CSE 484 / CSE M 584:
Computer Security and Privacy

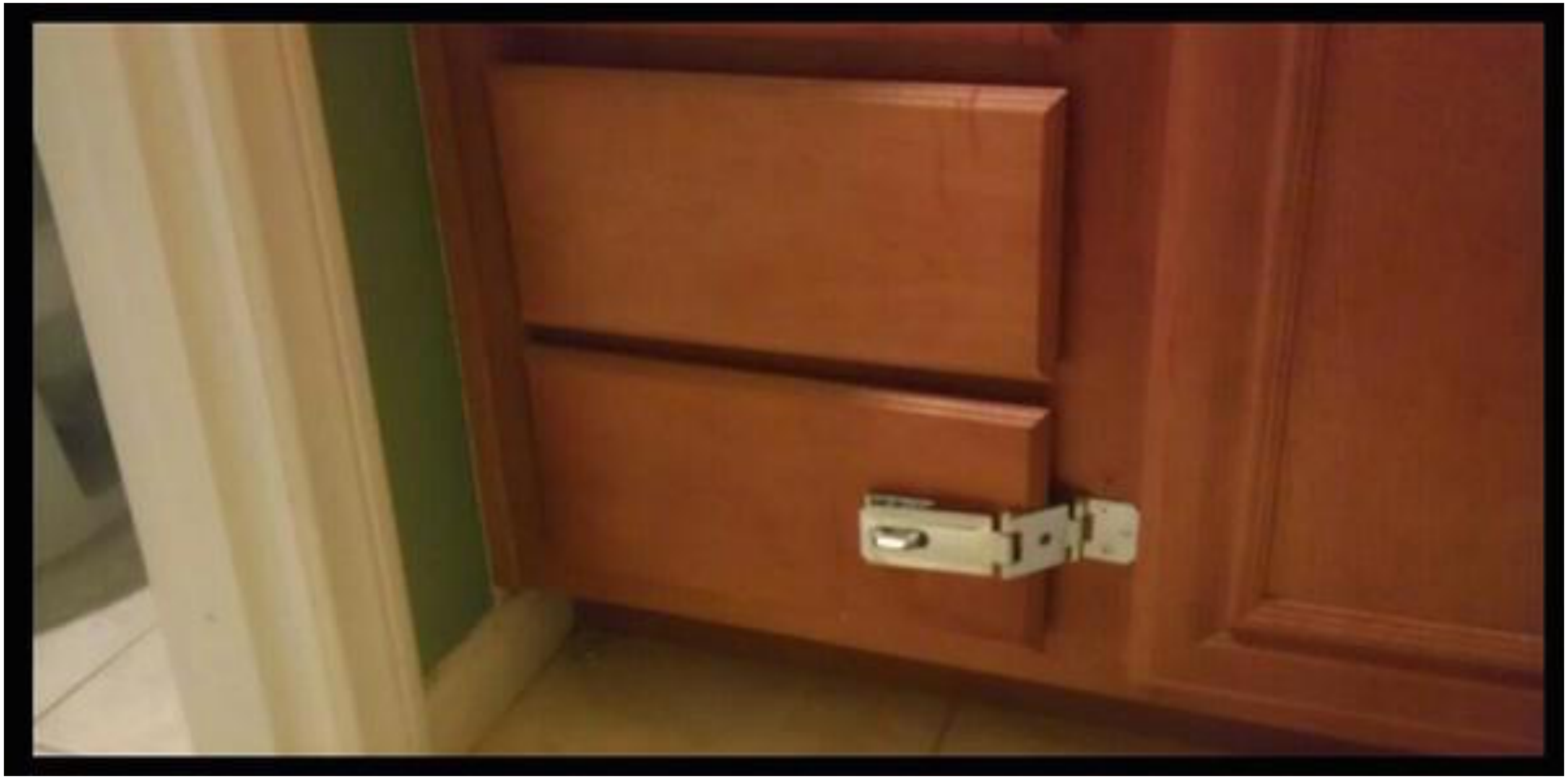
Fall 2016

Ada (Adam) Lerner

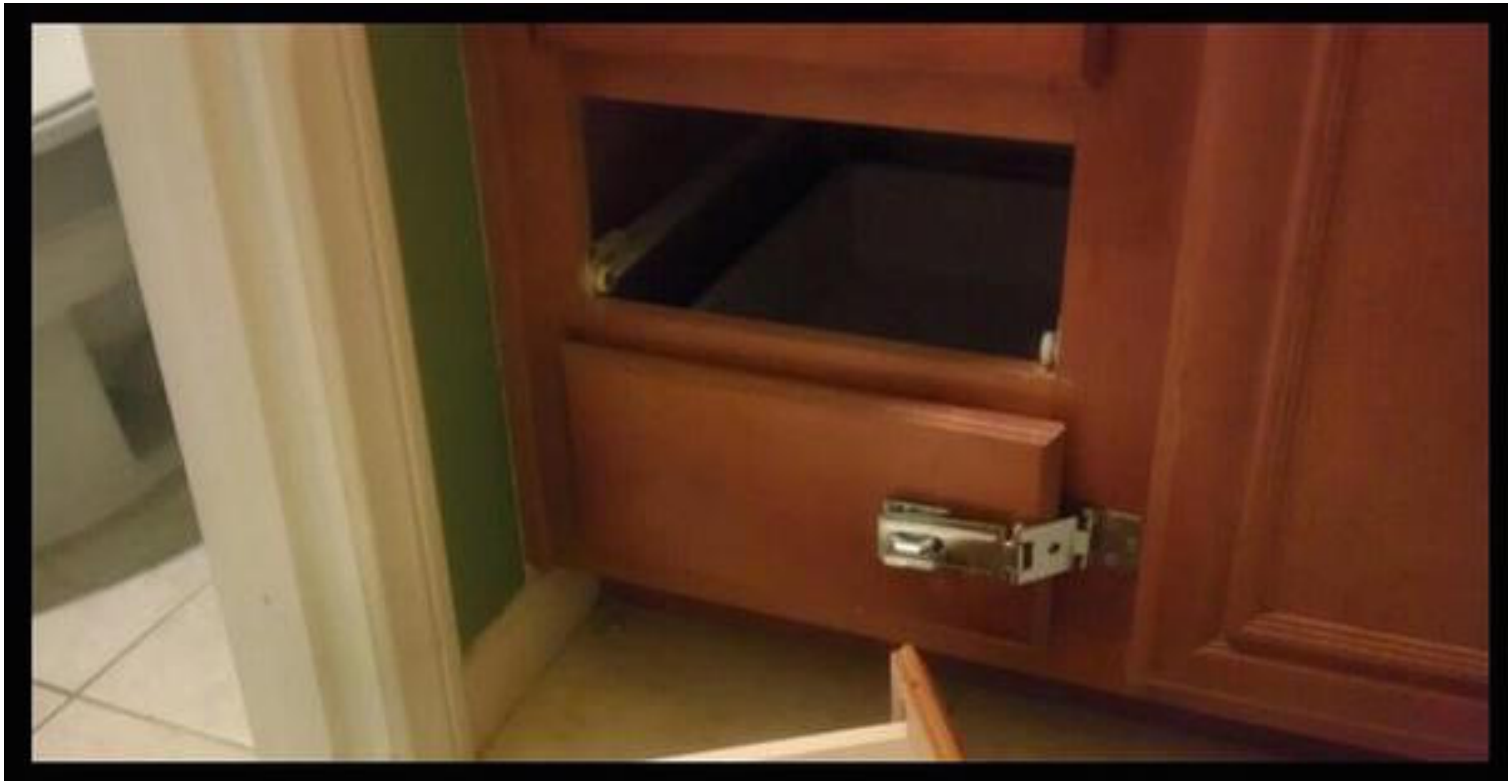
lerner@cs.washington.edu

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others…

What's Wrong With This Picture?



What's Wrong With This Picture?



