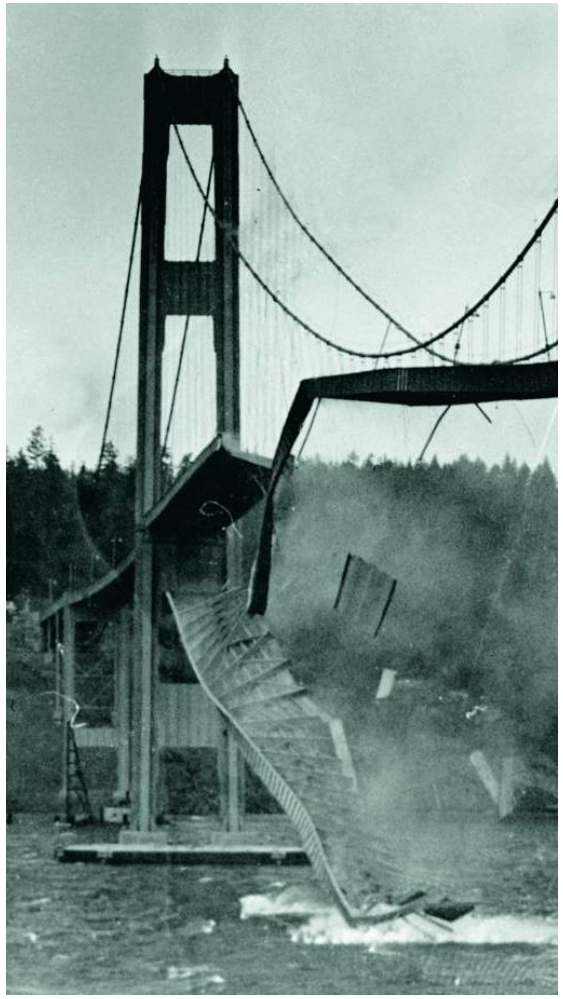
Meet the Adversary

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

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



What's the Difference?



Why is Security its own Area of CS?

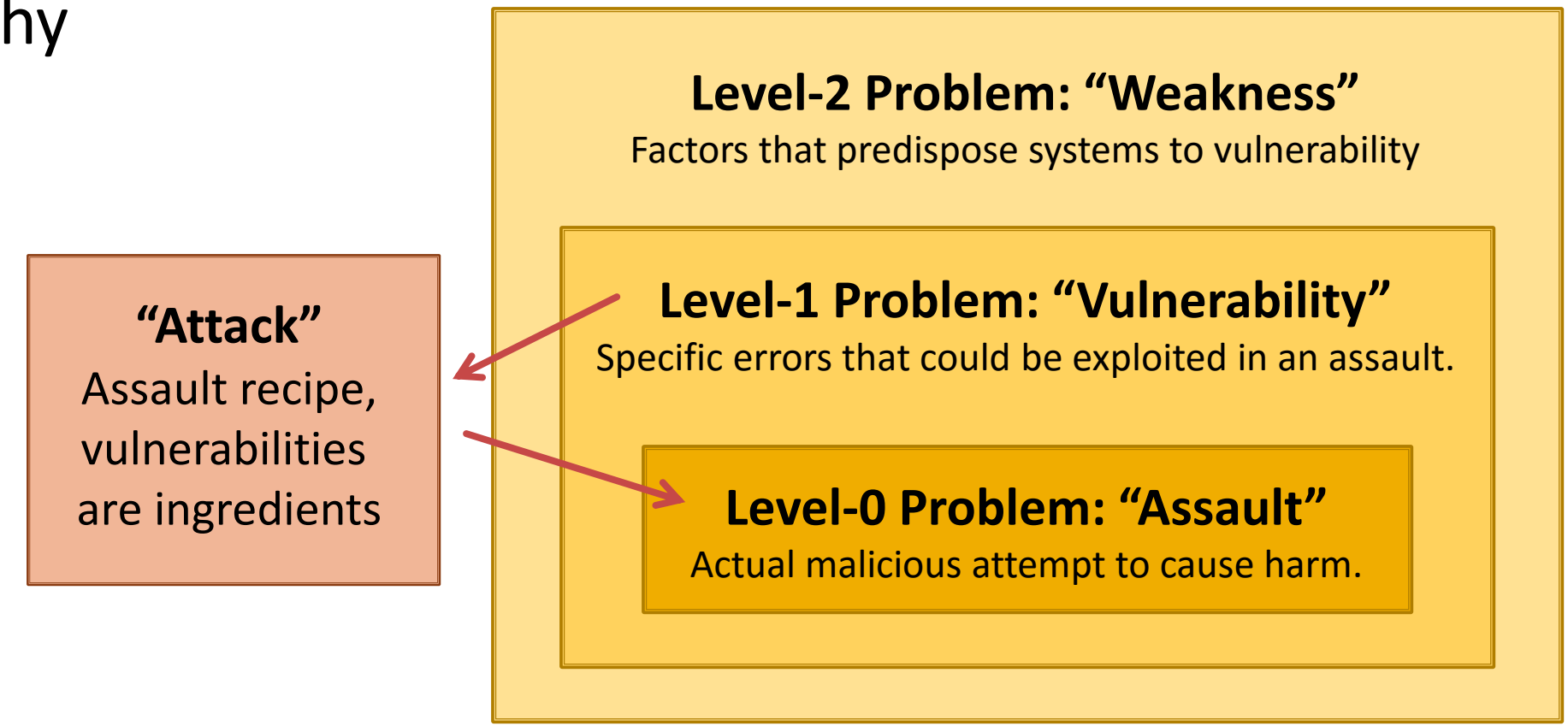
Who does Security Research?

