

Cryptography and Network Security

Behrouz
Forouzan

網路安全 與密碼學概論

Cryptography and Network Security

Behrouz A. Forouzan◎原著

李南逸、王智弘、林峻立、張智超、溫翔安、葉禾田◎翻譯



美商麥格羅·希爾
資訊科學 系列叢書



Inc. Permission required for reproduction or display.

Chapter 1

Introduction

Objectives

- To define three security goals**
- To define security attacks that threaten security goals**
- To define security services and how they are related to the three security goals**
- To define security mechanisms to provide security services**
- To introduce two techniques, cryptography and steganography, to implement security mechanisms.**

1-1 SECURITY GOALS

This section defines three security goals.

Topics discussed in this section:

1.1.1 Confidentiality 機密性

1.1.2 Integrity 完整性

1.1.3 Availability 可使用性

1.1.extra 不可否認性 (Nonrepudiation) :

1.1 Security Goals- 不包含 數位簽章系統需求

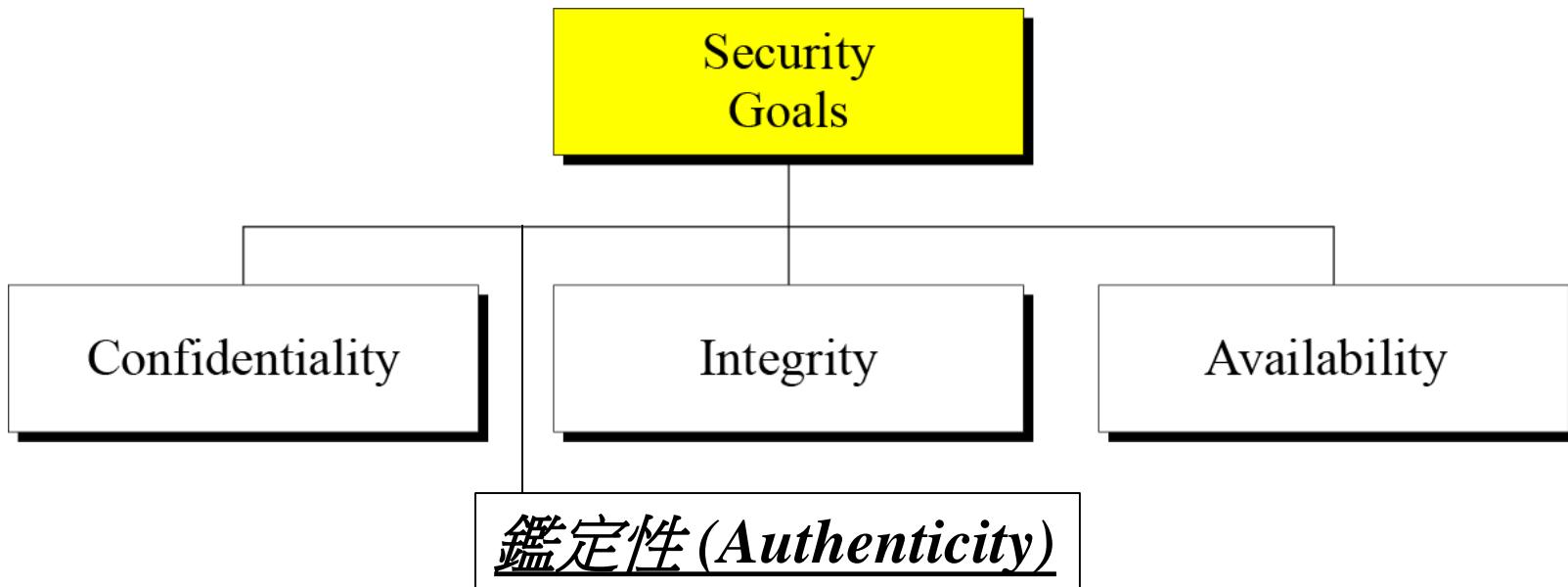


Figure 1.1 *Taxonomy of security goals*

1.1.1 Confidentiality

Confidentiality is probably the most common aspect of information security.

