02. Modeling Attackers & Threats; Security Architectures

Blase Ur and David Cash
January 8th, 2020
CMSC 23200 / 33250

THE UNIVERSITY OF CHICAGO

The security mindset

- Imagine that you anticipate David Cash has a copy of the final exam. You want this exam.
- We will now go through exercises in **adversary modeling** and **threat modeling**, which is the process of systematically identifying and enumerating the potential attackers and threats to a system

Step 1: Identify assets of value

- What are those assets?
- What is the value of those assets?
  - Can we place a $ value on having 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

What is our security policy?

- What policy characterizes our intentions for access to the exam?

Step 2: Characterize adversaries

- Objectives
- Methods
- Capabilities
- Funding level
- Outsider vs. insider

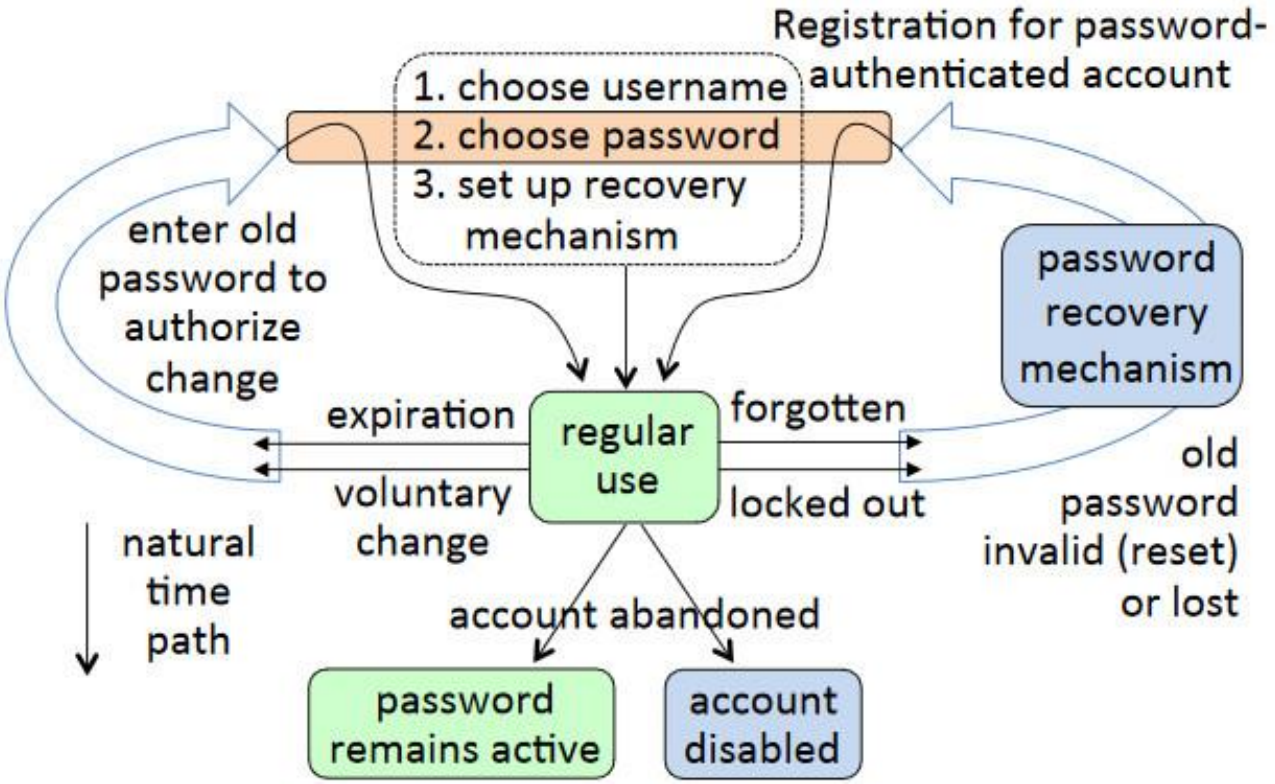
Step 2: Characterize adversaries

- 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

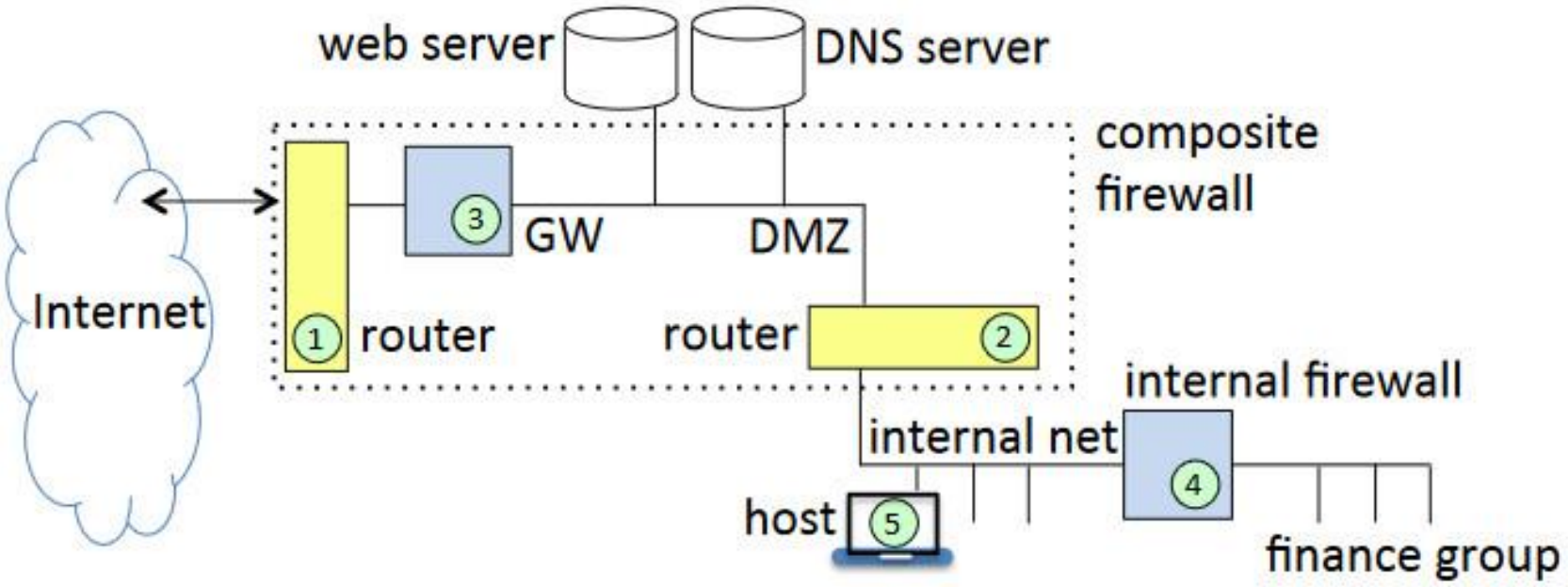
Step 3: Consider user workflow

- Where might the exam be stored?
  - Think about diagramming data flows and the data lifecycle (Fig. 1.7 in the textbook)
  - Think about diagramming the system architecture (Fig. 1.6 in the textbook)
  - “What can go wrong?”

Data lifecycle



System architecture



Where might the exam be stored?

Where might the exam be stored?

- David's laptop
- David's desktop
- David's tablet
- David's phone
- David's UChicago email
- David'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 4: Enumerate possible attacks

- The **attack surface** is the full set of points of entry into the system
- Draw attack trees

Attack surface for David's email?

Attack surface for David's email?

- Guess his password
  - How does Duo factor in?
- Compromise UChicago's email server
- Be friends with UChicago IT (*insider threat*)
- Passively watch network traffic
- …(many more)

Attack surface for laptop

Attack surface for laptop

- Physical access to laptop
  - Pick lock in Crerar
  - Dress up like David 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 David a phishing email with a keylogger
  - Send David 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 David'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 5: 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 a 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!