# Chapter 10:
# Security

## Electronic Commerce

# Objectives

- Security requirements
- Authentication
- Access control

# Security requirements

- Confidentiality
- Integrity
- Availability
- Non-repudiation

| Requirement | Meaning |
|---|---|
| Secrecy | Prevent unauthorized persons from reading messages and business plans, obtaining credit card numbers, or deriving other confidential information. |
| Integrity | Enclose information in a digital envelope so that the computer can automatically detect messages that have been altered in transit. |
| Availability | Provide delivery assurance for each message segment so that messages or message segments cannot be lost undetectably. |
| Key management | Provide secure distribution and management of keys needed to provide secure communications. |
| Nonrepudiation | Provide undeniable, end-to-end proof of each message's origin and recipient. |
| Authentication | Securely identify clients and servers with digital signatures and certificates. |



**FIGURE 10-2** Requirements for secure electronic commerce

# Policy and mechanism

- Need to have a security policy and appropriate security mechanism
  - A security policy is a statement of what is, and what is not, allowed
  - A security mechanism is a method, tool, or procedure for enforcing a security policy
- A security mechanism can implement a policy by
  - Prevent the attack
  - Detect the attack
  - Recover from the attack
- In designing policy, need to identify threat
  - A threat is a potential violation of security

# Security threats

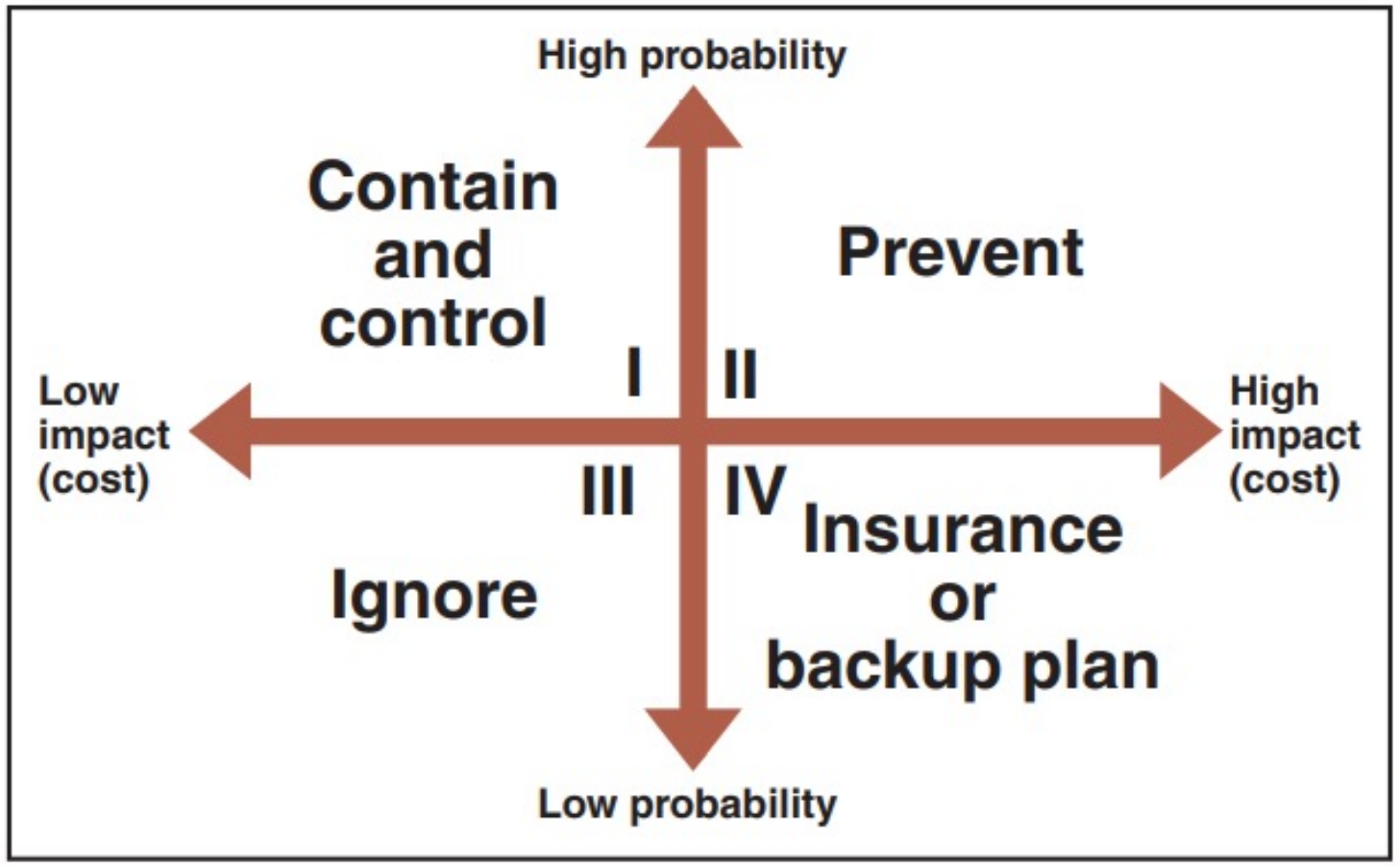
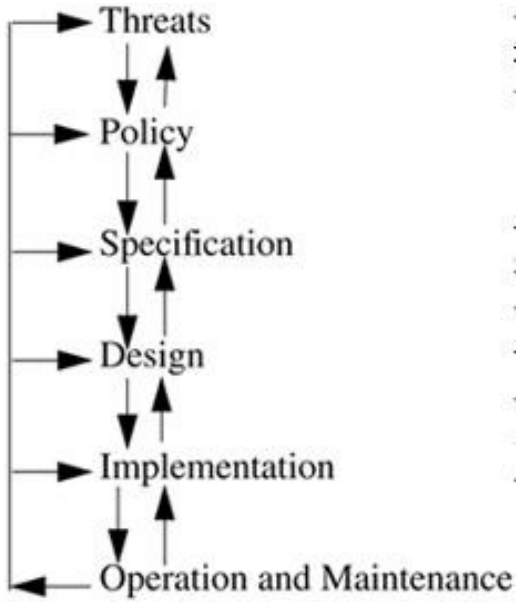





