

EECS 588: Computer and Network Security



Introduction
January 13, 2014

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.
Princeton Ph.D.

Web: <https://jhalderm.com>

Email: jhalderm@umich.edu

Office: 4717 BBB

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

Mobile: 609-558-2312



How I spent my winter vacation



How I spent my winter vacation



How I spent my winter vacation



How I spent my winter vacation









How I spent my winter vacation







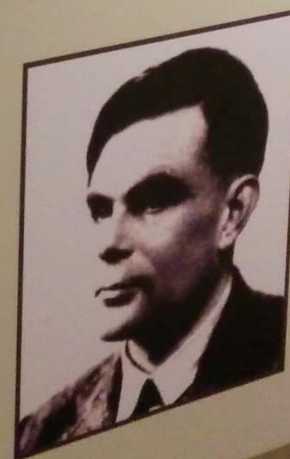
ALAN TURING'S OFFICE

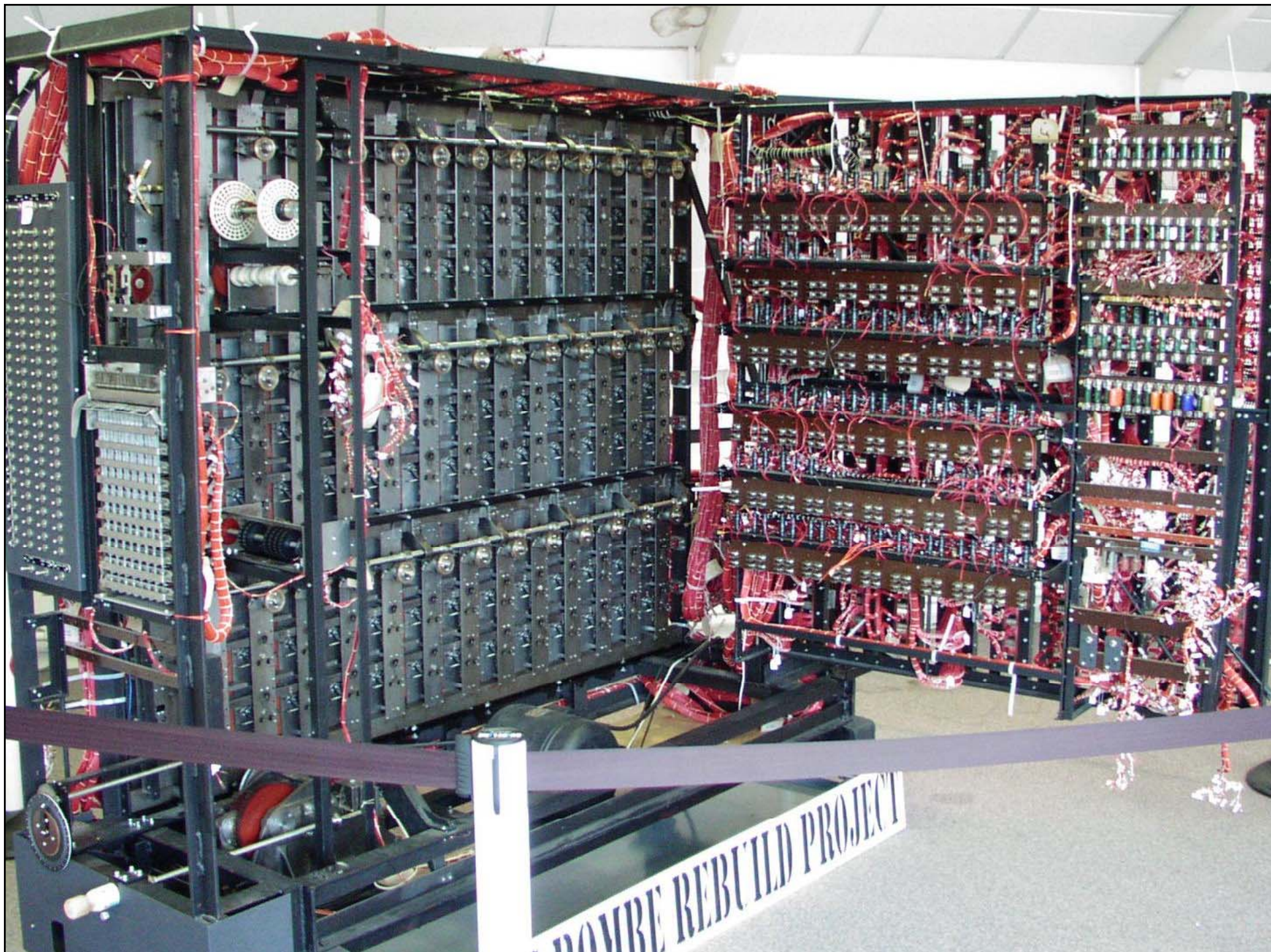
Here at his desk in Hut 8, Turing took the lead on breaking naval Enigma ciphers – something few thought could ever be done. His mathematical skills also enabled him to break other ciphers, including the complex Lorenz cipher where he used a method that became known as Turingery. Together with his fellow Codebreaker Gordon Welchman, he developed the Bombe machine to help speed up the codebreaking process.

