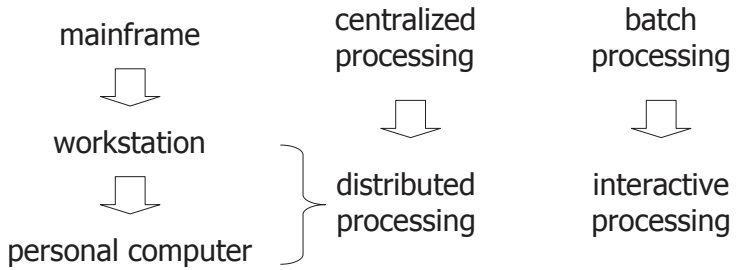
Information Security in Electronic Commerce

Course Introduction

Lecturer: Pei-yih Ting

Backgrounds (1/5)

- Starting from 70's …
  computation model evolves



Backgrounds (2/5)

- Business model evolves

face-to-face
phone / mail order
internet
e-commerce (advertisement, order, contract, payment, banking, e-cash, auction)

cash
check
credit card

Backgrounds (3/5)

- Documentation / archiving method evolves

paper-based documents → electronic documents

file cabinets/warehouse → computer databases

signature / seal → electronic signature

Backgrounds (4/5)

- Information exchange model evolves

face-to-face

⇩

radio / TV broadcast

⇩

email / ftp

⇩

WWW

Backgrounds (5/5)

- Access control technique evolves

key / PIN / password

⇩

magnetic card

⇩

smart card

⇩

biometric authentication

Goals of Technology Advances

- Originally, seeking automation that can help functioning correctly, smoothly, and efficiently without human intervening
- Later, people find that it is necessary to trust many machines and fixed mechanisms to obtain the automations.

  Fairness, security, and privacy play important roles in all operations of social and economic functions.

Security Concepts

- When you drive a car on the road, you are absolutely SAFE if
  - you obey strictly all traffic regulations
  - your car functions well
  - all other drivers obey strictly all traffic regulations
  - all other vehicles on the road function well
  - no earthquake, no tornado, ...
- You can still feel SAFE if you drive carefully and defensively.
- Secure/Safe: nobody can do anything that is harmful to your interests

Security Concepts (cont'd)

- Targets
  - Information (storage / transmission)
  - Systems (Host / clients / devices, Hardware / Software)
- Involving parties
  - Owners
  - Users
  - Adversaries, and others
- Aspects
  - Confidentiality (secrecy)
  - Integrity
  - Authenticity (data / user)

Security Concepts (cont'd)

- Identification / Authentication / Authorization
- Non-repudiation
- Robustness (Fault tolerance)
- Fairness (Verifiability)
- Accountability (Audit)

- Privacy
- Digital Rights Management

Intervening Parties

- All the social and economic activities are open to all eyes. There is always somebody having some other activities intervening with yours.

benign	sharing bandwidth
	sharing storage / data / information
	curiosity (look over the shoulder)
malicious	spying the data on the host / database
	sniffing the data over the network
	intercepting the communication
	jamming the host / network
	spoofing attack or hacking the host
	writing and spreading virus
	DRM, copying of digital materials

Security-related Events

- In the business world…
  - Defacing attacks on company's Web pages
  - Denial of Service attacks on business servers
  - Phishing with a fake Web server that results to fraudulent e-payments or fund transfer
  - Spam advertisements
  - Disruption of business information infrastructure
    - Client machines… blaster, SQL Injection, I Love You …
    - Server … hacking
    - Backend database server … hacking
    - Network … DOS (Red code…)
  - Trade secret / business decision protection … Trojan horse, backdoor, or social engineering

E-Commerce / E-Business

- Electronic information infrastructure
- Electronic transaction / data exchange (EDI) / data processing / data archiving
- Automation of advertisement / ordering / payment / distribution / banking / customer service
- B2B / B2C internet store

  Kimo/Yahoo Taiwan auction

  2,000 sale items (2001) -> 3,000,000 items (05)

  estimated NTD 35,000,000,000 sales in 2005

Adversaries and Their Objectives

- Adversaries: business opponents / individual crackers / disgruntle former employees
- Objectives: (for self interest, curiosity, or revenge)
  - Peeking trade secret / learning business decisions
  - Defaming business reputation: paralyze business information supporting system, DOS attack on internet business platform, defacing the web pages
  - Causing direct business losses: fraudulent business contract, deceived ordering, fake supplying
  - Gaining direct advantage through fraudulent fund transfer

Main Topics Around e-Commerce Security

- Web page / Internet business platform security
- Information system security
  - Computer system security
  - Network security
  - Security practice principles
  - Data transmission / storage security
- Secure ordering / payment system
- E-cashes
- E-auctions / e-agents
- Computer related crimes and computer forensics

Goals of this courses!

Textbook & References

- Textbook:
  - Information Security Illuminated, by Solomon and Chapple, Jones and Bartlett, 2005
- References:
  - 電子商務安全技術與應用, 林祝興、張真誠, 旗標, 2004
  - 資訊安全入門, 賴溪松、葉育斌, 全華

Course Activities

- Class lectures Tuesday 1:00-4:00
- Class discussions
- Assignments
  http://squall.cs.ntou.edu.tw/InformationSecurity/Assign
- Group assignments and presentations
  http://squall.cs.ntou.edu.tw/InformationSecurity/GroupAssign
- Auxiliary software labs.
  http://squall.cs.ntou.edu.tw/InformationSecurity/SoftwareLabs
- Office hours Wednesday 12:20-14:00

Auxiliary Software Labs

- Anti-virus software
- Anti-spam software
- SSH client (putty and sftp)
- Apache SSL setup
- GNUPG / SMIME (Keys and Certificates)
- Brute-force dictionary attack (John, L0phtCrack)
- Vulnerability Scanners (Saint, Nessus, MBSA, CISecurity)
- Md5, sha, tripwire
- Fingerprinting (nmap, sprint, xprobe2)
- Firewall (Sygate, ICF, BlackICE)
- Intrusion detection system (BlackICE)
- VPN (FreeSWAN)

Evaluations

- Class involvement 10%
- Assignments 30%
- Group Assignment Presentations 15%
- Midterm exam 20%
- Final exam 25%