Quiz Section

- Quiz sections:
  - Thursday, 1:30-2:20pm, LOW 105
  - Thursday, 2:30-3:20pm, LOW 105

Office Hours

- Office hours
  - Ada: Wednesdays 4:30-5:30pm, CSE 220 (Immediately after Wednesday class!)
  - TAs: Mondays 11:00-noon, CSE 220

How to Contact Me and the TAs

- cse484-tas@cs.washington.edu

Prerequisites (CSE 484)

- Required: Data Structures (CSE 326) or Data Abstractions (CSE 332)
- Required: Hardware/Software Interface (CSE 351) or Machine Org and Assembly Language (CSE 378)
- Assume: Working knowledge of C and assembly
  - One of the labs will involve writing buffer overflow attacks in C
  - You must have detailed understanding of x86 architecture, stack layout, calling conventions, etc.
- Assume: Working knowledge of software engineering tools for Unix environments (gdb, etc)
- Assume: Working knowledge of Java and JavaScript

Prerequisites (CSE 484)

- Strongly recommended: Computer Networks; Operating Systems
  - Will help provide deeper understanding of security mechanisms and where they fit in the big picture
- Recommended: Complexity Theory; Discrete Math; Algorithms
  - Will help with the more theoretical aspects of this course.

Prerequisites (CSE 484)

- Most of all: Eagerness to learn!
  - This is a 400 level course.
  - We expect you to push yourself to learn as much as possible.
  - We expect you to be a strong, independent learner capable of learning new concepts from the lectures, the readings, and on your own.

Course Logistics (CSE 484)

- Lectures: MWF: 3:30-4:20pm ;

- Sections: Thurs: 1:30-2:20pm and 2:30-3:20pm
- Security is a contact sport!

Late Policy

- Email us for a 2 day grace period, no questions asked, on any assignment

- If you won’t finish within those two days, **you MUST meet with me** to talk about a schedule for completing the assignment

Participation Grade

- In-class activities (like the one from today!)
  - You may miss (at least) 3 of these, no questions asked
- Regular contributions to class forums
  - Don’t be silent for 9 weeks and then make 10 posts on the last day of the quarter
- In class: harder in a large class, but worth it!

Course Materials

- Textbook:
  - Daswani, Kern, Kesavan, “Foundations of Security”
  - Additional materials linked to from course website
- Attend lectures
  - Lectures will not follow the textbook and will cover a significant amount of material that is not in the textbook
  - Lectures will focus on “big-picture” principles and ideas
- Attend sections
  - Details not covered in lecture, especially about homeworks and labs

Other Helpful Books (Online)

- Ross Anderson, "Security Engineering"
  - Focuses on design principles for secure systems
  - Wide range of entertaining examples: banking, nuclear command and control, burglar alarms
- Menezes, van Oorschot, and Vanstone, "Handbook of Applied Cryptography"
- Many many other useful books exist, not all online

Other Books, Movies, …

- Pleasure books include:
  - Little Brother by Cory Doctorow
    - Available online here http://craphound.com/littlebrother/download/
  - Cryptonomicon and REAMDE by Neal Stephenson
  - The Art of Intrusion and The Art of Deception by Kevin Mitnick
  - Many more -- please feel free to post your favorites on the forum!
- Movies include:
  - Hackers
  - Sneakers
  - Die Hard 4
  - WarGames
  - Many more -- please feel free to post your favorites on the forum!
- Historical texts include:
  - The Codebreakers by David Kahn
  - The Code Book by Simon Singh

Guest Lectures

- We will have a few guest lectures throughout the quarter
  - Useful to give you a different perspective: research, industry, law enforcement, government, legal
  - Most already scheduled, others TBD

Ethics

- To learn to defend systems, you will learn to attack them. You must use this knowledge ethically.