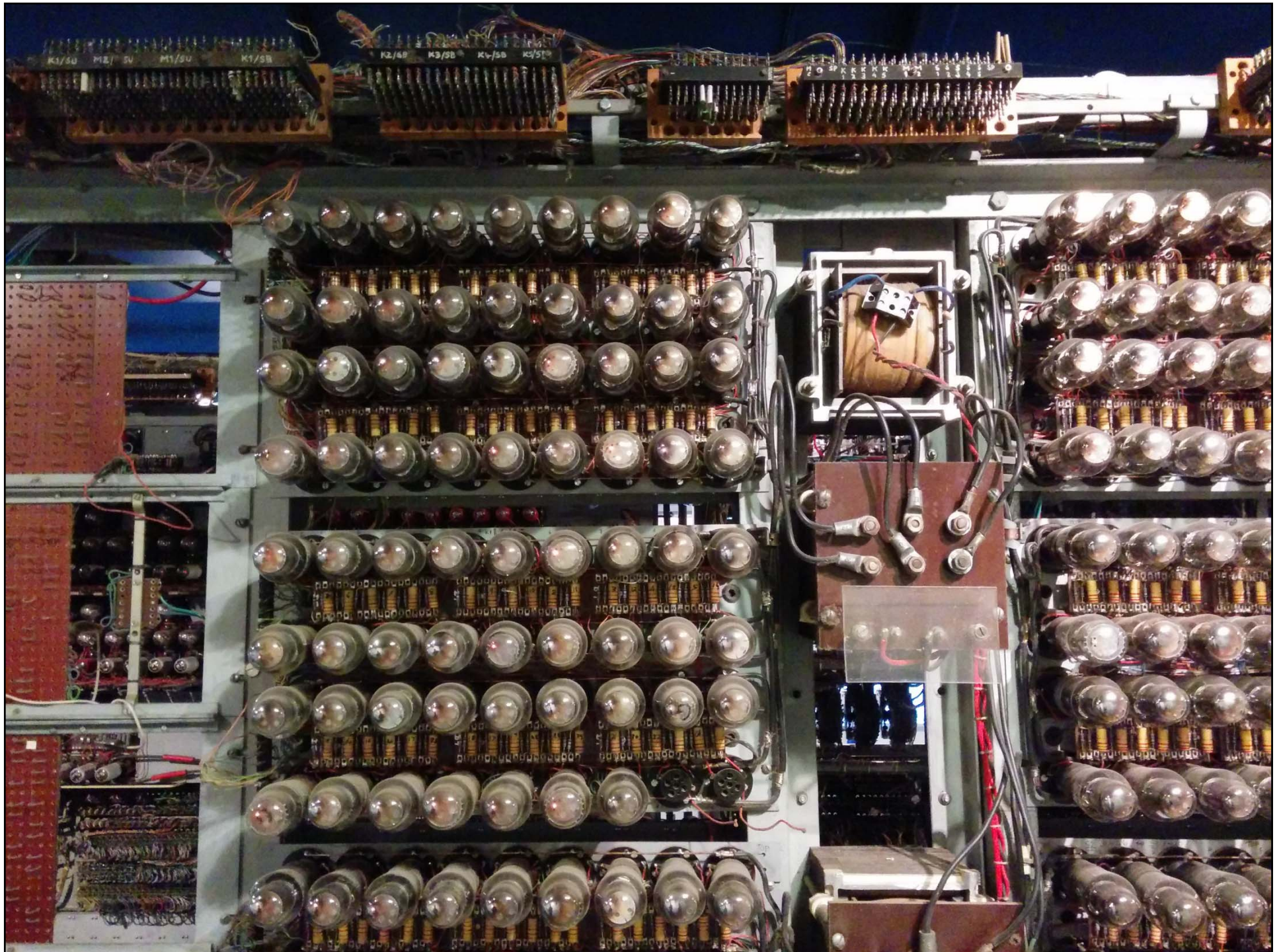
IN THEIR WORDS

If anyone was indispensable to Hut 8 it was Turing. The pioneer work always tends to be forgotten when experience and routine later make everything seem easy, and many of us in Hut 8 felt that the magnitude of Turing's contribution was never fully realised by the outside world.

