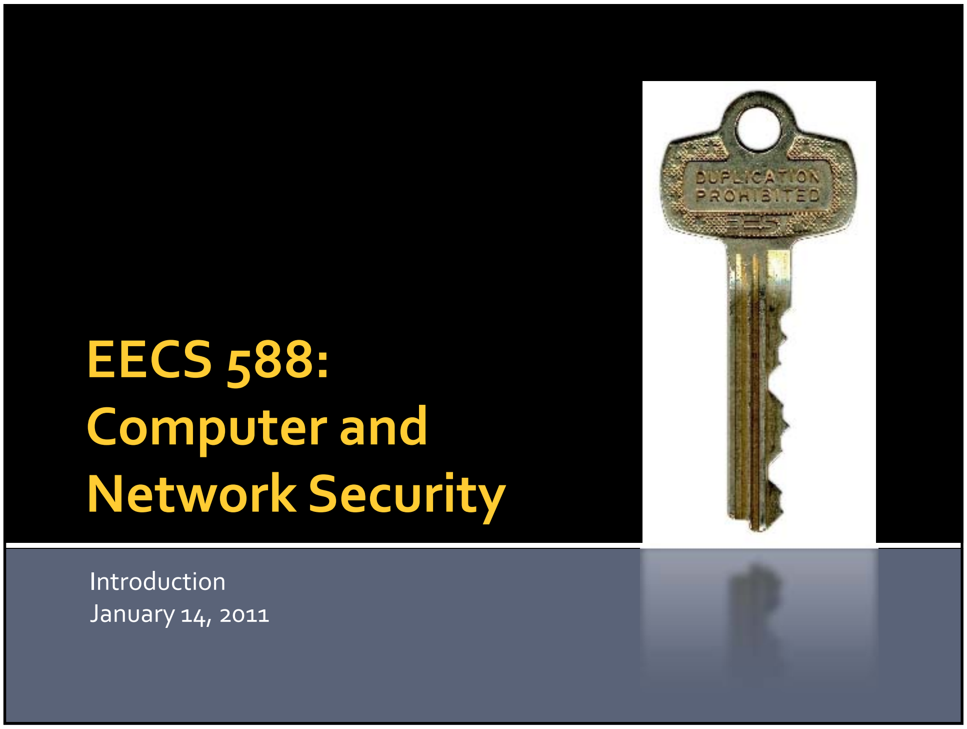
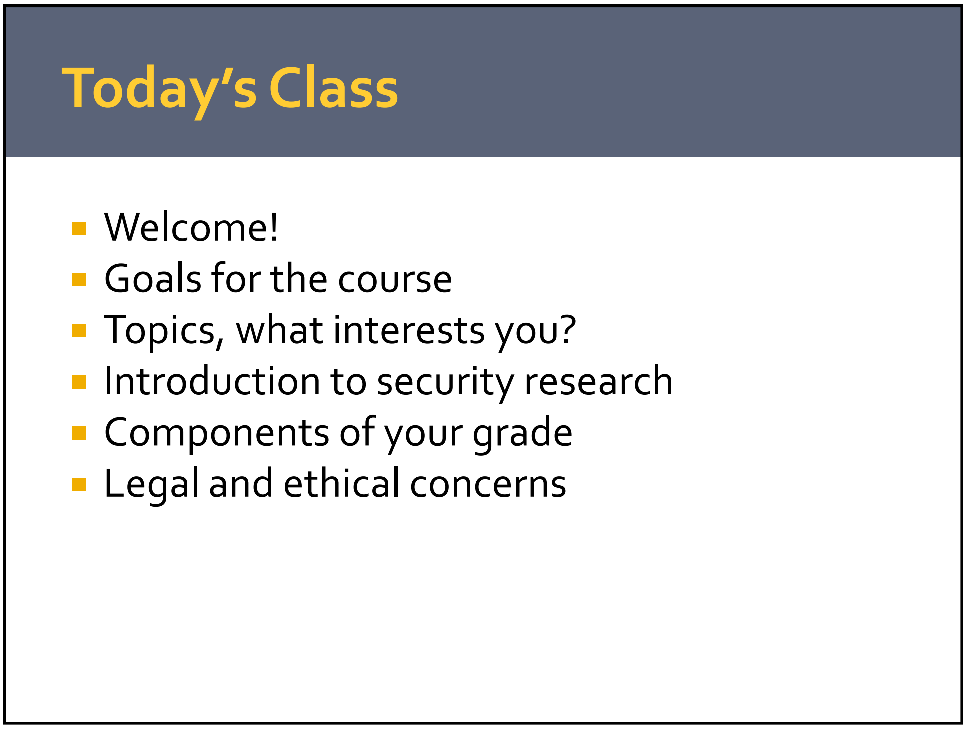

