CSE P 564: Computer Security

Instructor: Yoshi Kohno
TA: Adrian Sham
Course Syllabus


• Primary Goals:
  – Develop “security thinking” (e.g., identifying and assessing threats, thinking about defenses, looking at “unusual targets”)
  – Survey (some) key emerging areas in computer security
  – Help you develop concrete practices on how to be secure, both as a user and as a system designer / developer (or whatever your position/occupation is)
Mailing lists

• Make sure you’re email address is on the course mailing list
  – We will use this for announcements

• Cse-pmp-564-staff@cs – email address to reach course staff
Assignments

• Research readings
• Assignment 1: Security Reviews
• Assignment 2: How to be Secure (for Users)
• Assignment 3: How to Design/Build for Security (for people in your position)
• Course URL: http://courses.cs.washington.edu/courses/csep564/15wi/
Definitions

- **Computer security / cyber security**: Computation in the presence of an adversary.
The Security Mindset

• Suppose that a new product is announced.

• Traditional mindset: “This product sounds cool. I wonder how I might use it.”

• Security mindset: “This product sounds cool. I wonder how I might use it. And I wonder how I (or someone else) might abuse it.”
Today’s Outline

• Security thinking in the physical world
• Case studies of computer security vulnerabilities and threat models: non-traditional systems
• Threat modeling and computer security thinking
Today’s Outline

• Security thinking in the physical world
• Case studies of computer security vulnerabilities and threat models: non-traditional systems
• Threat modeling and computer security thinking
Question 1

- Conduct a thought experiment for bringing onto the airplane an item prohibited by TSA regulations that could be used by hijackers.

(Question from the homework assignment for the 2014 Congressional Cyber Security Bootcamp.)
Question 2

- How would you change TSA (or other) practices to defend against one of the attack methods that we just discussed?
Question 3

• How would you bypass the protection mechanisms that we just discussed?
Question 4

• Suppose we implement as many defenses as we can think of. How can we be sure that we have protected against everything?
Question 5

• Question 1 was about hijacking. What other nefarious things, besides hijacking, might current TSA procedures not protect against?
Example Lessons Thus Far

- Cat-and-mouse game: **ongoing attack and defend cycle** inevitable
- **The world surrounding a technology can change**, creating new threats
- There is a diversity of attack techniques
- There is a diversity of attacker goals
- Insider attacks can be serious
- Security risks can arise at the intersection / interface points between systems
- Security is not just about prevention, but about monitoring and deterrence
- Security is risk management
Today’s Outline

• Security thinking in the physical world
• Case studies of computer security vulnerabilities and threat models: non-traditional systems
• Threat modeling and computer security thinking
Three Examples Consumer Technologies:

Medical Devices, Children’s Toys, and Cars
Example Lessons Thus Far

- All technologies have potential security risks
  - Including non-traditional technologies, like cars, medical devices, and toys
  - Including technologies without wireless interfaces
- Can be hard to know when a technology has been compromised
- Can be hard to identify the attackers involved (anonymity)
- Attackers and targets can be thousands of miles apart, but still connected via computers
- Defense is difficult
  - Attackers only need one way to win; defenders must defend against everything
  - A big potential oversight: not anticipating attackers, their goals, and their methods
Today’s Outline

• Security thinking in the physical world
• Case studies of computer security vulnerabilities and threat models: non-traditional systems
• Threat modeling and computer security thinking
Traditional Computer Security Goals

• Confidentiality
• Integrity
• Availability
Threat Modeling

• Threat modeling is a good way to develop the security mindset

• Steps (one way):
  – Accurately describe the system
  – Identify the assets
  – Identify potential adversaries
  – Identify potential attack methods
  – Evaluate risk
Example Adversaries (unordered)

- Consumers
- Suppliers
- National governments
- Activists
- Organized crime
- Business competitors
- Reporters
- Friends
- Ex-friends
- Family
The Security Cards
The Security Cards

• Computer security threat brainstorming toolkit
  – Educational purposes
  – Threat modeling purposes
• Extensible – no single deck can anticipate all possible issues
Human Impacts

- Emotional Wellbeing
- Financial Wellbeing
- Personal Data
- Physical Wellbeing

- Relationships
- Societal Wellbeing
- The Biosphere
- Unusual Impacts
Adversary’s Motivations

- Access of Convenience
- Curiosity or Boredom
- Desire or Obsession
- Diplomacy or Warfare
- Malice or Revenge
- Money
- Politics
- Protection
- Religion
- Self-Promotion
- Unusual Motivations
- World View
Adversary’s Resources

- Expertise
- A Future World
- Impunity
- Inside Capabilities
- Inside Knowledge

- Money
- Power or Influence
- Time
- Tools
- Unusual Resources
Adversary’s Methods

• Attack Cover-up
• Indirect Attack
• Manipulation or Coercion
• Multi-Phase Attack

• Physical Attack
• Process
• Technological Attack
• Unusual Methods
Exercise: Setup

• What type of computer systems are important to you at work?
• Or automobiles
• Or Airbnb
Exercise: Card Sorting

• In groups of three or four, sort the Human Impact deck in order of relevance*

• Write down the order, as well as your reasons

• Note *: There is no “right” ordering; part of the value is in discussing the tradeoffs.
Explore Adversary Motivations

• For each card in the Adversary’s Motivations suit: Brainstorm an adversary that might have that motivation

• Write down notes about your adversaries
Explore Adversary Resources and Adversary Methods
# Threat Matrix (example: e-voting)

|                | Voter | Election official | Manufacturer | ...
|----------------|-------|-------------------|--------------|-------
| Privacy of vote|       |                   |              |       |
| Integrity of vote |      |                   |              |       |
| Availability of voting system |     |                   |              |       |
| Confidence in election |    |                   |              |       |
| ...             |       |                   |              |       |
Example Lessons Thus Far

• Security is not a binary – there is no such thing as “secure” or “insecure;” computer security is about risk management

• Diversity of assets, adversaries, goals, and methods

• Subtlety of computer security

• Explored tools to assist in thinking about security
On-going Practice

• Look for new computer technology product announcements

• Conduct security reviews of those technologies (Assignment 1)

• Do the security reviews informally, when you have time (e.g., while commuting, while preparing a meal)

• Involve your colleagues in the brainstorming (e.g., over coffee)