Cryptography and Network Security -W. Stalling (2nd Ed.)

Hoon-Jae Lee
CNSL
Cryptography and Network Security Lab.
hjlee@dongseo.ac.kr
http://cg.dongseo.ac.kr/~hjlee

Chap 1. Introduction

- 1.1 Attacks, Services, and Mechanisms
- 1.2 Security Attacks
- 1.3 Security Services
- 1.4 A Model for Network Security
- 1.5 Outline of this Book
- 1.6 Recommended Reading

1.1 Attacks, Services, and Mechanisms

- Three aspects of information security:
  - *Security attack*: compromises the security of information owned by an organization
  - *Security Mechanism*: is designed to detect, prevent, or recover from a security attack
  - *Security service*: enhances the security of the data processing systems and the information transfers of an organization

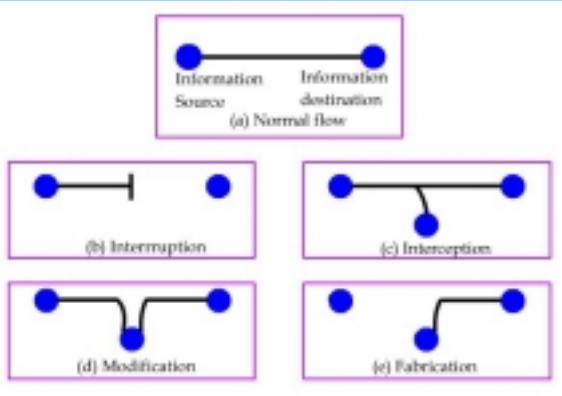
1.1 Attacks, Services, and Mechanisms

- Services:
  - *Confidentiality*: ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.
  - *Authentication*: ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false
  - *Integrity*: ensures that only authorized parties are able to modify computer system assets and transmitted information
  - *Non -repudiation*: requires that neither the sender not the receiver of a message be able to deny the transmission
  - *Access control*: requires that access to information resources may be controlled by or for the target system
  - *Availability*: requires that computer system assets be available to authorized parties when needed

1.2 Security Attacks (1)

❑1. Threats to security

- ✓Interruption
- ✓Interception
- ✓Modification
- ✓Fabrication



1.2 Security Attacks (2)

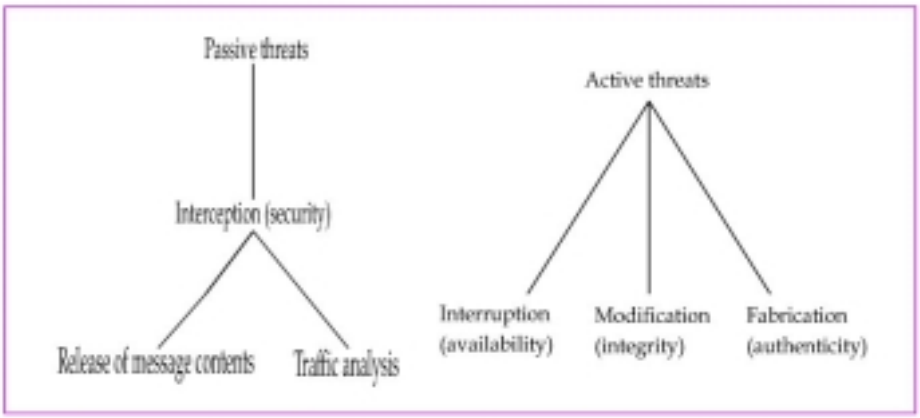


Fig. Active and Passive Network Security Threats

1.2 Security Attacks (3)

❑2. Methods of Attacks

✓***Ciphertext Only Attack:*** Attacker has only the intercepted cryptogram.

✓***Known Plaintext Attack:*** Attacker knows plaintext equivalence of some ciphertext.

✓***Chosen Plaintext Attack:*** Attacker can obtain ciphertext equivalent to some plaintext selected by attacker.

