Chapter 1 Introduction

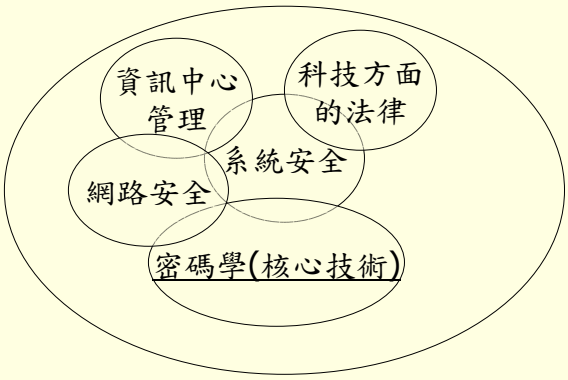
Cryptography and Network Security:
Principles and Practices (3rd Ed.)

1.0 Introduction

- 資訊安全的重要性--日常生活中的資訊安全
  - 銀行提款機的密碼：身分辨識
    - 數位世界中，人的代號變成一組數字。
    - 還有哪些身分辨識的例子?
  - 內政部的自然人(公開金匙)憑證
  - 網頁的安全傳輸機制：SSL
    - 網路銀行
    - 網路購物
  - 趨勢公司的GateLock
  - 防毒軟體

1.0 Introduction

- 資訊安全的範疇



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 (阻擾) 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 form a security attack.
  - **Security service**:
- Consider in reverse order

1.1 Services. Mechanisms, and Attacks

- 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.

1.1 Services. Mechanisms, and Attacks

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

•Identification	•Endorsement
•Authorization	•Access (egress)
•License and/or certification	•Validation
•Signature	•Time of occurrence
•Witnessing (notarization)	•Authenticity—software and/or files
•Concurrence	•Vote
•Liability	•Ownership
•Receipts	•Registration
•Certification of origination and/or receipt	•Approval/disapproval
	•Privacy (secrecy)

1.1 Services. Mechanisms, and Attacks

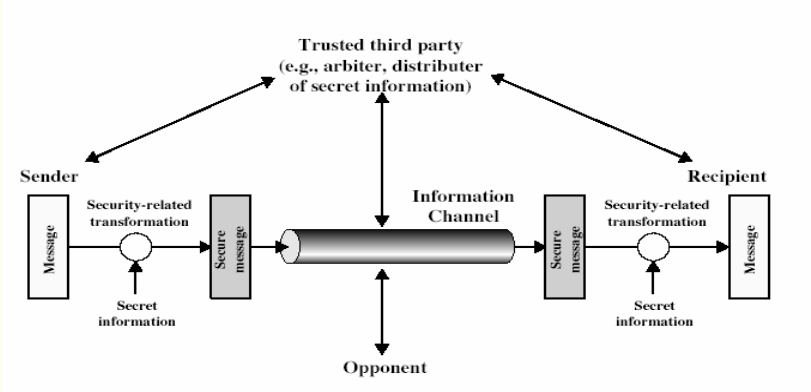
- Security Mechanism
  - a mechanism that is designed to *detect, prevent, or recover* from a security attack
  - *no single mechanism that will support all functions required*.
  - however one particular element underlies many of the security mechanisms in use: **cryptographic techniques**
  - hence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

1.1 Services. Mechanisms, and Attacks

- 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]



1.3 A Model for Network security

- Model for Network Access Security [Fig. 1.2]