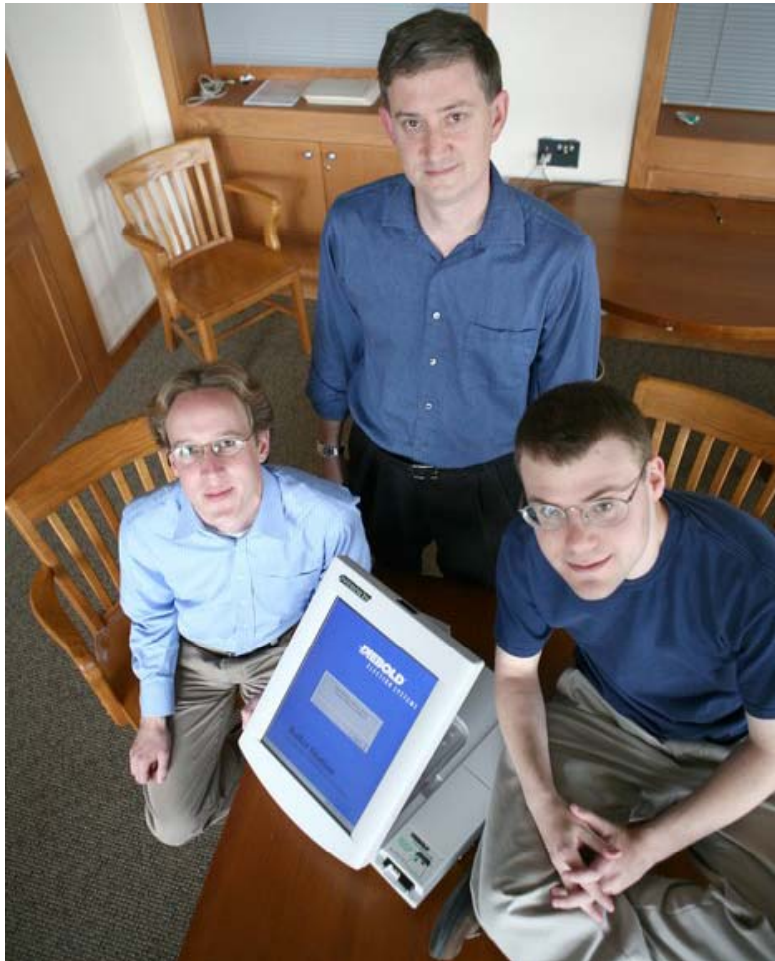
Hugh Alexander, Codebreaker, Hut 8



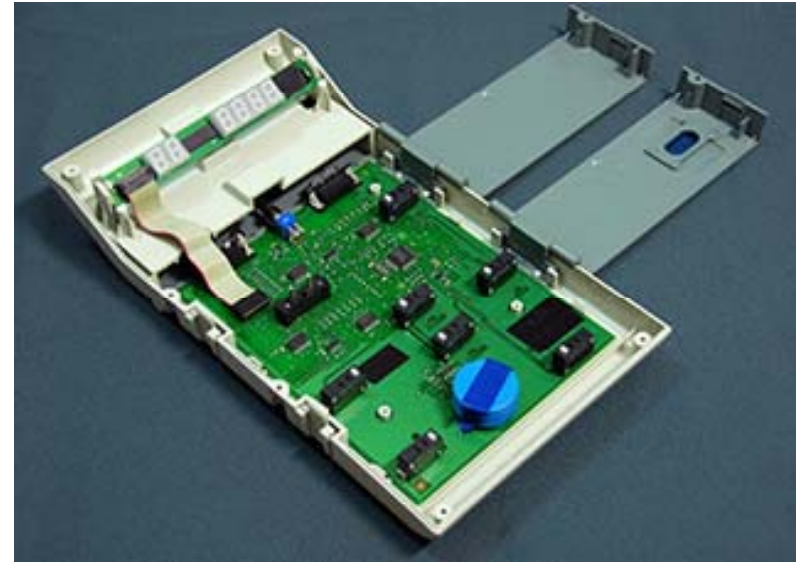




My Work – Electronic Voting