1.3 Security Service (1)

❑1. Data Confidentiality

for the protection of data from unauthorized disclosure as described below

- Connection confidentiality

  for the confidentiality of all (N)-user-data on an (N)-connection

- Connectionless confidentiality

  for the confidentiality of all (N)-user-data in a single connectionless (N)-SDU

1.3 Security Service (2)

- 1. Data Confidentiality (cont'd)
  - Selective field confidentiality

    for the confidentiality of selected fields within the (n)-user-data on an (n)-connection or in a single connectionless (N)-SDU
  - Traffic flow confidentiality

    for the protection of the information which might be derived from observation of traffic flows

1.3 Security Service (3)

- 2. Authentication
  - Peer entity authentication
    - ✓This service, when provided by the (N)-layer, provides corroboration to the (N+1)-entity that the peer entity is the claimed (N+1)-entity.
  - Data origin authentication
    - ✓This service, when provided by the (N)-layer, provides corroboration to an (N+1)-entity that the source of the data is the claimed peer (N+1)-entity.

1.3 Security Service (4)

- 3. Data integrity

  These services counter active threats and may take one of the forms described below.

  - Connection integrity with recovery

    for the integrity of all (n)-user-data on an (n)-connection and detects any modification, insertion, deletion or replay of any data within an entire SDU sequence (with recovery attempted)

  - Connection integrity without recovery

    same as "connection integrity with recovery" but with no recovery attempted

1.3 Security Service (5)

- Selective field connection integrity

  for the integrity of selected fields within the (n)-user data of an (N)-SDU transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted or replayed

- Connectionless integrity

  provides integrity assurance to the requesting (n+1)-entity

- Selective field connectionless integrity

  provides for the integrity of a single connectionless SDU and may take the form of determination of whether a received SDU has been modified

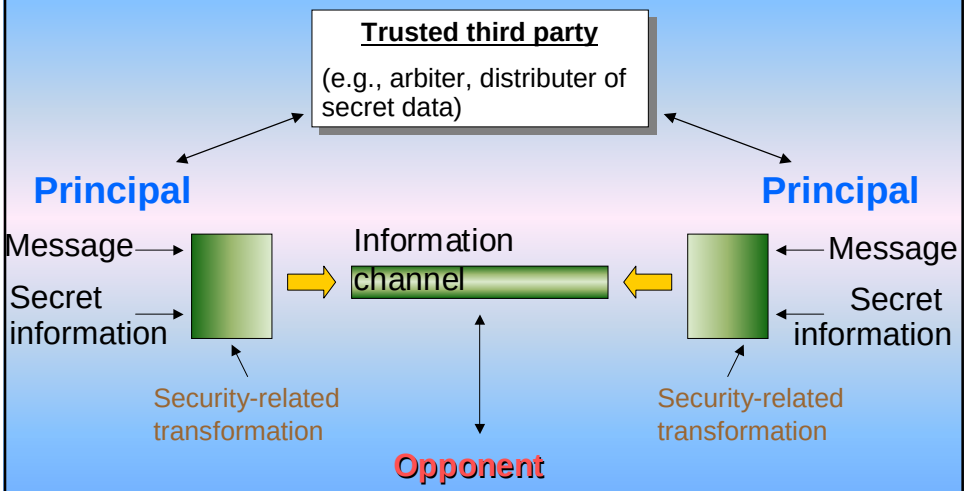
1.3 Security Service (6)

- 5. Non-repudiation
  - Non-repudiation with proof of origin :
    The recipient of data provide with proof of the origin of data.
  - Non-repudiation with proof of delivery :
    The sender of data is provided with proof of delivery of data.

1.3 Security Service (7)

- 6. Access Control
  - *provides protection against unauthorized use of resources*
- 7. Availability
  - requires that computer system assets be available to authorized parties when needed

1.4 A Model for Network Security



Security Mechanism (1)

- 1. Encipherment
  can provide confidentiality of either data or traffic flow information and can play a part in or element a number of other security mechanisms
- 2. Digital signature mechanisms
  A) signing a data unit; and
  B) verifying a signed data unit
- 3. Access control mechanisms
  determine and enforce the access rights of the entity

Security Mechanism (2)

- 4. Data integrity mechanisms
  - A) The integrity of a single data unit or field.
  - B) The integrity of a stream of data units or fields.
- 5. Authentication exchange mechanism
  - A) use of authentication information, such as passwords
  - B) cryptographic techniques
  - C) use of characteristics and/or possessions of the entity
- 6. Traffic padding mechanism
  - *to provide various levels of protection against traffic analysis*

Security Mechanisms (3)

- 7. Routing control mechanism
  - Routes can be chosen either dynamically or by prearrangement so as to use only physically secure sub-networks, relays or links.
- 8. Notarization mechanism
  - The assurance is provided by a third party notary, which is trusted by the communicating entities, and which holds the necessary information to provide the required assurance in a testifiable manner.

