

# Lecture 4: Security Mechanism Overview

Yuan Xue

## I. SECURITY THREAT IN NETWORKS

As we have seen in the last two lectures, a network, especially one that grows to global scale, has many vulnerabilities. Threats are raised to against the key aspects of security: confidentiality, integrity, and availability.

- *Attacks against confidentiality*
  - eavesdropping
  - traffic flow analysis
- *Attacks against integrity*
  - IP spoof
  - Sequence number attack
  - Man-in-the-middle attack
- *Attacks against availability*
  - Denial of Service attack
  - Traffic redirection
- *Precursor to attack*
  - Port scan

## II. SECURITY SERVICES AND MECHANISMS

To protect the network from various security threats, we study the security mechanisms and security services in this section. First, let us examine some related terms.

### A. Terms

- *Vulnerability*: an aspect of the system that permits attackers to mount a successful attack, sometimes also called a “security hole”.
- *Weakness* a potential vulnerability, whose risk is not clear. Sometimes several weaknesses might combine to yield a full-fledged vulnerability.
- *Threat*: a circumstance or scenario with the potential to exploit a vulnerability, and cause harm to a system.
- *Attack*: A deliberate attempt to breach system security. Note that not all attacks are successful. An attack usually refers to a specific stratagem. A threat refers to a broader class of ways that things could go wrong. Attacks are usually classified into two types: (1) *Passive attack* refers to attack that does not result in a change to the system, and attempts to break the system solely based upon observed data. (2) *Active attack*, on the other hand, involves modifying, replaying, inserting, deleting, or blocking data.
- *Security Mechanism*: a mechanism that is designed to detect, prevent, or recover from a security attack.

- *Security Service* makes use of security mechanisms to counter security attacks.

ITU – T<sup>2</sup> Recommendation X.800, *Security Architecture for OSI* defines a systematic approach for security services and security mechanisms. In particular, X.800 divides the security services into five categories.

- *Authentication*: the assurance that the communicating entity is the one that it claims to be. In particular,
  - *Peer Entity Authentication* is used in connection-oriented communication to provide assurance on the identity of the entities connected.
  - *Data Origin Authentication* is used in connectionless communication to provide assurance on the identity of the source of the received data block.
- *Access Control*: the prevention of unauthorized use of a resource.
- *Data confidentiality*: the protection of data from unauthorized disclosure. It has four specific services:
  - *Connection Confidentiality*: the protection of all user data on a connection.
  - *Connectionless Confidentiality*: the protection of all user data in a single data block.
  - *Selective-Field Confidentiality*: the protection of selected fields within user data on a connection or in a single data block.
  - *Traffic-flow Confidentiality*: the protection of the traffic flow pattern.
- *Data integrity*: the assurance that data received are the same as send by an authorized entity. It has five specific services:
  - *Connection Integrity with Recovery*: provides detection and recovery from any integrity violation (modification, insertion, deletion, relay) against any user data within an entire data sequence in connection-oriented communication.
  - *Connection Integrity without Recovery*: provides only detection of integrity violation in connection-oriented communication.
  - *Selective-Field Connection Integrity*: provides for the integrity of selected fields within the user data of a data block transferred over a connection, and determines whether the selected fields have been modified, inserted, deleted, or replayed.
  - *Connectionless Integrity*: provides for the integrity of a single data block, and detects data modification. A limited form of replay detection may be also provided.
  - *Selective-Field Connectionless Integrity*: provides for the integrity of selected fields within a single data block, and determines whether the selected field is modified.
- *Nonrepudiation*: provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. In particular,
  - *Nonrepudiation of origin* provides proof that the message was sent by the specified party.
  - *Nonrepudiation of destination* provides proof that the message was received by the received party.

Security mechanisms are used to implement the above security services. Each specific security mechanism and its corresponding security service is given in Table. I.

Security Service	Supporting Security Mechanisms
Peer entity authentication	encipherment, digital signature, authentication exchange
Data origin authentication	encipherment, digital signature
Access control	access control
Confidentiality	encipherment, routing control
Traffic flow confidentiality	encipherment, traffic padding, routing control
Data integrity	encipherment, digital signature, data integrity
Nonrepudiation	digital signature, data integrity, notarization
Availability	access control, authentication exchange

TABLE I  
RELATIONSHIP BETWEEN SECURITY SERVICES AND MECHANISMS