機密性：防制非法揭露或得到資料

*We need to protect our confidential information.
An organization needs to guard against those
malicious actions(惡意行動) that endanger the
confidentiality of its information.*

1.1.2 Integrity

完整性：防制非法更改資料

Integrity means that changes need to be done only by authorized entities(授權的人) and through authorized mechanisms.

Class Exercise: list some examples that might compromise integrity

1.1.3 Availability

The information created and stored by an organization needs to be available to authorized entities.

可用性：避免系統拒絕合法使用者存取資料

*Information must **be accessible** to authorized entities.*

1.1.4- 鑑定性 (Authenticity)

- 確定資訊來源的合法性，亦即此資訊確實是由發送方所傳送。而非別人偽造，或利用以前的訊息來重送。
- *Class Challenges*
 1. *Why we need authenticity*
 2. *List some examples of authentications we use daily*

1.1.5.extra 不可否認性 (Nonrepudiation)

1. 發送方在事後，不可否認其傳送過/做過之資訊

- ***Class Exercise: list some examples that might compromise nonrepudiation***

1-2 ATTACKS

The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.

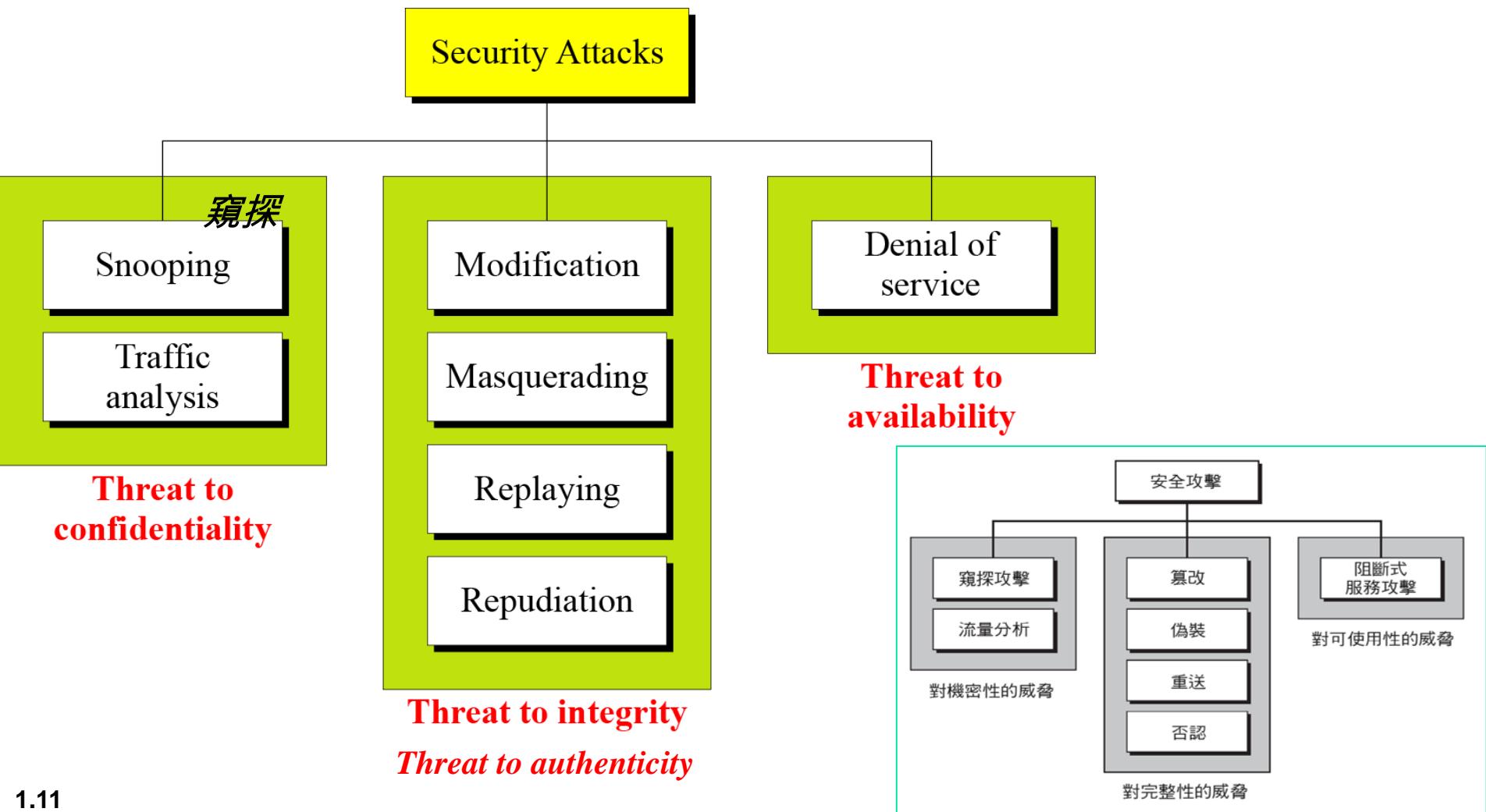
三個安全目標（機密性、完整性、可使用性）
會被安全攻擊所威脅。

Topics discussed in this section:

- 1.2.1 Attacks Threatening Confidentiality
- 1.2.2 Attacks Threatening Integrity
- 1.2.3 Attacks Threatening Availability
- 1.2.4 Passive versus Active Attacks

1.2 Continued

Figure 1.2 Taxonomy of attacks with relation to security goals



1.2.1 Attacks Threatening Confidentiality p.3

Snooping refers to unauthorized access to or interception of data.

Q: How to prevent snooping?

A:

Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

Q: What type of information an interceptor can monitor or collect online ?

A:

Q: What tools can be used to eavesdrop transmissions

1.2.2 Attacks Threatening Integrity

Modification means that the attacker intercepts the message and changes it.

Masquerading or spoofing happens when the attacker impersonates somebody else.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

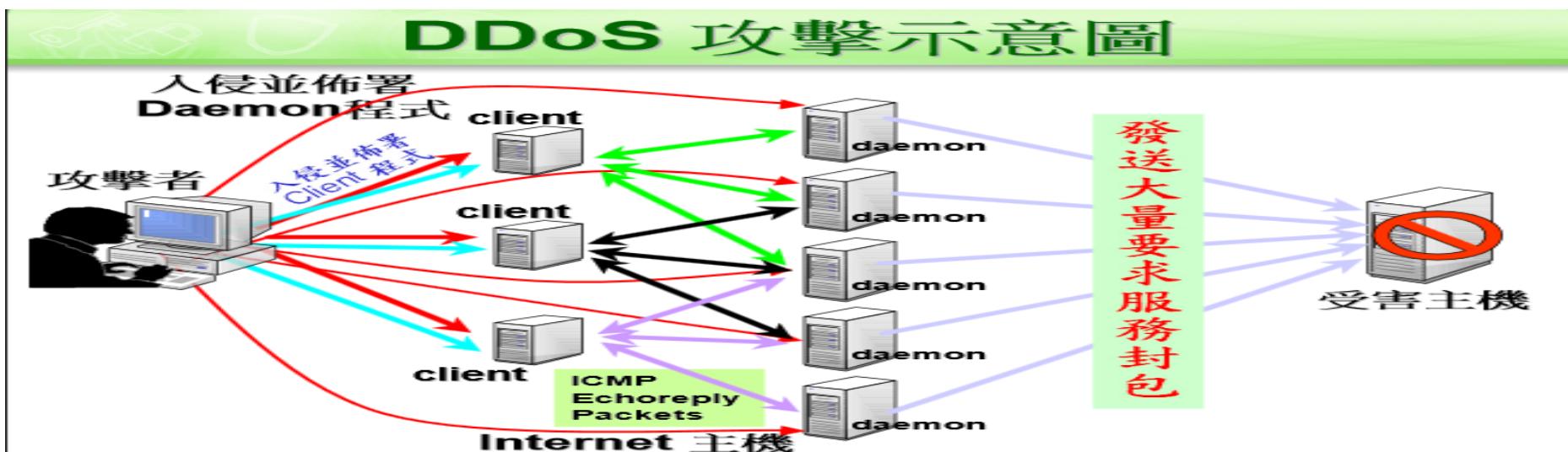
Q: Please give Examples for each attack.

