Security Overview

1 Risks and Defending Measures

- Risks
  - There is a public computer in the classroom, and you are about to log into your account on that computer; what are the risks?
  - You are working on your project in Bird library, and you leave your laptop unattended for a while, what are the risks?
  - You are running a web server on your machine, what are the risks? How do you lower the risks?
  - A trick question: what is the most secure system?
    - A system that is disconnected from the networks, shutdown, dead, and useless.
  - Vulnerabilities: the most common attack is to exploit known software vulnerabilities.
  - An important objective of this course: to develop sharp risk-awareness skills, so you can identify potential risks when you use computers, operate computer systems, or develop software.
- Defense Techniques (Three lines of defense)
  - Prevention
    - prevent it: make it impossible
    - deter it: make it harder
    - deflect it: make other targets more attractive
  - Detection
    - monitoring
    - intrusion detection
  - Recovery
    - recover the data
    - identify the damage
    - find the culprit: forensics
  - The focus of this course: prevention
- How does prevention work?
  - Policies (IST courses)
  - Cryptography: Not just the encryption. Examples include digital cash, timestamping, secure multiparty computation, e-voting, e-bidding, etc.
  - Control (the key component of this course)
    - hardware control
    - software control
    - Examples: make sure that only those with security clearance can read this file.

- How could prevention not work correctly?
  - Vulnerabilities
  - Malicious program: virus, trap doors, etc.
- How to achieve correct prevention?
  - Security engineering principles, awareness of risk, secure programming, etc.

2 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
- For different applications, the interpretation of CIA is different.
- Confidentiality: access (reading, viewing, printing, knowing, etc.)
  - Contents : encryption (cryptography)
  - Existence of data: steganography. Example: stock investigation, prisoner, spy, watermarking
  - Resource hiding: operating system information and configuration. Example: 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 (network traceback)
- Availability.
  - Denial of service