Introduction of Computer and Network Security

1 Overview

A good security professional should possess two important skills: (1) the sense of security, and (2) the knowledge of security principles. I hope that students who finish this course can possess both. Possessing does not mean "knowing"; it means "being able to apply these skills".

2 Risks and Threats

- Risks when using computer systems:
  - You are working on your project in a public library, and you have remotely logged into your department's UNIX server. You have to leave for one minute, and you feel lazy and decide not to lock the screeen of your computer. What is the most severe damage that you can get if a malicious person takes this oppurtunity? How much time does it a malicious person need to achieve the most severe damage?
  - You go to a public lab and wants to use a computer there to remotely login to your department's computer or conduct online banking; what is the risk that you are facing?
  - You go to an ATM machine to get cash in a nice neighbourhood (i.e., there is no forced robbery), what is your risk?
- Risks when setting up computer systems.
  - You want to access your office computer from your home, so you set up your office computer so you can access its desktop remotely. What is the risk?
  - You intall a wireless access point in your house to build a wireless network. What is the risk?
  - You are system administrator, and turn several programs into privileged programs, so you will not be bothered by some of the tasks (users can use those privileged programs to finish those tasks). What is the risk?
- Risks when developing computer systems.
  - Your program has a few buffer-overflow problem, but you are under pressure to release the software product in time, and decide not to fix this bug for this release. What is the risk?
  - Your company just wins the bid for building e-voting systems for the government. What are the risks that you system might face?
  - You are developing an online shopping web site for a store. What are the risks that you will face.
- *Sense* of Security: The ability to see and foresee the risks. If you cannot systematically enumerate the risks in the above examples, you do not have a good sense of security. I hope that after this course, you can gain a good sense of security, and be able to assess your risks when you are to use, setup, or develop computer systems.
- *Lessons learned from previous classes:* students in this class in the past did not pay enough attention to foster the sense of security. Every semester in the demonstration of final project, I saw students (not just a few, but majority of them) who demonstrated excellent functionalities of their systems, but

showed no sense of security. They spent many hours implementing a useful functionality for their systems, but did not spend a single second to think about the security consequence of that functionality (e.g., should we put in access control to prevent the functionality from being abused by malicious users to gain extra privileges?)

3 Countermeasures

- Methods: There are three lines of defense.
    1. Prevention: the focus of this course.
        - prevent it: make it impossible
        - deter it: make it harder
        - deflect it: make other targets more attractive
    2. Detection
        - monitoring
        - intrusion detection
    3. Recovery
        - recover the data
        - identify the damage
        - find the culprit: forensics
- How does prevention work?
    - Policies (IST courses)
    - Cryptography
        - Cryptography is not just for encryption; it can be used to achieve many security-related objectives, such as digital cash, timestamping, secure multiparty computation, e-voting, e-bidding, etc.
        - We only cover some basic cryptography in this class.
    - Control (the key component of this course)
        - Examples: make sure that only those with security clearance can read a file.
        - Hardware control
        - Software control
- How could prevention not work correctly?
    - Vulnerabilities
    - Malicious program: virus, trap doors, etc.
    - Incorrect use of controls
    - Users' mistakes
- How to achieve correct prevention?
    - Security engineering principles
    - Awareness of risk
    - Secure programming

4 The Meaning of Computer Security

When we talk about "computer security", we mean that we are addressing three very important aspects of any computer-related system.

- Confidentiality
- Integrity
- Availability

The meanings of these three words (CIA) are quite broad. For different applications, the interpretation of CIA is different.

- Confidentiality: access (reading, viewing, printing, knowing, etc.)
  - Contents : encryption (cryptography)
  - Existence of data: steganography. For example, stock investigation, prisoner, spy, watermarking
  - Resource hiding: operating system information and configuration
  - Fingerprinting
  - Identity: (anonymity)
- Integrity: modification (includes writing, changing, changing status, deleting, and creating).
  - Data integrity
  - Program integrity
  - System integrity
  - Identity integrity (non-repudiation)
  - Origin (location) integrity (e.g. network traceback)
- Availability.
  - Denial of service
- Examples: what category do they belong to?
  - TCP SYN flooding
  - Sniffering
  - Faked identity
  - ATM machine spoofing
  - Saving passwords in a plaintext file