DUPLICATION
PROHIBITED

EECS 588: Computer and Network Security

Introduction
January 14, 2011



Today's Class

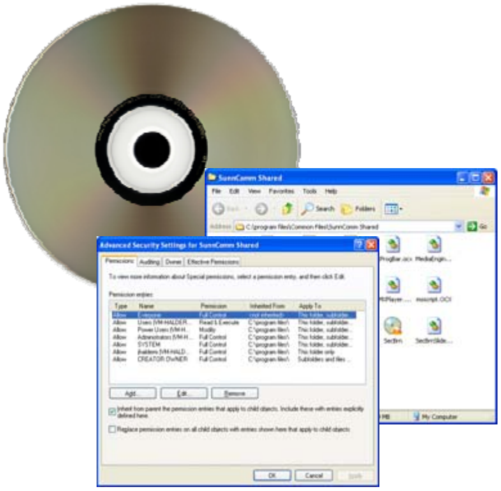
- Welcome!
- Goals for the course
- Topics, what interests you?
- Introduction to security research
- Components of your grade
- Legal and ethical concerns

Who am I?

J. Alex Halderman
CSE Prof
Princeton PhD

Email:	jhalderm@
Office:	4717 CSE
Hours:	TuTh 3:30-4:30 or by appointment
Mobile:	609-558-2312

My Work – DRM



To view more information about Special permissions, select a permission entry, and then click Edit.

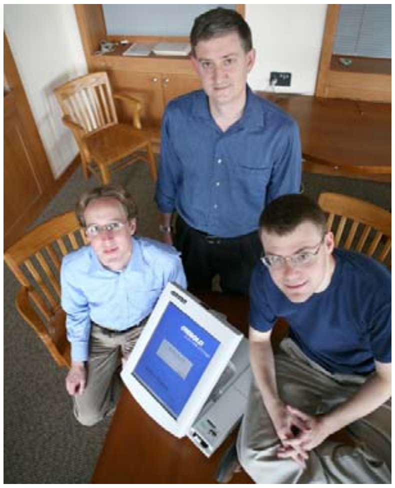
Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Everyone	Full Control	<not inherited>	This folder, subfolder...
Allow	Users (VM-HALDER...	Read & Execute	C:\program files\	This folder, subfolder...
Allow	Power Users (VM-H...	Modify	C:\program files\	This folder, subfolder...
Allow	Administrators (VM-H...	Full Control	C:\program files\	This folder, subfolder...
Allow	SYSTEM	Full Control	C:\program files\	This folder, subfolder...
Allow	jhalderm (VM-HALD...	Full Control	C:\program files\	This folder only
Allow	CREATOR OWNER	Full Control	C:\program files\	Subfolders and files ...

☑ Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.

☐ Replace permission entries on all child objects with entries shown here that apply to child objects

My Work – Electronic Voting



My Work – Disk Encryption

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!

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 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?