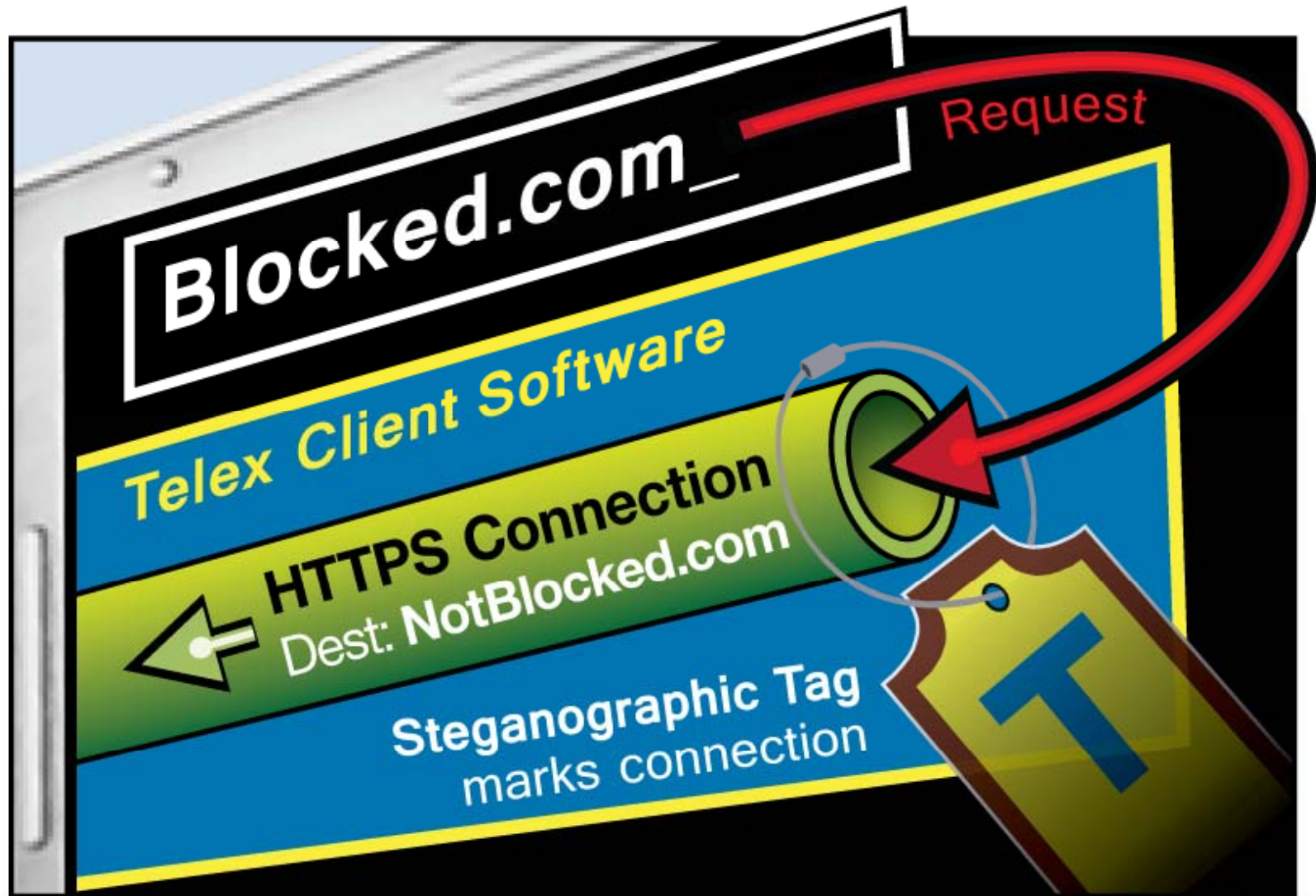
Alex's Work – Electronic Voting



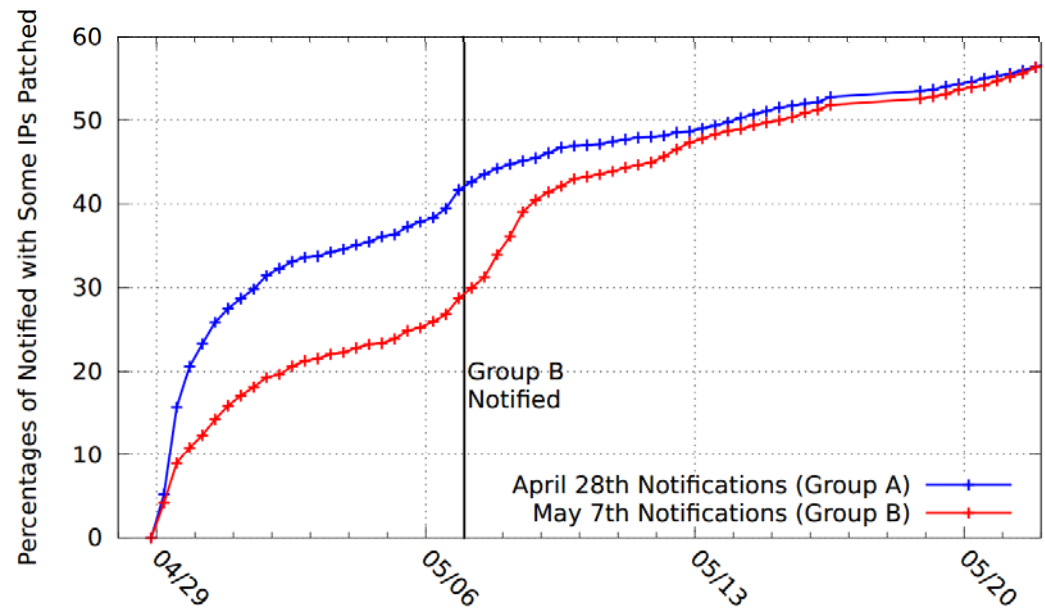
My Work – Disk Encryption



My Work – Anticensorship



My Work – Internet Measurement



My Work – HTTPS



LAUNCHING IN 2015:

Let's Encrypt

A CERTIFICATE AUTHORITY TO
ENCRYPT THE ENTIRE WEB

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.