1.2.3 Attacks Threatening Availability

Denial of service (DoS, 阻斷式服務) is a very common attack. It may slow down or totally interrupt the service of a system.

- *Ping of death:*
- *Ping flood*

ICMP (Internet Control Message Protocol) 是一種「錯誤偵測與回報機制」，主要目的在於偵測遠方主機是否存在。



Class Challenge

- 1) ***What is ICMP***
- 2) ***Which layer is ICMP in***
- 3) ***Why ping can cause death of victim***
- 4) ***Ping of death:***



- 5) ***Ping flood:***



- 6) ***Use wireshark to analyze IP/TCP/SSL/HTTPS***

1.2.4 Passive Versus Active Attacks

Table 1.1 Categorization of *passive* and *active* attacks

Attacks	Passive/Active	Threatening
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity authenticity
Denial of service	Active	Availability

Passive attacks:

- the attacker's goal is **just to obtain information.**
- The system is not affected(危害), and continues with its normal operation.
- **Hard to detect** passive attacks.
- Can be prevented by **encipherment** of the data.

Active attacks:

- the attacker will **change the data** and **harm the system.**
- Threaten **authenticity**, integrity and availability

Notice: the differences between snooping vs spoofing

1-3 SERVICES AND MECHANISMS

Topics discussed in this section:

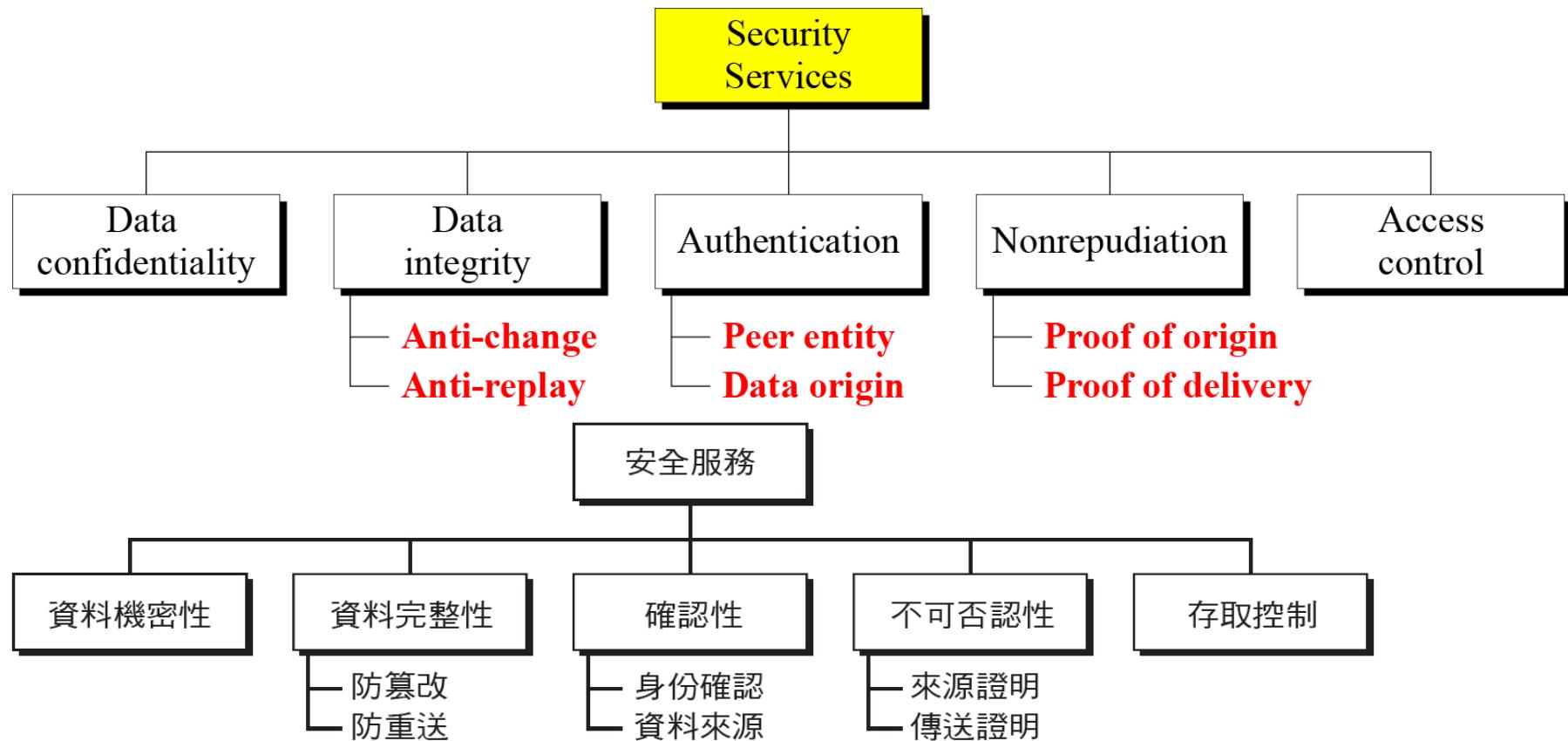
1.3.1 Security Services

1.3.2 Security Mechanism

1.3.3 Relation between Services and Mechanisms

1.3.1 Security Services

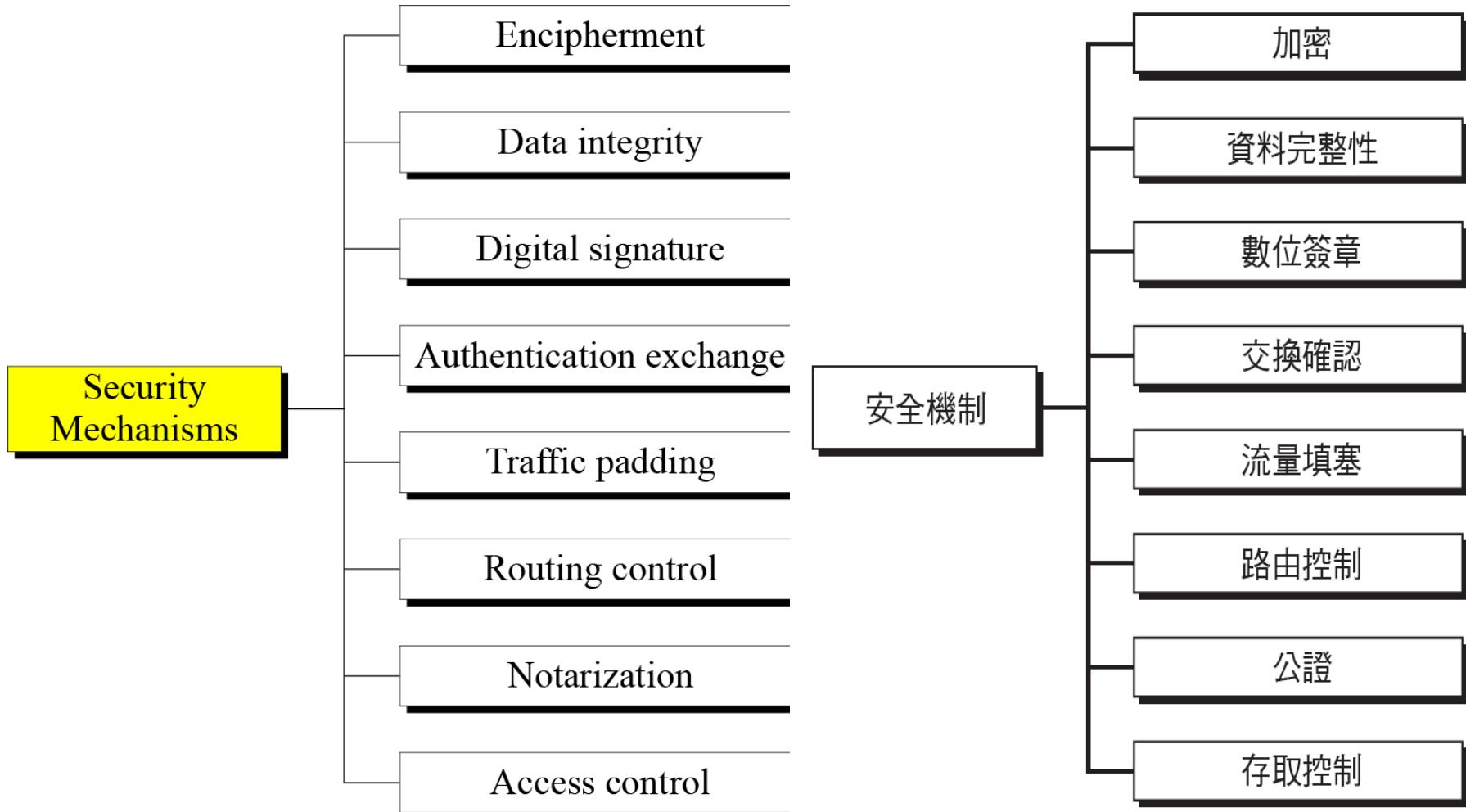
Figure 1.3 Security services



Class challenge: 1)finding the missing key info of the above chart
2) Unix `rwxrwxrwx` in file system corresponds to which of the above services

1.3.2 Security Mechanism

Figure 1.4 Security mechanisms



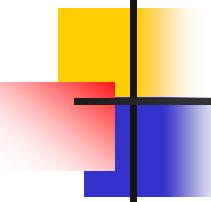
Class challenge: what mechanisms can achieve integrity

1-4 TECHNIQUES

Topics discussed in this section:

1.4.1 Cryptography – 密碼術

1.4.2 Steganography - 隱碼術



1.4.1 Cryptography

Cryptography, a word with Greek origins, means “secret writing.” However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

1.4.2 Steganography

The word steganography, with origin in Greek, means “covered writing,” in contrast with cryptography, which means “secret writing.”

Example: covering data with text

This book is mostly about cryptography, not steganography.

0

1

0

0

0

0

1

Class challenge: what is this?

1.4.2 *Continued*

Example: covering data under color image

0101001 <u>1</u>	1011110 <u>0</u>	0101010 <u>1</u>
0101111 <u>0</u>	1011110 <u>0</u>	0110010 <u>1</u>
0111111 <u>0</u>	0100101 <u>0</u>	0001010 <u>1</u>

Class challenge:

- 1) *What is this?*
- 2) *Why hide here? Adv. Vs. Disadv*

1-5 THE REST OF THE BOOK

The rest of this book is divided into four parts.