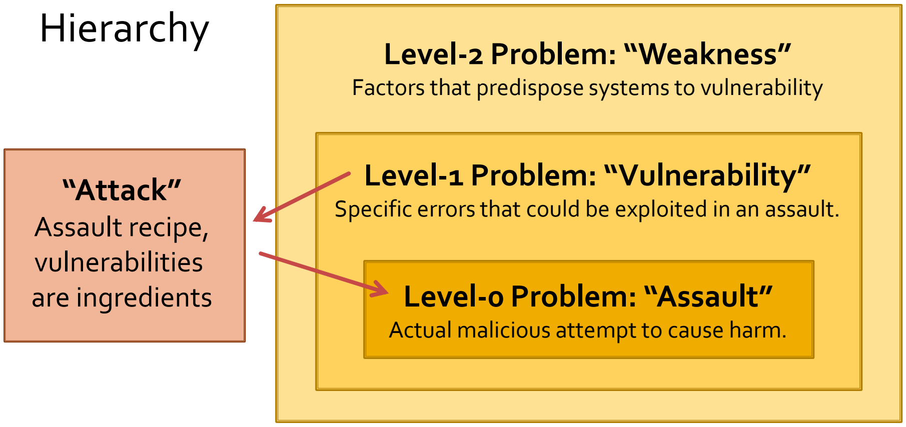
Who does Security Research?

- Academia
- Industry
- Military
- Hobbyists

- Bad guys…

“Insecurity”?

Hierarchy



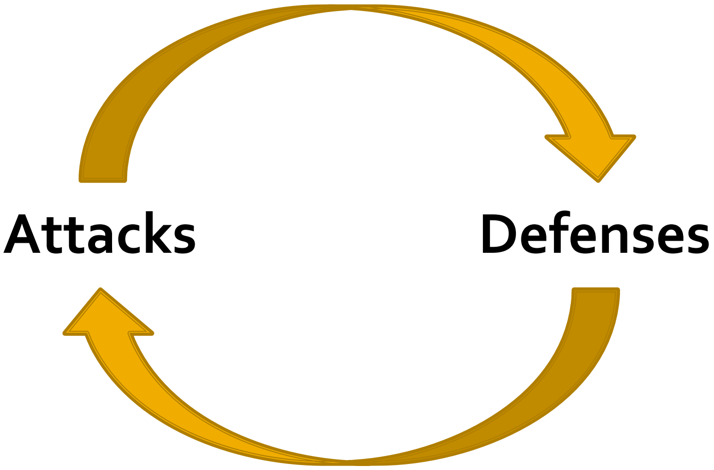
“Attack”
Assault recipe, vulnerabilities are ingredients

Level-2 Problem: “Weakness”
Factors that predispose systems to vulnerability

Level-1 Problem: “Vulnerability”
Specific errors that could be exploited in an assault.

Level-0 Problem: “Assault”
Actual malicious attempt to cause harm.