- In order to get a non-zero grade in this course, **you must electronically sign the "Security and Privacy Code of Ethics" form** by 5pm on October 5

Mailing List

multi_cse484a_sp16@uw.edu

- Make sure you're on the mailing list
  - We'll send a test mail after class; everyone enrolled should receive it
- URL for mailing list on course website
- Used for announcements

Forum

- We’ve set up a forum for this course to discuss assignments
  - https://catalyst.uw.edu/gopost/board/lerner/43195/
- Please use it to discuss the homework assignments and labs and other general class materials
- You can also use it to exercise the “security mindset”
  - (Including discussions of movies, books, and security in the real world)

Labs

- General plan:
  - 3 labs (timeline TBD, tentative dates on website)
    - First lab out approximately next Wednesday
  - Submit to Catalyst system (URL on website)
  - Groups of up to three generally allowed (check each project page for details)
- http://courses.cs.washington.edu/courses/cse484/16au/assignments.html

Labs

- First lab: Software security
  - Buffer overflow attacks, double-free exploits, format string exploits, …
- Second lab: Web security
  - XSS attacks, SQL injection, …
- Third lab: Mobile security
  - Android

Homework

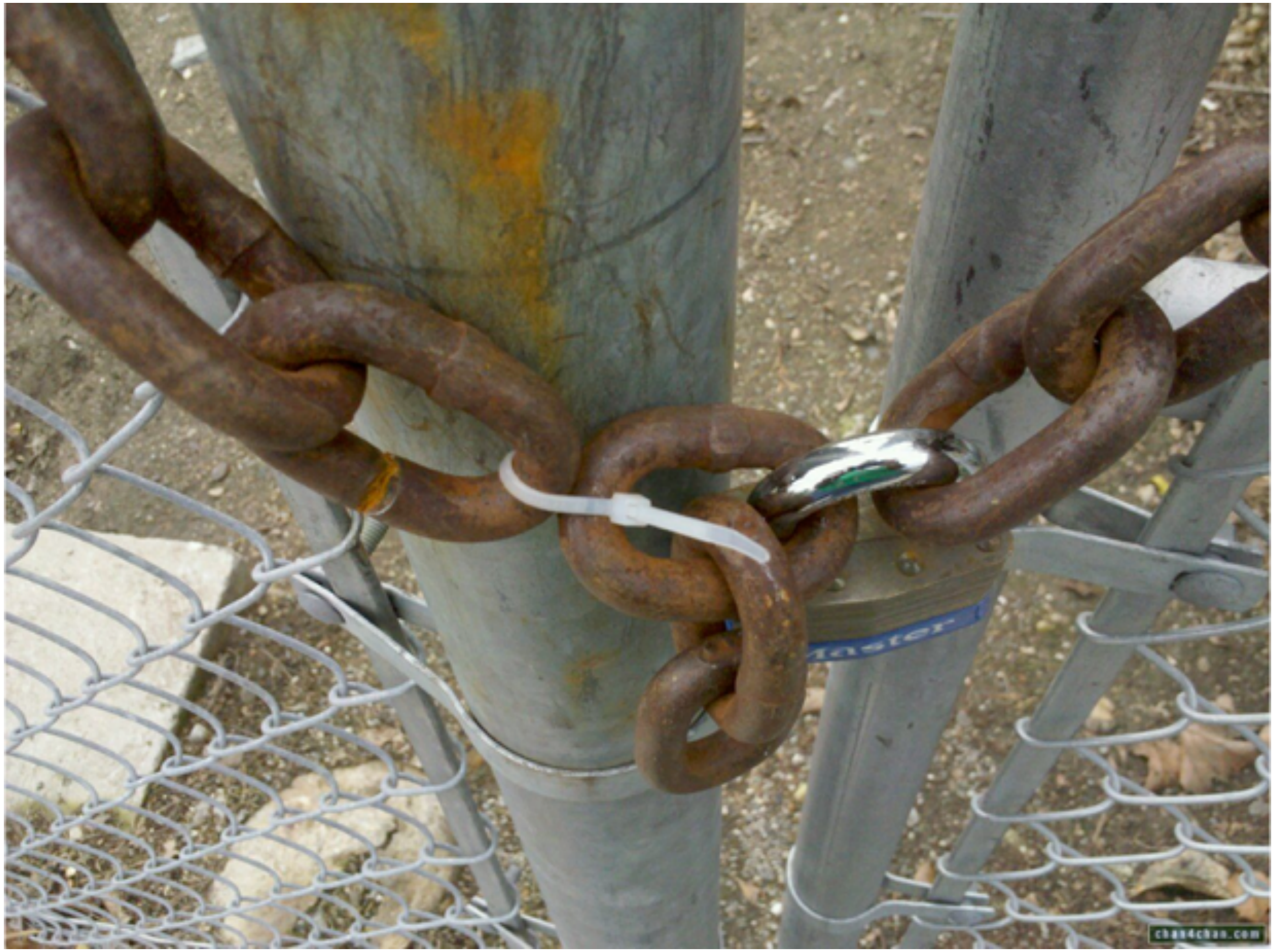
- 3 or 4 homeworks distributed across the quarter (tentative dates on website)
  - http://courses.cs.washington.edu/courses/cse484/16au/assignments.html