FIGURE 10-1 Risk management model

# Security threats

- Type of threats
  - Disclosure: unauthorized access to information
  - Deception: acceptance of false data
  - Disruption: interruption or prevention of correct operation
  - Usurpation: unauthorized control of some part of a system
- The security life cycle



# Common attacks

- Snooping: unauthorized interception of information, is a form of disclosure
  - Passive
  - Passive wiretapping: snooping happen on a network
- Modification (or alteration): deception, disruption, and usurpation
  - Active
  - Active wiretapping: modification happen on a network
  - Example: man-in-the-middle attack

# Common attacks

- Masquerading (or spoofing): impersonation of one entity by another, is a form of deception, and usurpation
  - Passive or active
- Repudiation of origin: false denial that an entity sent something, is a form of deception
  - Active
- Denial of service: long-term inhibition of service, is a form of usurpation
  - Active
  - May happen at the source, the destination, or the communication path

# Common attacks

- Malicious code: is a set of instructions that cause a site's security policy to be violated
- Trojan horse: is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect
- Example: this UNIX script is named ls, what does it do?
  - cp /bin/sh /tmp/.xxsh
  - chmod o+s,w+x /tmp/.xxsh
  - rm ./ls
  - ls $*

# Common attacks

- Computer virus: is a program that inserts itself into one or more files and then performs some actions
  - A boot sector infector is a virus that inserts itself into the boot sector of a disk
  - An executable infector is a virus that infects executable programs
  - An encrypted virus is one that enciphers all of the virus code except for a small decryption routine
  - A polymorphic virus is a virus that changes its form each time it inserts itself into another program
  - A macro virus is a virus composed of a sequence of instructions that is interpreted, rather than executed directly

# Common attacks

- Computer worm: is a program that copies itself from one computer to another
- Defense: multilevel strategy
  - 1. Written policies and procedures.
  - 2. User awareness and education.
  - 3. Physical security.
  - 4. Product selection, configuration, and maintenance.
  - 5. Password management.
  - 6. Anti-virus software for servers, clients, and electronic mail.
  - 7. Adequate system backups.