High-Level Approaches



Attacks

Defenses

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

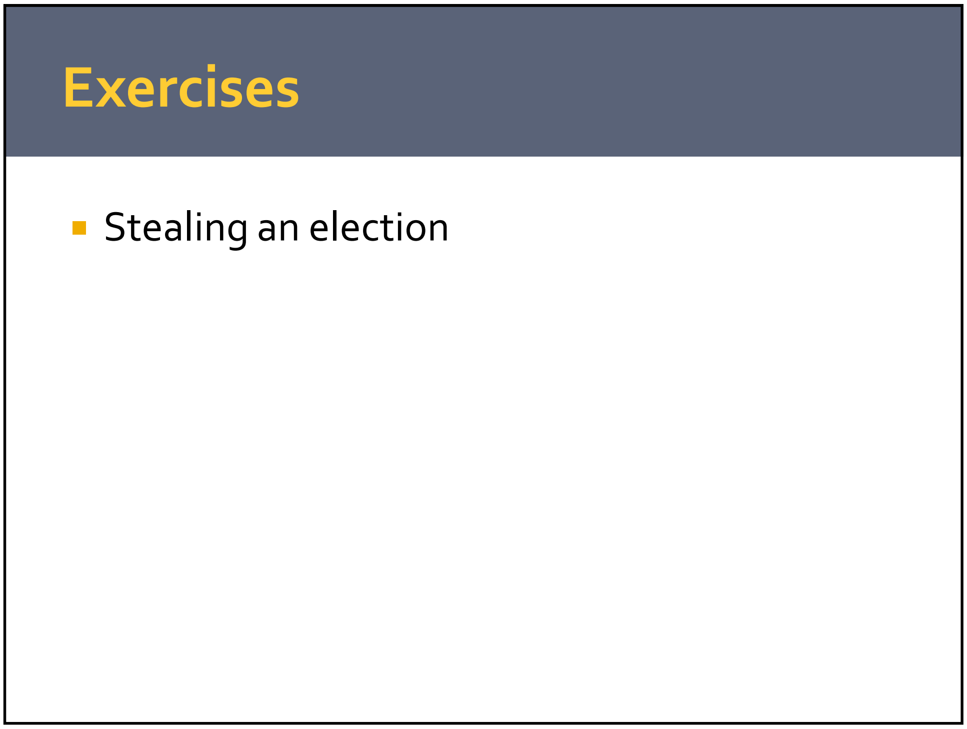
Thinking Like an Attacker

- 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.*

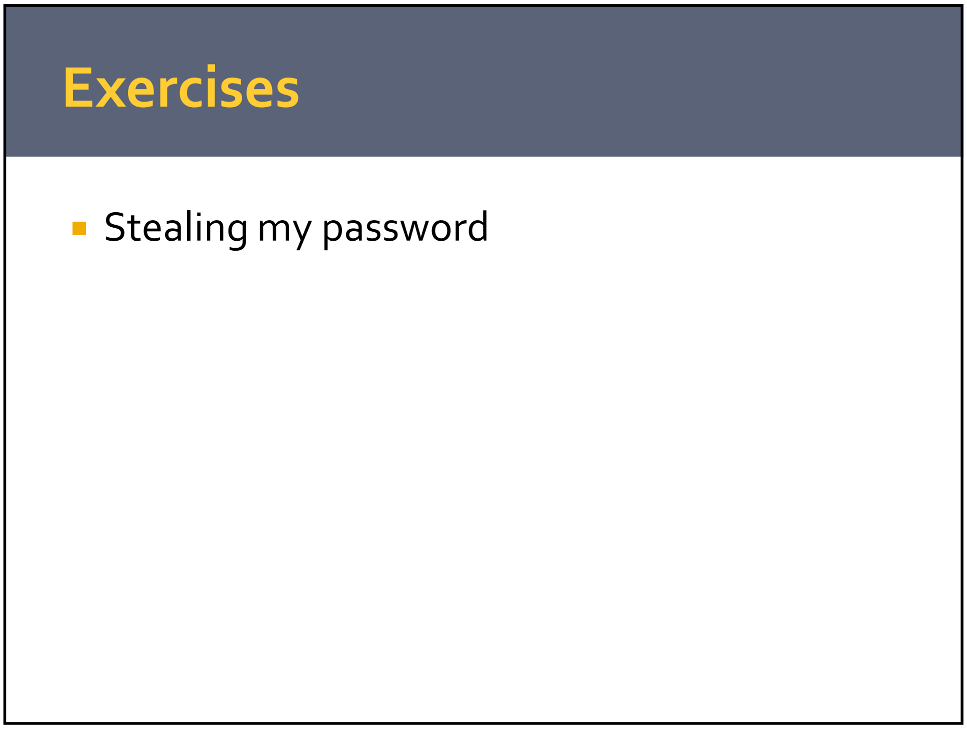
Exercises

- Breaking into the CS building



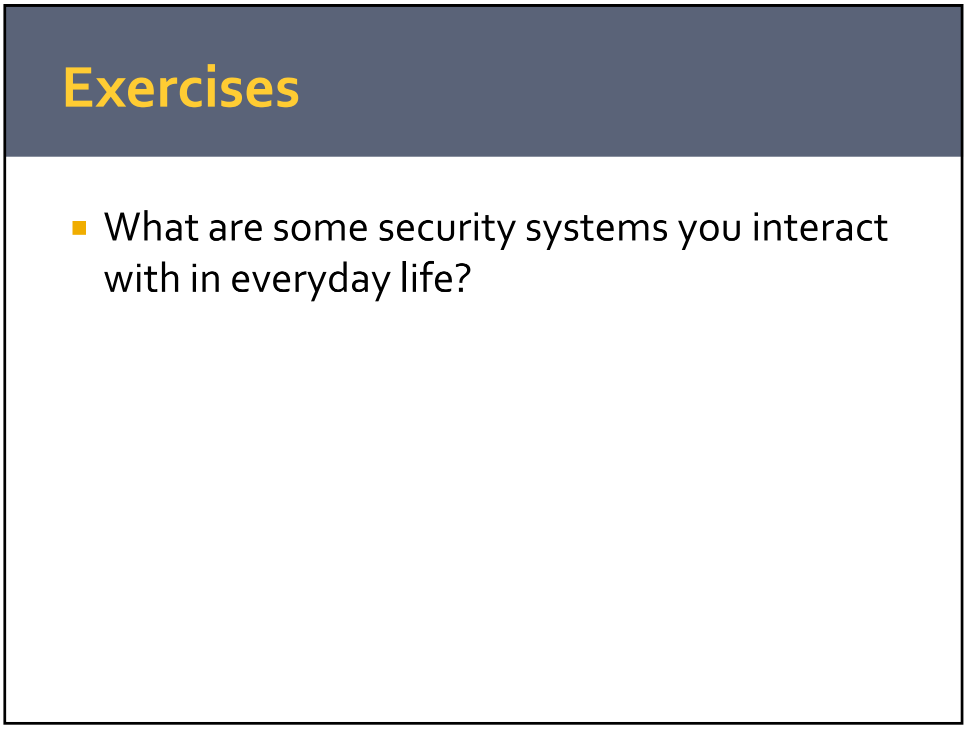
