FLORIAN ALT & ALBRECHT SCHMIDT

SECURITY IN HUMAN-COMPUTER INTERACTION

WINTER SCHOOL 2018

Based on the lecture “Introduction to Security” by Lorrie Faith Cranor

WHAT IS COMPUTER SECURITY?

- Protecting information systems against misuse and interference
- “Building systems to remain dependable in the face of malice, error or mischance” (Ross Anderson)

PROPERTIES OF A SECURE SYSTEM

- **Confidentiality:**
  information is protected from unintended disclosure (secrecy, privacy, access control)

- **Integrity:**
  system and data are maintained in a correct and consistent condition

- **Availability:**
  systems and data are usable when needed (includes timeliness)

SECRECY, CONFIDENTIALITY, PRIVACY, ANONYMITY

- **Secrecy:** Keep data hidden
  - e.g., Alice kept the incriminating information secret
- **Confidentiality:** Keep (someone else's) data hidden from unauthorized entities
  - e.g., banks keep much account information confidential
- **Privacy:** Use/disclose a person's data according to a set of rules
  - e.g., to protect Alice's privacy, company XYZ removed her name before disclosing information about her purchases
- **Anonymity:** Keep identity of a protocol participant secret
  - e.g., to hide her identity from the web server, Alice uses The Onion Router (TOR) to communicate

INTEGRITY, AUTHENTICATION

- **Data integrity:** Ensure data is "correct" (i.e., correct syntax & unchanged) / Prevents unauthorized or improper changes
  - e.g., Trent always verifies the integrity of his database after restoring a backup, to ensure that no incorrect records exist
- **Entity authentication or identification:** Verify the identity of another protocol participant
  - e.g., Alice authenticates Bob each time they establish a secure connection
- **Data authentication:** Ensure that data originates from claimed sender
  - e.g., For every message Bob sends, Alice authenticates it to ensure that it originates from Bob

ATTACKERS EXPLOIT BUGS

- Software bugs
- Hardware bugs
- Humans (social engineering)

EXERCISE I: SPEED DATING

Discuss in groups of two the following questions:

- Why are you not encrypting your email and why are you encrypting WhatsApp?
- Why are secure systems often not usable?
- How do humans make interactive systems unsafe?
- Why are humans the weak link?
- How can we make humans aware that they are putting systems at risk?

EXERCISE II: DESIGNING A PHISHING ATTACK

- What is a phishing attack?

- Design a phishing attack to find out who reviewed your CHI paper!

(10 Minutes to design an attack, groups of 4)

THINK LIKE AN ATTACKER

- **Adversary is targeting assets, not defences**
- **Will try to exploit the weakest part of the defences**
  - E.g., bribe human operator, social engineering, steal (physically) server with data

MODELING THE ATTACKER

- **What type of action will they take?**
  - Passive (look, but don't touch)
  - Active (look and inject messages)
- **How sophisticated are they?**
- **How much do they care? What resources do they have?**
  - How much time/money will they spend?
- **How much do they already know?**
  - External / internal attacker?

EXPLOITING BUGS AS A NUISANCE

- **Pranks, to be annoying**
  - Newsday tech writer & hacker critic found …
    - Email box jammed with thousands of messages
    - Phone reprogrammed to an out of state number where caller's heard an obscenity-loaded recorded message [TimeMagazine, December 12, 1994]
- **May be costly**
  - MyDoom (2004) - $38.5 billon
  - SoBig (2003) - $37.1 billion
  - Love Bug (2000) - $15 billion
  - Code Red (2001) - $2 billion

EXPLOITING BUGS FOR PROFIT

- Credit card and financial account fraud
- Stealing intellectual property or confidential information
- Ransom
- Extortion
- Stealing computing resources to sell

BASIC SECURITY ANALYSIS

How do you secure X? Is X secure?

1. What are we protecting?
2. Who is the adversary?
3. What are the security requirements?
4. What security approaches are effective?

Based on the lecture “Introduction to Security” by Lorrie Faith Cranor

1. WHAT ARE WE PROTECTING?

- Enumerate assets and their value
- Understand architecture of system
- Useful questions to ask

  - What is the operating value, i.e., how much would we lose per day/hour/minute if the resource stopped?
  - What is the replacement cost? How long would it take to replace it?

2. WHO IS THE ADVERSARY?

- **Identify potential attackers**
  - How motivated are they?
- **Estimate attacker resources**
  - Time and money
- **Estimate number of attackers, probability of attack**

COMMON (ABSTRACT) ADVERSARIES

- **Attacker action**
  - Passive attacker: eavesdropping
  - Active attacker: eavesdropping + data injection
- **Attacker sophistication**
  - Ranges from script kiddies to government-funded group of professionals
- **Attacker access**
  - External attacker: no knowledge of cryptographic information, no access to resources
  - Internal attacker: complete knowledge of all cryptographic information, complete access (result of system compromise)

3. WHAT ARE THE SECURITY REQUIREMENTS?

- **Enumerate security requirements**
  - Confidentiality
  - Integrity
  - Authenticity
  - Availability
  - Auditability
  - Access control
  - Privacy
  - …

Based on the lecture “Introduction to Security” by Lorrie Faith Cranor

4. APPROACHES TO ACHIEVE SECURITY

- **No security**
  - Legal protection (deterrence)
  - Innovative: get protection through patent law
- **Build strong security defence**
  - Use cryptographic mechanisms
  - Perimeter defence (firewall), VPN
- **Resilience to attack**
  - Multiple redundant systems (“hot spares”)
- **Detection and recovery (& offence ?)**
  - Intrusion detection system
  - Redundancy, backups, etc.
  - Counterstrike? (Legal issues?)

THREAT MODELS

- **Can’t protect against everything**
  - Too expensive
  - Too inconvenient
  - Not worth the effort
- **Identify most likely ways system will be attacked**
  - Identify likely attackers and their resources
    - Dumpster diving or rogue nation?
  - Identify consequences of possible attacks
    - Mild embarrassment or bankruptcy?
  - Design security measures accordingly
    - Accept that they will not defend against all attacks

Based on the lecture “Introduction to Security” by Lorrie Faith Cranor