Part One: Symmetric-Key Enciphermen

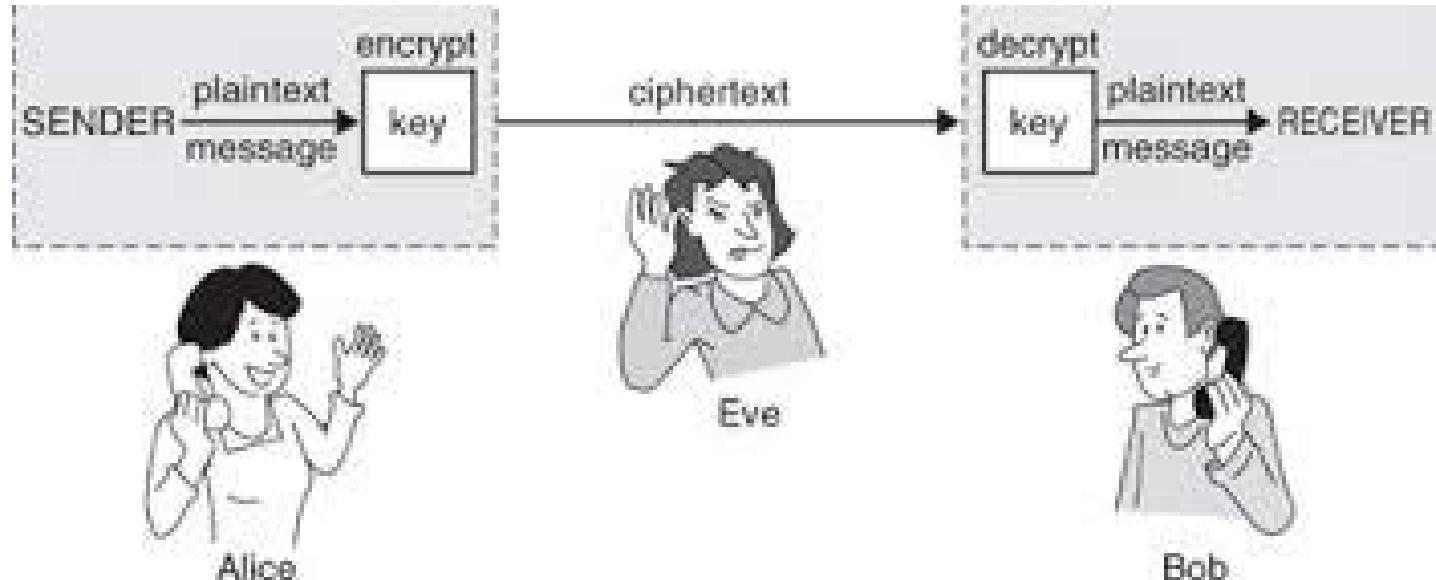
Part Two: Asymmetric-Key Encipherment

Part Three: Integrity, Authentication, and Key Management

Part Four: Network Security – Web-SSL

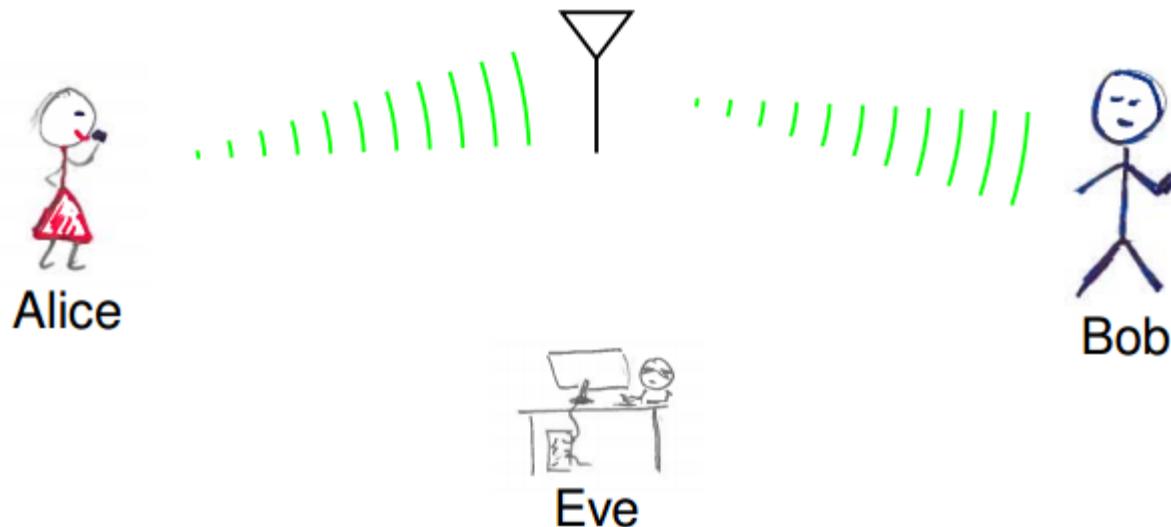
角色登場

- 密碼學家喜歡在其密碼劇本中談論一組熟悉的角色。
- Alice 和 Bob 領頭的人物表。Eve (偷聽者)



How can Alice and Bob protect their secret?