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



Not a
crypto
course

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?

What is Security Research?

“The study of how systems behave in the presence of an **adversary***.”

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



What's the Difference?



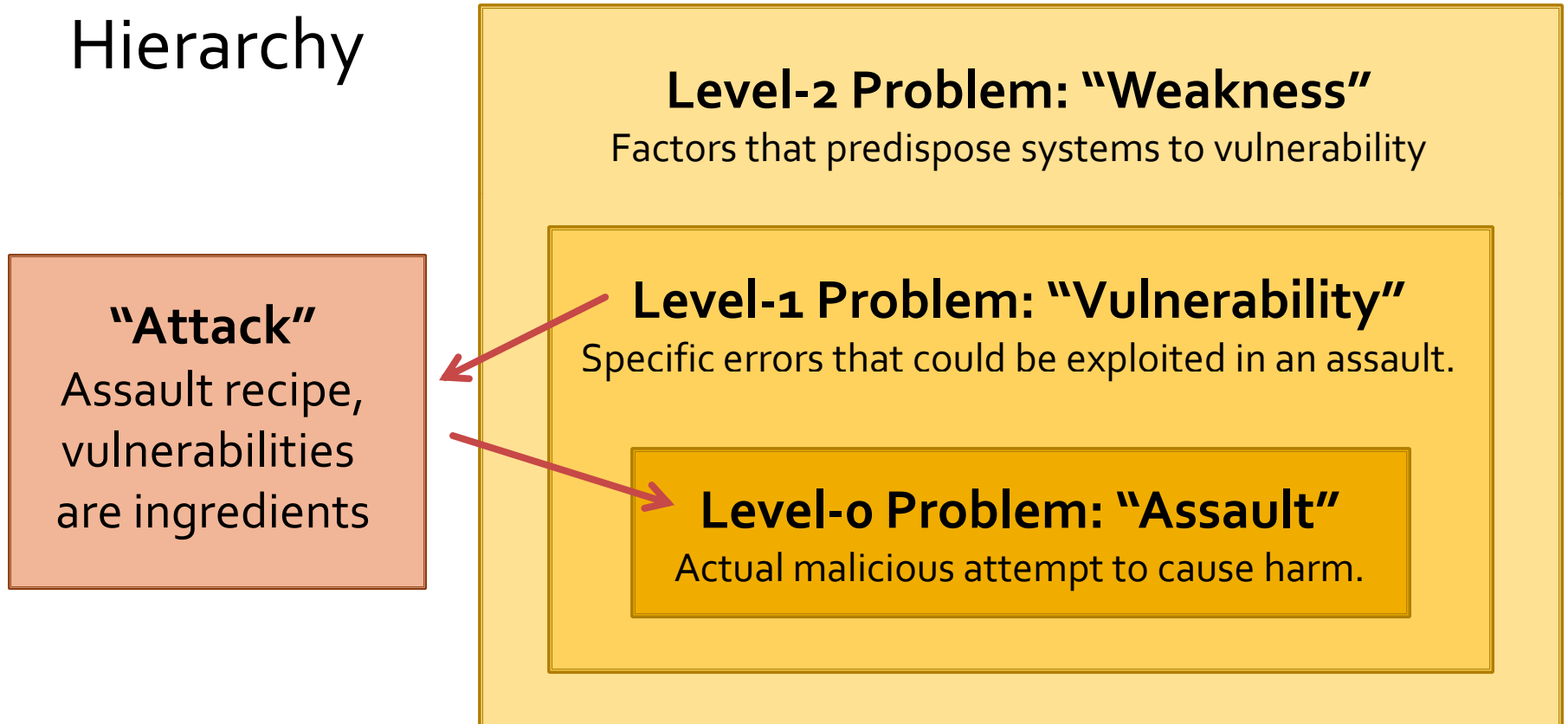
Why is Security its own Area of CS?

