01. Course Introduction; Threat Modeling

Ben Zhao, Blase Ur, David Cash

October 1st, 2018

CMSC 23200 / 33250

THE UNIVERSITY OF CHICAGO

Today’s class

- Course requirements / structure
- The security mindset
- Threat modeling

Website / Syllabus

https://www.classes.cs.uchicago.edu/archive/2018/fall/23200-1/

or

https://bit.ly/2OmeFa2

Undergraduate (2-) vs. Graduate (3-)

- Shared requirements:
  - 7 assignments
  - Take-home, open-book midterm exam
  - Closed-book final exam
  - Class participation
- Graduate (3-) only:
  - Research project in groups of 2 – 3 students
  - Weekly reading “reviews”

Are you not signed up yet?

- Currently 75 students enrolled
  - 61 for 23200 (undergraduate)
  - 14 for 33250 (graduate)
- Want to switch from 23200 to 33250?
  - Submit a consent request
- Do you not have a seat at all?
  - We will try our best…
  - …but there are 26 pending consent requests

Three instructors?!?

- **David Cash**: Cryptography, secure communication, security protocols
  - Office hours Tuesdays 2:30p – 4:00p or by appointment
  - Office: Crerar 353
  - Also teaches classes on crypto

Three instructors?!?

- **Ben Zhao**: Network security, underground economies, anonymity, ML security
  - Office hours by appointment
  - Office: Crerar 369
  - Also teaches classes on networks

Three instructors?!?

- **Blase Ur**: Authentication, access control, web security, systems security
  - Office hours Mondays 1:00p - 2:00p or by appointment
  - Office: Crerar 363
  - Also teaches classes on usable security

Two TAs

- **Minhaj Khan**
  - Office hours Thursdays 11:00a – 12:00p or by appointment
  - Office: Crerar 391 Desk 19

- **Xu Zhang**
  - Office hours Wednesdays 1:00p – 2:00p or by appointment
  - Office: Crerar 381 Desk 20

The security mindset

- Imagine that you anticipate Ben Zhao has a copy of the midterm exam. You want this exam.
- We will now go through an exercise in **threat modeling**, which is the process of systematically identifying and enumerating the potential threats to a system

Step 1: Identify assets of value

- What are those assets?
  - In this case, a copy of the exam
- What is the value of those assets?
  - Can we place a dollar value on having a copy of the exam?
  - What factors impact this calculation?
    - Your expected score on the exam without cheating
    - How your grade in this class will impact your future
    - Whether other people will get a copy

Where might the exam be stored?

- Ben's laptop
- Ben's desktop
- Ben's tablet
- Ben's phone
- Ben's UChicago email
- Ben's personal email
- Blase's / David's / TAs' email accounts or computers
- Github / other version-control repository
- The memory of a printer / copier in the CS building
- A recycling bin or garbage can in Crerar
- A garbage dump somewhere in the city of Chicago
- Email account or computer of an exam proctor / accommodations coordinator / admin

Step 2: Enumerate the attack surface

- The **attack surface** is the full set of points of entry into the system
- What is the attack surface for Ben's email?
  - Guess his password
  - Compromise UChicago's email server
  - Make friends with UChicago IT (*insider threat*)
  - Passively watch network traffic
  - …(many more)

Attack surface for laptop

- Physical access to laptop
  - Pick lock in Ryerson
  - Dress up like Ben and get UCPD to help you get back into “your” office (*social engineering*)
  - Dress up like admin staff or custodial staff
  - Bribe his family
  - Bring a baseball bat to a dark street corner
  - Strategically pull the fire alarm
  - …

Attack surface for laptop

- Remote, virtual access
  - Send Ben a phishing email with a keylogger
  - Send Ben a phishing email asking for his password
  - Try to ssh into his laptop (guess password)
  - Introduce a backdoor into software he uses
  - Introduce a backdoor into the hardware
  - Buy a *zero-day exploit*
  - Conduct a fake tech support scam
  - …

Attack surface for laptop

- Physical proximity to laptop
  - Point a camera at the screen through the window
  - Slide a microphone under the door
  - Drop a USB key outside Ben's office containing a keylogger
  - Eavesdrop on the network traffic
  - Set up your own "UChicago" wifi access point (*rogue AP, active man in the middle attack*)
  - …

Step 3: Model attackers

- Map attackers to the things of value that they are after
- What resources do these attackers have?
  - Are they a casual thief? A computer expert? The FBI? A secretive nation-state?
- How much effort will they expend?
- *Local* vs. *remote* attacker
- *Passive* vs. *active* attacker

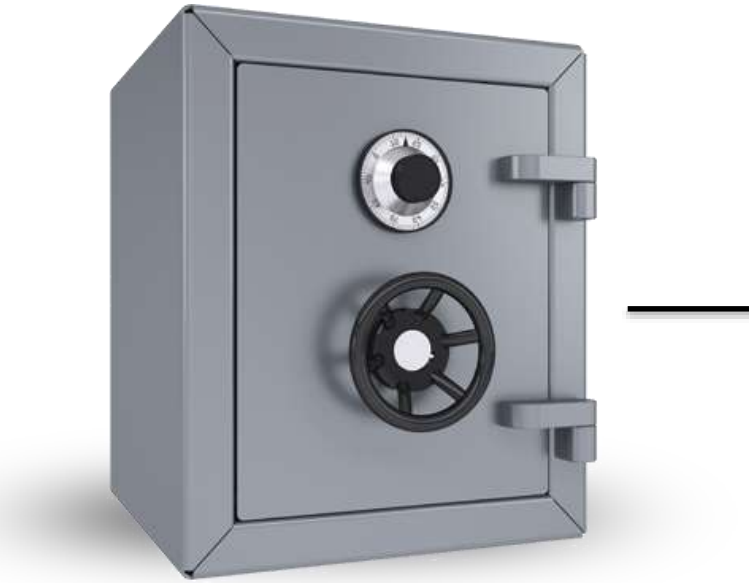
Step 4: Consider mitigations

- How can we minimize the likelihood that each attack vector will be used?
- Weight costs and benefits

Mitigations can be unpleasant

- Some organizations can legally (or physically) compel you to unlock your device
- Destroying a device can be considered obstruction of justice
- Not using cloud services or modern features can be annoying
- Updating / patching devices is annoying
  - And imperfect!

How can we keep something secure?



What properties do we want?

- **Confidentiality**: Information hidden from people who should not be able to view it
- **Integrity**: Information is consistent, accurate, and trustworthy; it has not been secretly modified
- **Availability**: One can readily access the system or resource
- This is the “CIA Model”