- *Alice shares a secret with Bob*
- *Eve spies on them*



密碼學簡介

1. 密碼學(*Cryptology*)一詞乃為希臘字根''隱藏'' (*Kryptós*) 及 ''訊息'' (*lógos*) 組合而成，現泛指所有有關研究秘密通訊之學問(包括如何達到秘密通訊及破解秘密)。
2. 國際密碼研究學會(*International Association for Cryptologic Research*) 簡稱 **IACR** 。

*IACR*於1981年成立

現每年五月於歐洲舉辦一次學術研討會，稱為EUROCRYPT。

每年八月於美國舉辦學術研討會，稱為CRYPTO

每年於亞洲舉辦ASIACRYPT。

$\text{Cryptology} := \text{Cryptography} \oplus \text{Cryptanalysis}$



3. *Cryptology* 可分為兩個領域：

(1) 密碼學 (*Cryptography*)

Encryption Decryption
(Public-Key) (Private-Key)

(2) 破密學 (*Cryptanalysis*)

Signature Generation Signature Verification
(Private-Key) (Public-Key)

密碼學術語 Basic Terminology

- Plaintext
 - The original message
- Ciphertext
 - The coded message
- Enciphering or encryption
 - Process of converting from plaintext to ciphertext
- Deciphering or decryption
 - Restoring the plaintext from the ciphertext
- Cryptography
 - Study of encryption
- Cryptographic system or cipher
 - Schemes used for encryption
- Cryptanalysis
 - Techniques used for deciphering a message without any knowledge of the enciphering details
- Cryptology
 - Areas of **cryptography** and **cryptanalysis** together

密碼破解法(cryptanalysis)

- 當演算法受到攻擊時，分析師會找尋將原文轉成密文的“演算法缺點”，且在沒有金鑰的情況下還原資訊的原文。若是具有這類弱點的演算法，也就不能稱為牢靠的演算法，當然也就不能使用。
- 例如2005~2006年山東大學數學與系統科學學院教授、資訊安全實驗室主任—王小雲領導的研究團隊成功地破解國際上廣泛應用的兩大密碼演算法MD5和SHA-1。
- 王小雲及她的團隊在2005年將該成果發表為4篇論文，被公認為近年來國際密碼學最出色的成果之一。

- *I refuse to accept the idea that the 'isness' of man's present condition makes him morally incapable of reaching up for the eternal 'oughtness' that forever confronts him.“*
/* from Obama */
- *The absence of hope can rot a society from within.*
/* from Dr. Martin Luther King jr. */
- *For we are fallible (/'fæləbl/, 會犯錯誤的). We make mistakes, and fall victim to the temptations of pride, and power, and sometimes evil. Even those of us with the best of intentions will at times fail to right the wrongs before us.*
/* from Obama */

Education vs. Passion

TEDTalks 》 Sir Ken Robinson 推動學習革命 (中英字幕)

<http://www.youtube.com/watch?v=1ZbF6wryyh0&feature=related>

Ken Robinson - The Element

<http://www.youtube.com/watch?v=3TAqSBMZDY8&feature=related>

林書豪, 李安

ICRT 普林斯頓 超強記憶

吉蘭·貝兒·瑟吉教導孩子如何發揮影響力中英文

http://www.ted.com/talks/kiran_bir_sethi_teaches_kids_to_take_charge.html

【TEDx】羅根·拉普蘭特：用駭客思維學習 Logan LaPlante: Hackschooling Makes Me Happy *<http://www.youtube.com/watch?v=UJKitCtkti0>*