- Academia
- Industry
- Military
- Hobbyists

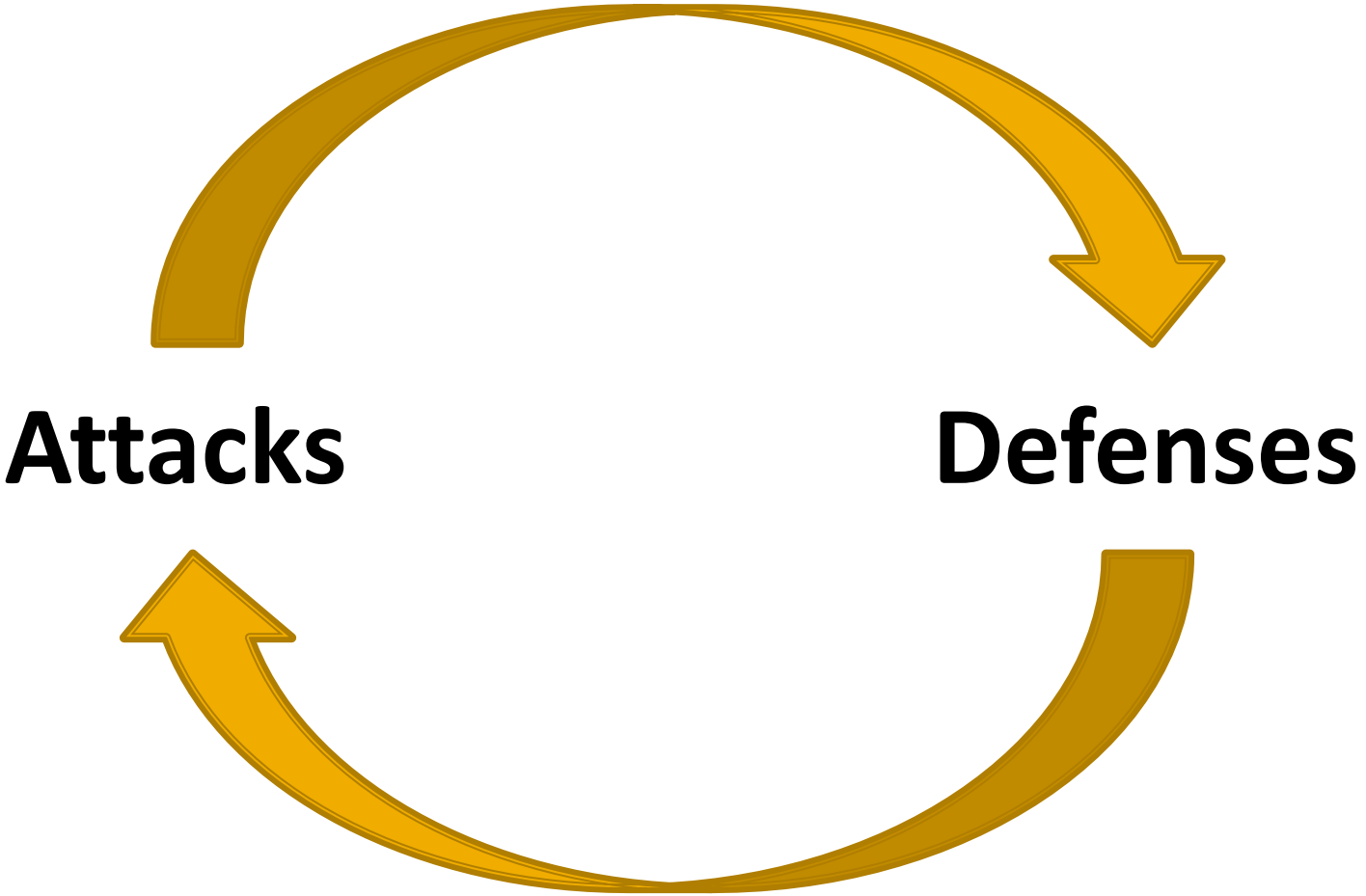
- Bad guys…

“Insecurity”?