Exercises

- Stealing an election



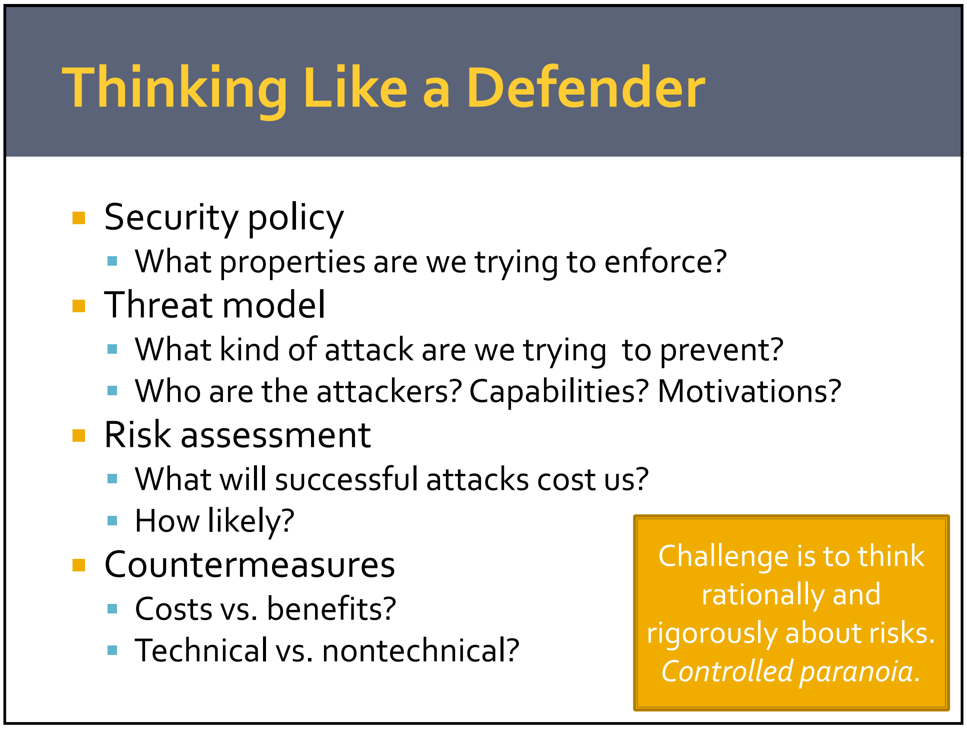
Exercises

- Stealing my password



Exercises

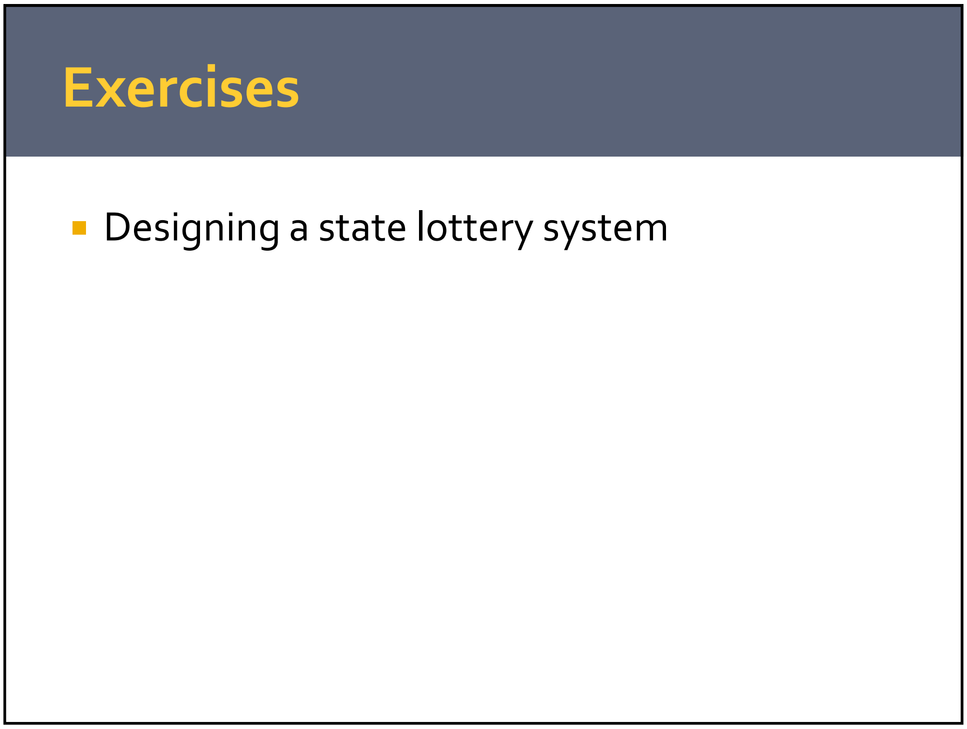
- What are some security systems you interact with in everyday life?



Thinking Like a Defender

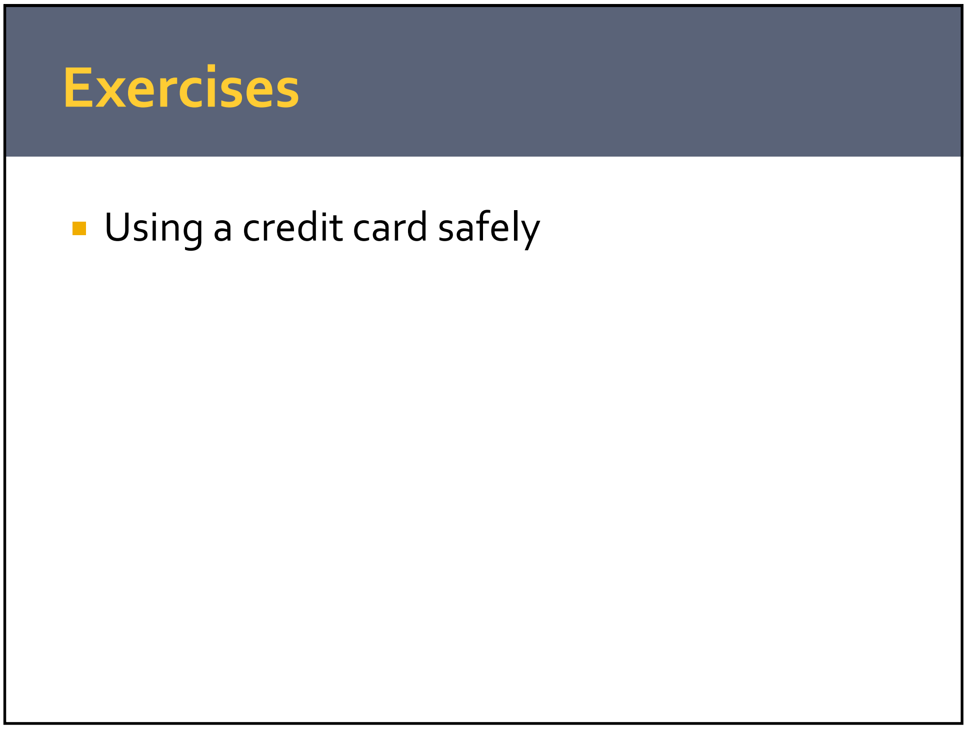
- Security policy
  - What properties are we trying to enforce?
- Threat model
  - What kind of attack are we trying to prevent?
  - Who are the attackers? Capabilities? Motivations?
- Risk assessment
  - What will successful attacks cost us?
  - How likely?
- Countermeasures
  - Costs vs. benefits?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