- Do now: sign ethics form!

Waitlist / Overload Instructions

- If you are not yet enrolled:
  - Overload request link: http://tinyurl.com/zlarys2
  - Code word: <redacted>
  - Honor system: Please don’t share this code word with students who did not attend class.

Theme: The Security Mindset



Theme: The Security Mindset

- Thinking critically about the design of a system, and challenging assumptions

Theme: The Security Mindset

- Being curious
- Thinking like an attacker

Theme: The Security Mindset

- "That new product X sounds awesome, I can't wait to use it!" versus…
- "That new product X sounds cool, but I wonder what would happen if someone did Y with it…"

Theme: The Security Mindset

- Why it's important
  - Technology changes, so learning to think like a security person is more important than learning specifics of today
  - Will help you design better systems/solutions
  - Interactions with broader context: law, policy, ethics, etc.

Not just Technology – Social Systems are Systems too

- Social Engineering
  - Lying
  - Being nice to people
  - Acting like you belong

Q2

Answer question 2 on the worksheet

How Systems Fail

- Systems may fail for many reasons, including
- **Reliability deals with accidental failures**
- **Usability deals with problems arising from operating mistakes made by users**
- Security deals with intentional failures created by intelligent parties
  - Security is about computing in the presence of an adversary
  - But security, reliability, and usability are all related

How Systems Fail

- Systems may fail for many reasons, including
- Reliability deals with accidental failures
- Usability deals with problems arising from operating mistakes made by users
- **Security deals with intentional failures created by intelligent parties**
  - Security is about computing in the presence of an adversary
  - But security, reliability, and usability are all related

Apparently Harmless Failures

- donotreply.com

- Some websites use this “fake” domain, sending mail with reply-to of: donotreply@donotreply.com

Two Key Themes of this Course

1. How to **think** about security
   – The "Security Mindset" – a "new" way to think about systems
2. **Technical aspects of security**
   – Vulnerabilities and attack techniques
   – Defensive technologies
   – Topics including: software security, cryptography, malware, web security, web privacy, smartphone security, authentication, usable security, anonymity, physical security, security for emerging technologies

What This Course is Not About

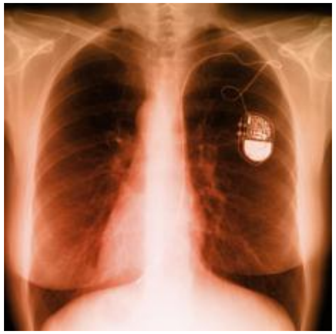
- Not a **comprehensive** course on computer security
  - Computer security is a broad discipline!
  - Impossible to cover everything in one quarter
  - So be careful in industry or wherever you go!
- Not about all of the latest and greatest attacks
  - Read news
- Not a course on ethical, legal, or economic issues
  - We will touch on these issues, but the topic is huge
- Not a course on how to "hack" or "crack" systems
  - Yes, we will learn about attacks ... but the ultimate goal is to develop an understanding of attacks so that you can build more secure systems