Hierarchy



High-Level Approaches



Why Study Attacks?

Identify vulnerabilities so they can be fixed.
Create incentives for vendors to be careful.
Learn about new classes of threats.

- Determine what we need to defend against.
- Help designers build stronger systems.
- Help users more accurately evaluate risk.

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 CSE building?

Exercises

- Stealing my password

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.

Exercises

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

Exercises

- Using a credit card safely?

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***
  Must be practiced continuously; can't be retrofitted

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?

Selfie Time!

To: **eecs588@umich.edu**

Subject: **<*your_uniqname*>**

> What name should we call you?

> What's your year and major?

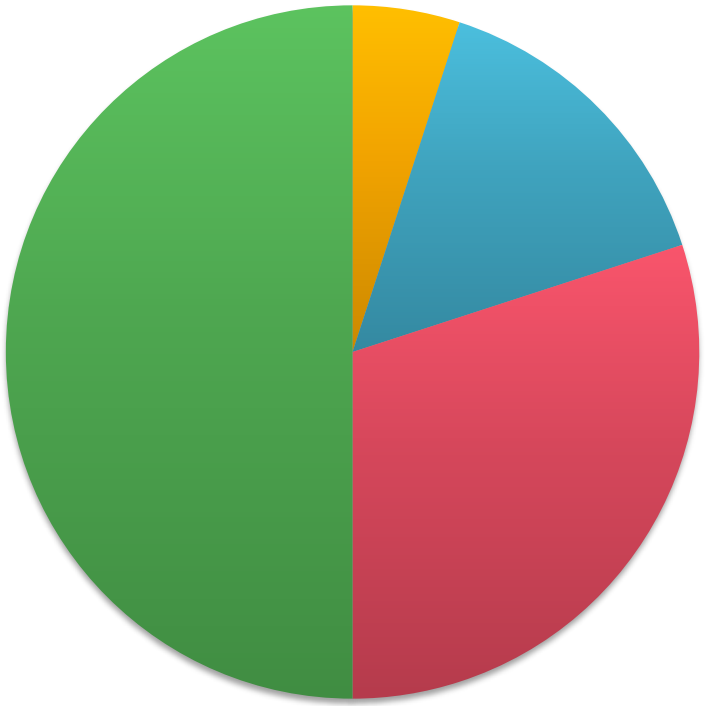
> What would you like to learn in 588?

3 minutes. **Go!**

Recall Goals for this Course

- Gain hands-on experience
  - Building secure systems
  - Evaluating system security
- Prepare for research
  - Computer security subfield
  - Security-related issues in other areas
- Generally, improve research and communication skills
- Learn to be a `1337` `hax0r`, but an ethical one!

Grading



- Class Participation (5%)
- Paper Responses (15%)
- Attack Presentation (30%)
- Research Project (50%)

No exams, no problem sets!

Class Participation (5%)

- ~2 required papers for discussion in each session
  (other readings optional but recommended)
- Come prepared to contribute!
- Full points for speaking up and contributing substantial ideas
- Lose points for being silent, missing class, Facebook, etc.

Paper Responses (15%)

Brief written response to each paper (~400 words)

- In the first paragraph:

  State the problem that the paper tries to solve; and

  Summarize the main contributions.
- In one or more additional paragraphs:

  Evaluate the paper's strengths and weaknesses;

  Discuss something you would have done differently if you had written the paper; and

  Suggest interesting open problems on related topics.

Attack Presentation (30%)

- *With a partner*, choose a specific attack from recent research and implement a demonstration
- Give a 15 minute presentation:

  (1) describe the attack

  (2) talk about how you implemented it, give a demo

  (3) discuss possible defenses
- Course schedule will list topics later today
- Each group send me ratings for each choice by 5pm Friday

Research Project (50%)

In groups, investigate new attack/defense/tool

Aim for a publishable workshop paper.

Components (more detail on website):

- Preproposal presentation
- Project proposal
- Project checkpoint
- Workshop-style presentation in class
- Final workshop-style report

Communication

Course Web Site

https://eecs588.org

schedule, reading list, reading response submission

Piazza

announcements, discussion, find a partner or group

Email Us

eecs588@umich.edu

administrativa, suggestions, questions, concerns

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

Your Assignments…

First paper discussion Thursday (2 MD5 papers)

See course site for required reading (*under construction*)

submit written responses via eecs588.org by start of class!

Find a partner and rate the topics for attack presentation;

updated topic list available tomorrow;

email topic ratings by 5pm on Friday

Start thinking about your course project;

Form a group, present topic idea February 18 in class