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



Exercises

- Designing a state lottery system



Exercises

- Using a credit card safely

Exercises

- Should you lock your door?

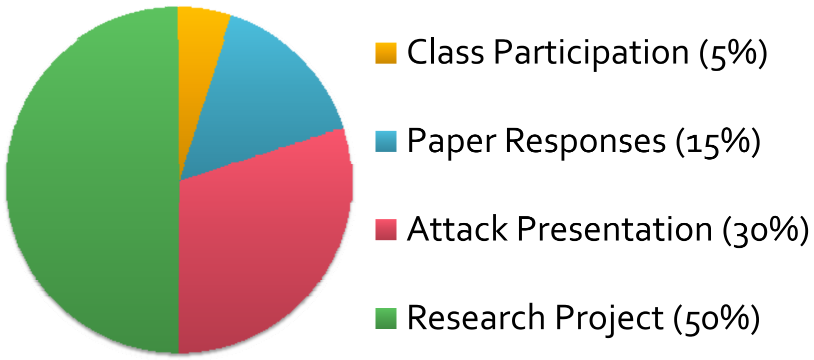
Spotting Security Snake-Oil?

- Kerckhoffs' 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-1, etc.
- References to *Applied Cryptography*
  If you need to look it up in a cryptography book, you probably should be consulting a cryptographer

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



No exams, no problem sets!

Class Participation (5%)

- 1-2 required papers for discussion in each sessions (other readings optional)

- Come prepared to contribute!
- Full points for speaking up and contributing substantial ideas
- Lose points for being silent, frequently missing class, browsing the web, etc.

Paper Responses (15%)

<u>Brief</u> 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 wrote the paper; and
  - Suggest at least two interesting open problems on related topics.
- List any areas you had trouble understanding.
  We'll try to explain them in class.

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 lists topics and dates
- Each group send me top 3 choices by Monday 1/17, I'll tell you your assignment on Tuesday

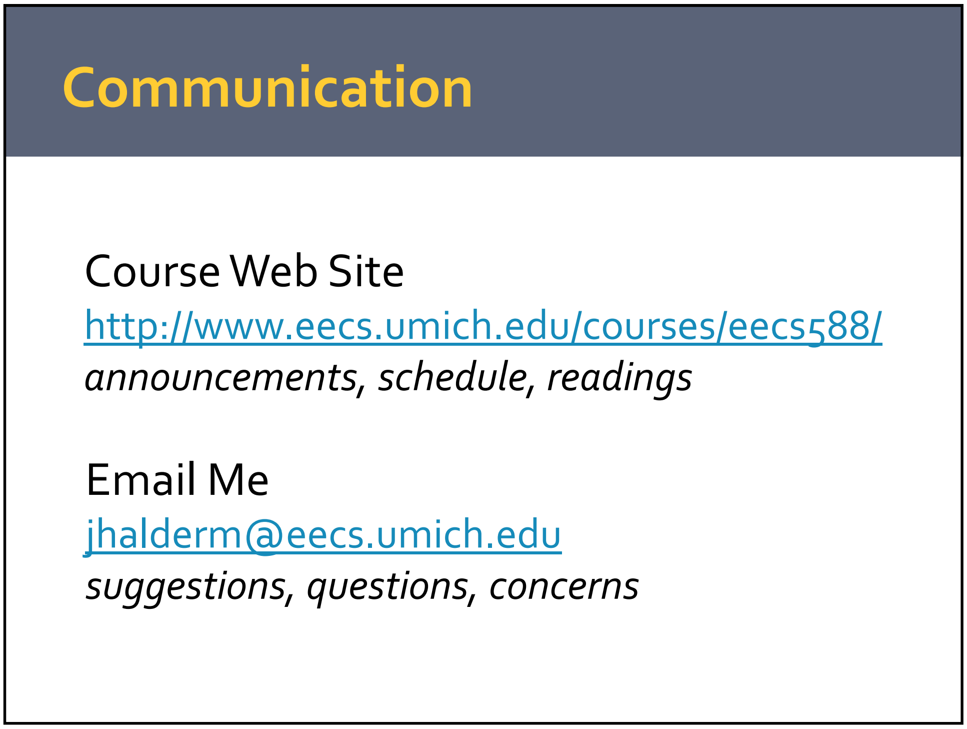
Research Project (50%)