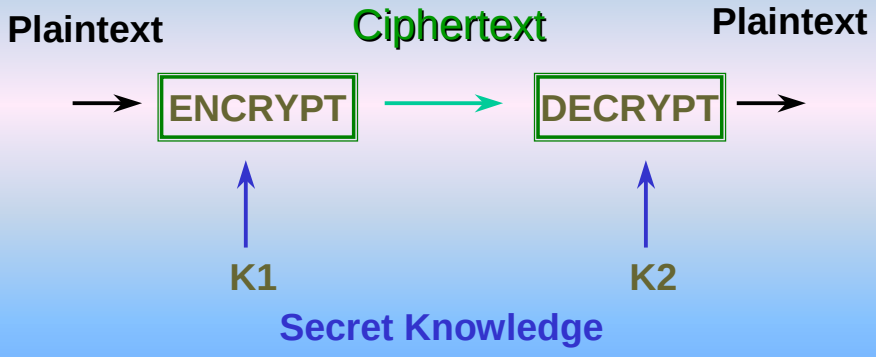
Security Mechanism (4)

Service \ Mechanism	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer Entity Authentication	Y	Y	.	.	Y	.	.	.
Data Origin Authentication	Y	Y	.	.	.	.	.	.
Access Control Service	.	.	Y	.	.	.	.	.
Connection Confidentiality	Y	.	.	.	.	.	Y	.
Connectionless Confidentiality	Y	.	.	.	.	.	Y	.
Selective Field Confidentiality	Y	.	.	.	.	.	.	.
Traffic Flow Confidentiality	Y	.	.	.	.	Y	Y	.
Connection Integrity with Recovery	Y	.	.	Y	.	.	.	.
Connection Integrity without Recovery	Y	.	.	Y	.	.	.	.
Selective Field Connection Integrity	Y	.	.	Y	.	.	.	.
Connectionless Integrity	Y	Y	.	Y	.	.	.	.
Selective Field Connectionless Integrity	Y	Y	.	Y	.	.	.	.
Non-reputation. Origin	.	Y	.	Y	.	.	.	Y
Non-reputation. Derivery	.	Y	.	Y	.	.	.	Y

- The mechanism is considered no to be appropriate

Y Yes:the mechanism is considered to be appropriate, either on its own or in combination with other mechanisms.

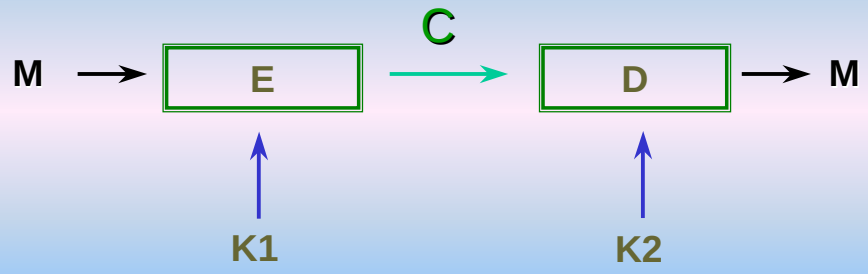
Security ALGORITHMS (Ex.1)



Security ALGORITHMS (Ex.2)

Key	Typical Examples	
Symmetric Key K1=K2	DES (1975)	Block length: 64, Key length : 56 bits Block Cipher
	IDEA (1987)	Block length: 64, Key length : 64 bits Block Cipher
Asymmetric Key K1≠K2	El-Gamal (1985)	Public Key Cipher Block and Key length variable
	RSA (1985)	

Cryptographic System (1)



Cryptographic System (2)

E = Encryption Function
D = Decryption Function
M = Message
C = Ciphertext
K1 = Encryption Key
K2 = Decryption Key

Encryption C = E(M,K1)
Decryption M = D(C,K2)