# Authentication

- Authentication is the process of verifying the identity a subject claims it to be
- The subject must provide information to enable the system to confirm its identity
  - Something the subject knows
  - Something the subject has
  - Something the subject is
  - Combination of them
- Authentication mechanism
  - Password
  - Challenge-response
  - Biometrics
  - Multi-factor

# Authentication

- Password
  - Based on “something the subject knows”
  - The subject supplies a password, and the system verifies it against the stored database
  - How to keep the passwords secret even from the administrators? => using a one-way hash function
- Attacks on password systems
  - Dictionary attack: trial and error, using a list of possible passwords
  - Brute force attack: trying every possible passwords
  - Rainbow table: pre-computed table for reversing cryptographic hash functions

# Authentication

- Defending the password system
  - Users need to use “good” password
  - Theorem: let the expected time required to guess a password be T, then T is maximum when the selection of any of a set of possible passwords is equals
  - Random computer-generated passwords: strong, but difficult for human users
  - Pronounceable computer-generated passwords: compromise between passwords selected by users and generated by computer randomly
  - Password aging: a password must be changed after some period of time or after some event has occurred

# Authentication

- Challenge-response
  - The fundamental problem with password: reusable
  - Idea: using passwords that change each time it is used
  - Challenge-response authentication:
    - Server and user agree on a function f
    - Server sends a random message m (the challenge) to user, and user replies with the transformation r = f(m) (the response). Server validates r by computing it separately
    - This is a form of one-time password
    - Also based on “something the subject knows”

# Authentication

- Challenge-response example: CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)


  - Challenge-response authentication (that you are human)
    - What is challenge, what is response?
  - Easy for authenticated subjects (human) but difficult for unauthenticated ones: is that assumption still valid now?

# Authentication

- Types of Captcha

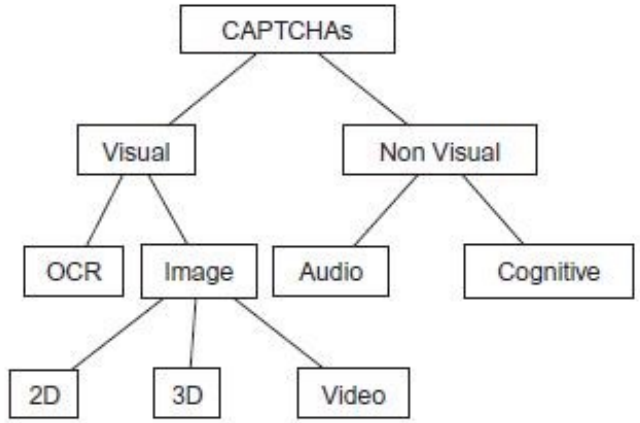



FIG. 8. Different types of CAPTCHAs.

- Attacks on Captcha system
  - Blind guessing
  - AI attacks
  - Relay attacks: Man in the middle, outsourcing, collusion attacks

# Authentication

- Biometrics
  - The automated measurement of biological or behavioral features that identify a person
  - Based on “something the subject is”
  - Many features can be used
    - Fingerprints
    - Voice
    - Face
    - Keystroke
    - Gesture
  - Problems
    - Noisy data
    - Not easy to change once be stolen
    - Availability

# Authentication

- Multi-factor
  - Using more than one way to authenticate a subject
  - Providing more layers of protection
  - But not convenient for users
- How to design an authentication system?
  - =>Using the security life cycle

# Access control

- Access control: exerting control over who can interact with a resource
- Types of access control
  - Discretionary access control (DAC): a subject with a certain access permission is capable of passing that permission on to any other subject
  - Mandatory access control: the operating system constrains the ability of a subject to access an object
- Access control presentation
  - Access control matrix
    - Objects: columns
    - Subjects: rows
    - Access permission: respected cells

# Access control

| | File 1 | File 2 | Process 1 | Process 2 |
|---|---|---|---|---|
| Process 1 | Read, own | Write | Own | |
| Process 2 | Append | Own, write | Execute | Own |

- Access control list:
  - There is a list of subjects and their permissions on a particular object
  - Example: acl(file 1) = { (Process 1, { read, own }), (Process 2, { append }) }
- Capabilities list:
  - There is a list of objects and what can be done on them for a particular subject
  - Example: cap(Process 1) = { (File 1, { read, own }), (file 2, { write
  - }), (process 1, {own}), }

# Access control

- Bell-LaPadula model
  - Subjects have security clearance: TS (top secret), S (secret), C (confidential), UC (unclassified) ($l_s$)
  - Object have security classification: the same as above ($l_o$)
  - Simple security condition: subject can read object if and only if $l_o <= l_s$
  - Star property: subject can write to object if and only if $l_s <= l_o$

# End of chapter 10