Who does Security Research?

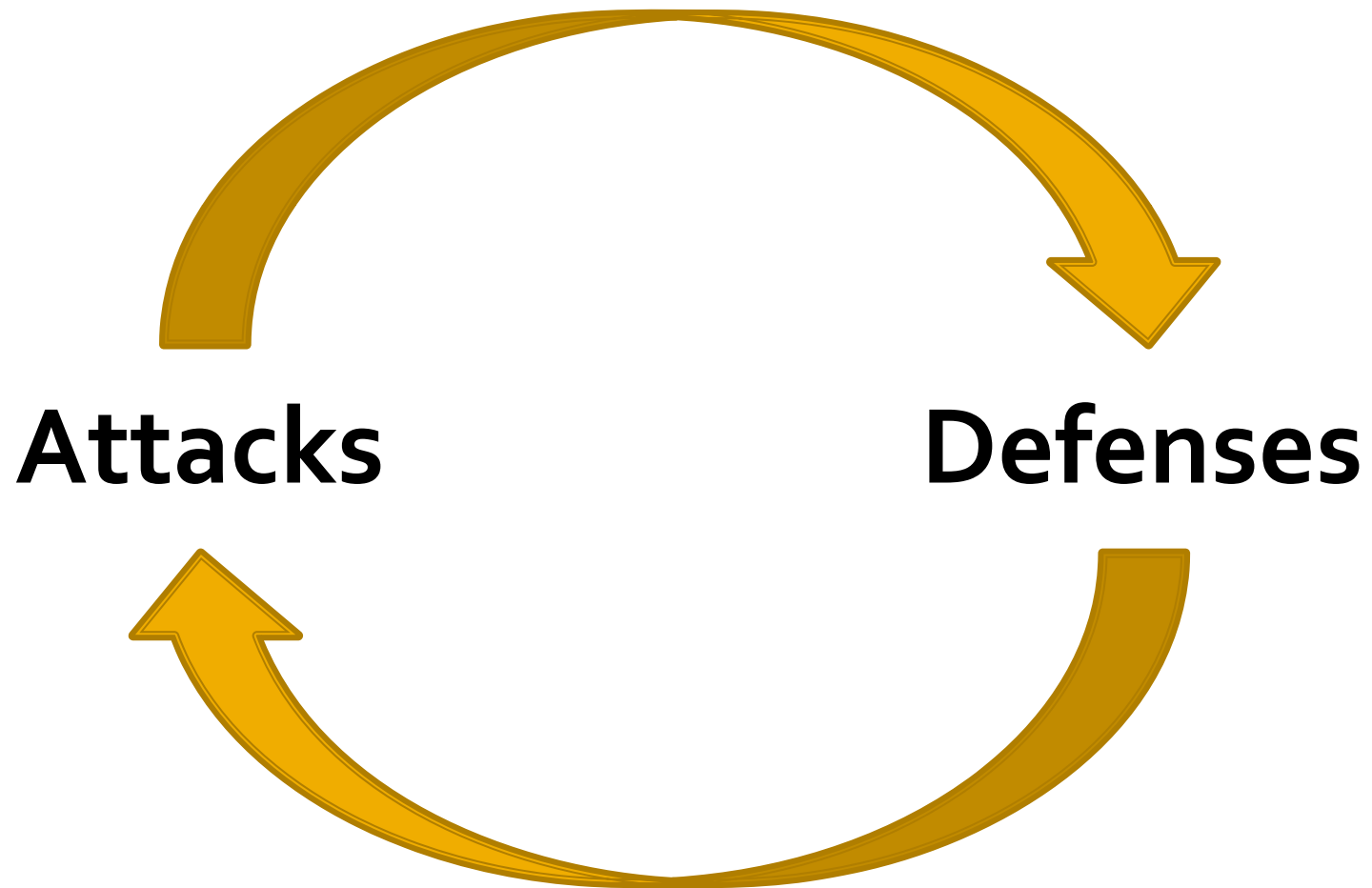
- Academia
- Industry
- Military
- Hobbyists
- Bad guys...