In groups, investigate a new attack or defense

Should have potential to become a marketable product or conference paper, *but not necessarily by the end of the term*

Components (more detail to follow):

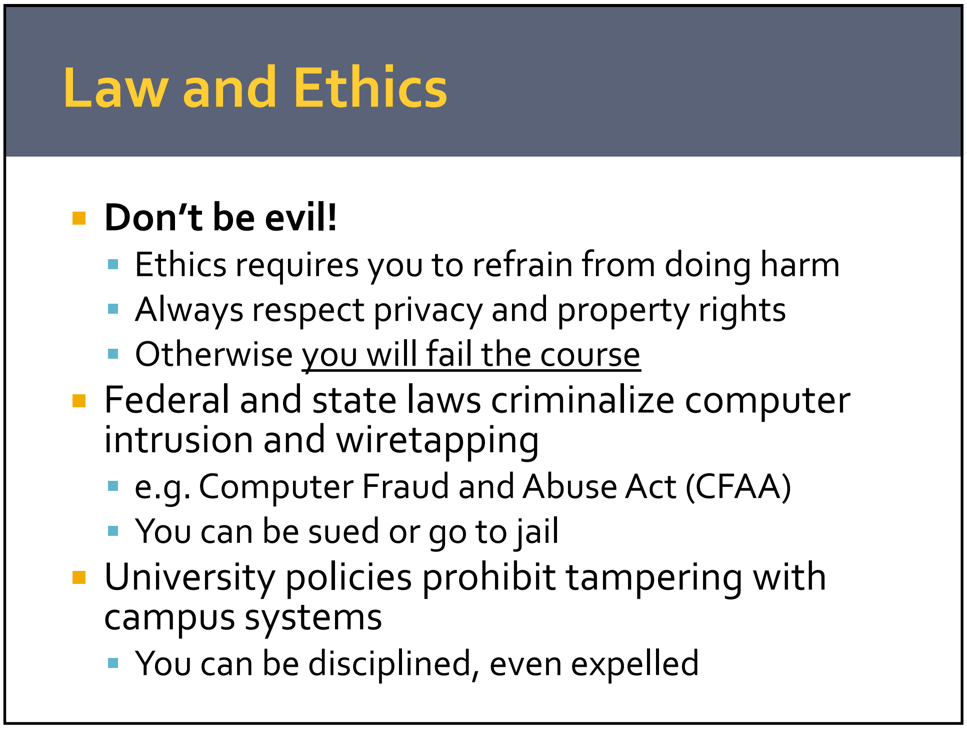
- Project proposal (5%)
- Project checkpoint (5%)
- Conference-style presentation in class (15%)
- Final conference-style report (25%)



Communication

Course Web Site
http://www.eecs.umich.edu/courses/eecs588/
announcements, schedule, readings

Email Me
jhalderm@eecs.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

Next Week

First paper discussion

- See course site for required reading
- Remember to send written responses

Find a partner and pick topics for your attack presentation – email topics by Monday

Start thinking about your course project;

- Form a group, proposal due February 18