Computer Security and Privacy

What is security?

- In the context of computers, **security** generally means three things:
  - Confidentiality
    - Access to systems or data is limited to authorized parties
  - Integrity
    - When you ask for data, you get the “right” data
  - Availability
    - The system or data is there when you want it
- A computing system is said to be **secure if it has all three properties**
  - **Well, usually**

Security and reliability

- Security has a lot to do with reliability
- A secure system is one you can rely on to (for example):
  - Keep your personal data confidential
  - Allow only authorized access or modifications to resources
  - Give you correct and meaningful results
  - Give you correct and meaningful results when you want them

What is privacy?

- There are many definitions of privacy
- A useful one: "informational self-determination"
  - This means that you get to control information about you
  - "Control" means many things:
    - Who gets to see it
    - Who gets to use it
    - What they can use it for
    - Who they can give it to
    - etc.

Example: PIPEDA

- PIPEDA (Personal Information Protection and Electronic Documents Act) is Canada's private-sector privacy legislation
- It lists ten Fair Information Principles companies have to abide by:
  - Be accountable
  - Identify the purpose of data collection
  - Obtain consent
  - Limit collection
  - Limit use, disclosure and retention
  - Be accurate
  - Use appropriate safeguards
  - Be open
  - Give individuals access
  - Provide recourse

Security vs. privacy

- Sometimes people place security and privacy as if they're opposing forces.

- Are they really? Do we have to give up one to get the other?

Who are the adversaries?

- Who's trying to mess with us?
- Various groups:
  - Murphy
  - Amateurs
  - “Script kiddies”
  - Crackers
  - Organised crime
  - Terrorists
- Which of these is the most serious threat today?

How secure should we make it?

- Principle of Easiest Penetration
  - "A system is only as strong as its weakest link"
  - The attacker will go after whatever part of the system is easiest for *him, not most convenient for you.*
  - *In order to build secure systems, we need to learn how to think like an attacker!*
  - *How would you get private information from the US Social Security Administration database?*
- Principle of Adequate Protection
  - "Security is economics"
  - Don't spend $100,000 to protect a system that can only cause $1000 in damage

Some terminology

- Assets
  - Things we might want to protect, such as:
    - Hardware
    - Software
    - Data
- Vulnerabilities
  - Weaknesses in a system that may be able to be exploited in order to cause loss or harm
  - e.g., a file server that doesn't authenticate its users

Some terminology

- Threats
  - A loss or harm that might befall a system
  - e.g., users' personal files may be revealed to the public
  - There are four major categories of threats:
    - Interception
    - Interruption
    - Modification
    - Fabrication
  - When we design a system, we need to state a threat model
    - This is the set of threats we are undertaking to defend against
    - Whom do we want to stop from doing what?

Some terminology

- Attack
  - An action which exploits a vulnerability
  - e.g., telling the file server you are a different user in an attempt to read or modify their files
- Control
  - Removing or reducing a vulnerability
  - You control a vulnerability to prevent an attack and block a threat.
  - How would you control the file server vulnerability?
  - Our goal: control vulnerabilities

Methods of defence

- How can we defend against a threat?
  - Prevent it: block the attack
  - Deter it: make the attack harder or more expensive
  - Deflect it: make yourself less attractive to attacker
  - Detect it: notice that attack is occurring (or has occurred)
  - Recover from it: mitigate the effects of the attack
- Often, we'll want to do many things to defend against the same threat
  - “Defence in depth”

Example of defence

- Threat: your car may get stolen
- How to defend?
  - Prevent: is it possible to absolutely prevent?
  - Deter: Store your car in a secure parking facility
  - Deflect: Use “The Club”
  - Detect: Car alarms, LoJack
  - Recover: Insurance

Defence of computer systems

- Remember we may want to protect any of our assets
  - Hardware, software, data
- Many ways to do this; for example:
- Cryptography
  - Protecting data by making it unreadable to an attacker
  - Authenticating users with digital signatures
  - Authenticating transactions with cryptographic protocols
  - Ensuring the integrity of stored data
  - Aid customers' privacy by having their personal information automatically become unreadable after a certain length of time

Defence of computer systems

- Software controls
  - Passwords and other forms of access control
  - Operating systems separate users' actions from each other
  - Virus scanners watch for some kinds of malware
  - Development controls enforce quality measures on the original source code
  - Personal firewalls that run on your desktop

Defence of computer systems

- Hardware controls
  - (Not usually protection of the hardware itself, but rather using separate hardware to protect the system as a whole.)
  - Fingerprint readers
  - Smart tokens
  - Firewalls
  - Intrusion detection systems

Defence of computer systems

- Physical controls
  - Protection of the hardware itself, as well as physical access to the console, storage media, etc.
  - Locks
  - Guards
  - Off-site backups
  - Don't put your data centre on a fault line in California

Defence of computer systems

- Policies and procedures
  - Non-technical means can be used to protect against some classes of attack
  - If an employee connects his own Wi-fi access point to the internal company network, that can accidentally open the network to outside attack.
    - So don't allow the employee to do that!
  - Rules about changing passwords
  - Training in best security practices