"Insecurity"?

Hierarchy



High-Level Approaches



Why Study Attacks?

- Identify flaws so they can be fixed
- Pressure vendors to be more careful
- Learn about new classes of threats
 - Motivate new research on defenses
 - Determine what we need to defend against
 - Help designers build better threat models
 - Help users more accurately evaluate risk
- Identify false design assumptions
Improve models used for proof of security

Thinking Like an Attacker

- Look for weakest links – easiest to attack
 - Insider attacks, social engineering
- Think outside the box – not constrained by system designer's worldview
 - Side-channel attacks (TEMPEST, power analysis)
- Identify assumptions that security depends on – are they false?
 - e.g. cold-boot attacks

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 an election

Exercises

- Stealing my password

Exercises

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

Thinking Like a Defender

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

Challenge is to think
rationally and
rigorously about risks.
Controlled paranoia.

Exercises

- Using a credit card safely

Exercises

- Should you lock your door?

Spotting Security Snake-Oil?

- Kerckhoffs's principle
Should be secure even if everything about the design is public—except for the secret keys
- Roll-Your-Own Encryption
Just because you can't break it doesn't mean it's hard to break – look for AES, SHA-2, etc.

Selfie Time!

To: `eeecs588@umich.edu`
Subject: `username`

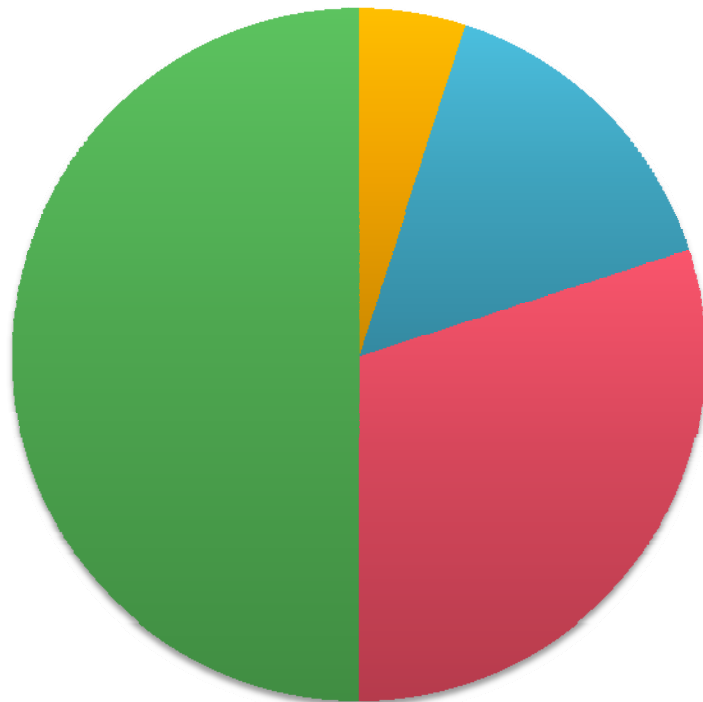


3 minutes. Go!

Recall Course Goals

- 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, frequently 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

[http://www.eecs.umich.edu/courses/eecs588/
schedule, readings](http://www.eecs.umich.edu/courses/eecs588/schedule_readings)

Piazza

announcements, discussion

Email Me

jhalderm@umich.edu
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 and state laws criminalize computer intrusion and 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 Tuesday (2 MD5 papers)

See course site for required reading

Remember to send written responses

Find a partner and rate the topics for your
attack presentation;

email topic ratings by 5pm this Friday

Start thinking about your course project;

Form a group, present topic idea February 26