Chapter 1 Introduction


1.0 Introduction

- Information security - importance in daily life
  - Bank ATM password: personal identification
    - In the digital world, a person’s identification becomes a group of numbers.
    - What are some other personal identification examples?
  - Ministry of the Interior’s natural person (public key) certificate
  - Webpage security transmission mechanism: SSL
    - Internet banking
    - Internet shopping
  - Trend company’s GateLock
  - Anti-virus software
1.0 Introduction

Background

- Information Security requirements have *changed* in recent times.
- Traditionally provided by *physical and administrative mechanisms*.
- Computer use requires automated tools to protect files and other stored information.
- Use of networks and communications links requires measures to protect data during transmission.
1.0 Introduction

- Definitions
  - **Computer Security** - generic name for the collection of tools designed to protect data and to thwart (攔阻) hackers.
  - **Network Security** - measures to protect data during their transmission.
  - **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks.

1.1 Services, Mechanisms, and Attacks

- A systematic way is needed to define requirements
- Consider three aspects of information security:
  - **Security attack**:
  - **Security mechanism**: A mechanism that is designed to detect, prevent, or recover from a security attack.
  - **Security service**:
  - Consider in reverse order
Security Service

- is something that enhances the security of the data processing systems and the information transfers of an organization.
- intended to counter security attacks.
- make use of one or more security mechanisms to provide the service.
- Replicate (複製的) functions normally associated with physical documents
  - eg have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed.

Table 1.1 A Partial List of Common Information Integrity Functions [SIMM92]

<table>
<thead>
<tr>
<th>Identification</th>
<th>Endorsement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>Access (egress)</td>
</tr>
<tr>
<td>License and/or certification</td>
<td>Validation</td>
</tr>
<tr>
<td>Signature</td>
<td>Time of occurrence</td>
</tr>
<tr>
<td>Witnessing (notarization)</td>
<td>Authenticity—software and/or files</td>
</tr>
<tr>
<td>Concurrence</td>
<td>Vote</td>
</tr>
<tr>
<td>Liability</td>
<td>Ownership</td>
</tr>
<tr>
<td>Receipts</td>
<td>Registration</td>
</tr>
<tr>
<td>Certification of origination and/or receipt</td>
<td>Approval/disapproval</td>
</tr>
<tr>
<td></td>
<td>Privacy (secrecy)</td>
</tr>
</tbody>
</table>
1.1 Services. Mechanisms, and Attacks

- **Security Mechanism**
  - a mechanism that is designed to *detect, prevent, or recover* from a security attack
  - *no single mechanism that will support all functions required.*
  - however one particular element underlies many of the security mechanisms in use: **cryptographic techniques**
  - hence our focus on this area.

- **Security Attack**
  - any action that compromises the security of information owned by an organization
  - information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems.
  - have a wide range of attacks.
  - can focus of generic types of attacks.
  - note: often *threat & attack* mean same.
1.3 A Model for Network Security

Model for Network Security [Fig. 1.1]

Model for Network Access Security [Fig. 1.2]