Security: Not Just for PCs

smartphones

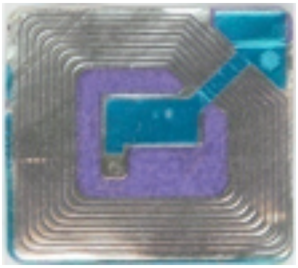
voting machines

EEG headsets



medical devices

wearables



RFID

mobile sensing platforms

cars

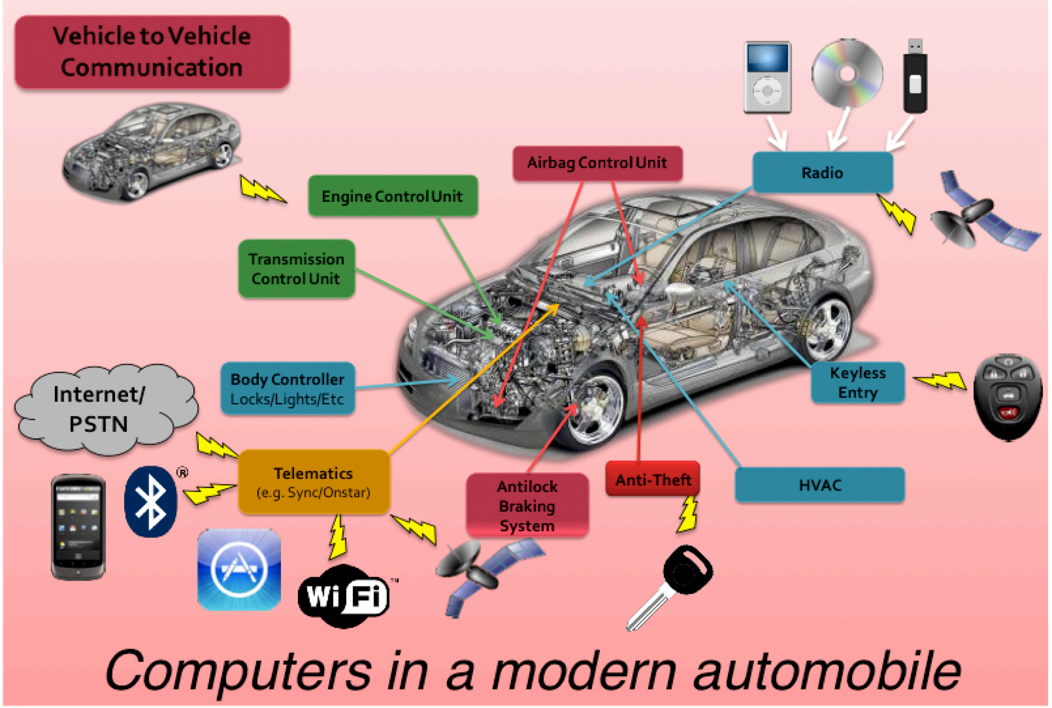
game platforms

airplanes

Example: Modern Automobiles

Modern automobiles contain dozens of computers.

Those computers control nearly everything in the car, including locks, lights, brakes, the engine, the airbags, etc.



Vehicle to Vehicle Communication
Airbag Control Unit
Radio
Engine Control Unit
Transmission Control Unit
Body Controller Locks/Lights/Etc
Keyless Entry
Internet/ PSTN
Telematics (e.g. Sync/Onstar)
Antilock Braking System
Anti-Theft
HVAC
Wi Fi

Computers in a modern automobile

Who might want to attack? Why, and how?

Learning the Security Mindset

- Several approaches for developing "The Security Mindset" and for exploring the broader contextual issues surrounding computer security
  - Homework #1
    - Current event reflections and security reviews
    - May work in groups of up to 3 people (groups are encouraged – **lots of value in discussing security with others!**)
  - In class discussions and activities
  - Participation in forums (e.g., critiquing movies)

“Homework #0”: Class Survey

- Find it from the Schedule or Assignments page of the course website
- Fill it out by Friday (simple questions about you and how I can help you learn)

Ethics Form

- Find it from the Schedule or Administrivia page of the course website

- Sign it (digitally) by October 5 to receive a non-zero grade in the class.

Homework #1: The Security Mindset

- Due Monday, October 10

- Review 1) a current event and 2) a technology, to practice the security mindset, threat modeling, and explaining security topics to different audiences.

Todo

- Class survey! (By Friday – do it now!)
- Ethics form! (Oct 5 – do it now!)

- Security reviews (Oct 10)
  - Start forming groups (forums are available) and thinking about events and technologies you'd like to review.