Overview

Yih-Kuen Tsay

Department of Information Management
National Taiwan University

Background

Requirements of **Information Security** have changed over the last few decades:

- Introduction of the computer for data processing
  - Physical and administration means alone no longer sufficient
  - Automated tools needed for protecting files stored on the *shared* computer
  - Hence **Computer Security**
- Introduction of distributed systems and use of networks and communication devices
  - Data need to be protected during their transmission
  - Hence **Network Security**
- No clear boundaries between the two forms of security

Security Violations

Network security (on which we will spend more time) can be violated in many different ways:

- Files with sensitive information disclosed during transmission
- Remote updates to an authorization file intercepted and
  - altered or
  - delayed
- Fabricated updates to an authorization file
- Trading transactions subsequently denied by either party

Key Objectives in Security

- **Confidentiality**
  - Data Confidentiality: sensitive information not disclosed to unauthorized entities
  - Privacy
- **Integrity**
  - Data Integrity: data/programs changed in a specified and authorized manner
  - System Integrity: operation in the intended way
- **Availability**
- The above is often referred to as the **CIA triad**.
- Additional objectives
  - Authenticity: verifiable genuineness
  - Accountability: actions of an entity traceable

Impacts of Security Breaches

- **Low**: limited adverse effect
  - effectiveness of primary organizational functions noticeably reduced
  - minor damage to organizational assets or financial loss
  - minor harm to individuals
- **Moderate**: significant adverse effect
  - effectiveness of primary organizational functions significantly reduced
  - significant damage to organizational assets or financial loss
  - significant harm to individuals (but no loss of life or life-threatening injuries)
- **High**: severe or catastrophic adverse effect
  - one or more of primary organizational functions disabled
  - major damage to organizational assets or financial loss
  - severe harm to individuals (involving loss of life or life-threatening injuries)

Why Is Network Security Complex?

- Subtle mechanisms needed for seemingly straightforward requirements:
  - many potential countermeasures (i.e., possible weaknesses in the mechanism) to consider
  - some measures elaborate and counterintuitive
- Deployment of security mechanisms
  - physical: which points in a network
  - logical: which layers in the protocol
- Creation and distribution of secret information (needed by the implementation of a mechanism)
- Unpredictable behavior of underlying communications protocols
- *All* weaknesses must be found and eliminated
- Etc.

Main Concepts in Security (The OSI View)

- **Security attack**:
  any action compromising the security of information owned by an organization or individual
- **Security mechanism**:
  a mechanism designed to detect, prevent or recover from security attacks
- **Security service**:
  a service built upon one or more security mechanisms that enhances the security of information

Threats and Attacks

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

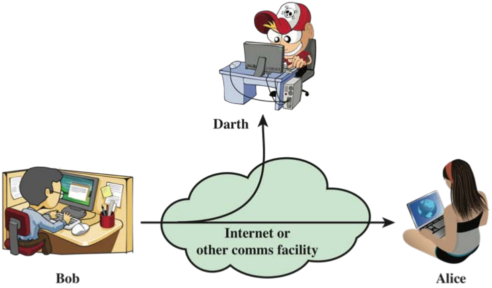
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Source: Table 1.1, Stallings 2014

Security Attacks

- Passive attacks:
  - attempts to learn information from the system
  - does not affect system resources
- Active attacks:
  - attempts to alter system resources or
  - affect their operation

Passive Attacks



Source: Figure 1.1, Stallings 2014

- Eavesdropping on or monitoring of transmissions.
  - release of message contents
  - traffic analysis
- Difficult to detect, but may be prevented (from success).

Traffic Analysis

IM NTU

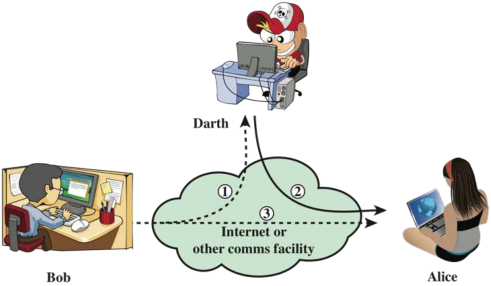
Types of information that can be derived from a traffic analysis attack:

- Identities of partners
- How frequently the partners are communicating
- Message pattern, message length, or quantity of messages
- Events correlated with conversations between particular partners
- Messages of a *covert channel*

Active Attacks

- **Masquerade**: one entity pretending to be another
- **Replay**: retransmission of a captured data unit
- **Modification of Message**: some portion of a message is altered, delayed, or reordered
- **Denial of Service**: preventing the normal use or management of communications facilities
- Difficult to prevent absolutely, but may be detected and recovered.

Active Attacks (cont.)



Source: Figure 1.1, Stallings 2014

- Masquerade: 2
- Replay: 1 + 2 + 3
- Modification of Message: 1 + 2
- Denial of Service: 3

Security Services (or Requirements)

- **Authentication**: assuring that a communication is authentic
  - Data origin authentication
  - Peer entity authentication
- **Access Control**: ability to limit and control access controlled
- **Data Confidentiality** (Secrecy): protection of transmitted data or even traffic flow (from passive attacks)
- **Data Integrity**: protection of transmitted data (from active attacks); with or without recovery
- **Nonrepudiation**: transmission undeniable by either party
- **Availability Service**: accessible and usable upon demand by authorized entities

Problems with Electronic Documents

Performing the functions associated with paper documents on electronic documents is challenging, due to the following aspects of electronic documents:

- No difference between the original and its copies
- Altering bits leaves no physical trace
- Any proof of authenticity must be based on internal evidence

Security Services – X.800

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

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 confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block 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 for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been 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.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Source: Table 1.2, Stallings 2014

Security Mechanisms

- To provide a particular security service, one utilizes a security mechanism or combine several of them
- **Encipherment** represents one prominent class of security mechanisms.
  - reversible encipherment: encryption algorithm
  - irreversible encipherment: hash function, message authentication code

Security Mechanisms – X.800

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys. **Digital Signature** Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient). **Access Control** A variety of mechanisms that enforce access rights to resources. **Data Integrity** A variety of mechanisms used to assure the integrity of a data unit or stream of data units. **Authentication Exchange** A mechanism intended to ensure the identity of an entity by means of information exchange. **Traffic Padding** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts. **Routing Control** Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected. **Notarization** The use of a trusted third party to assure certain properties of a data exchange.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy). **Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. **Event Detection** Detection of security-relevant events. **Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities. **Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Source: Table 1.3, Stallings 2014

Security Services vs. Mechanisms

	Mechanism							
Service	**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			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Source: Table 1.4, Stallings 2010

Network Security Model

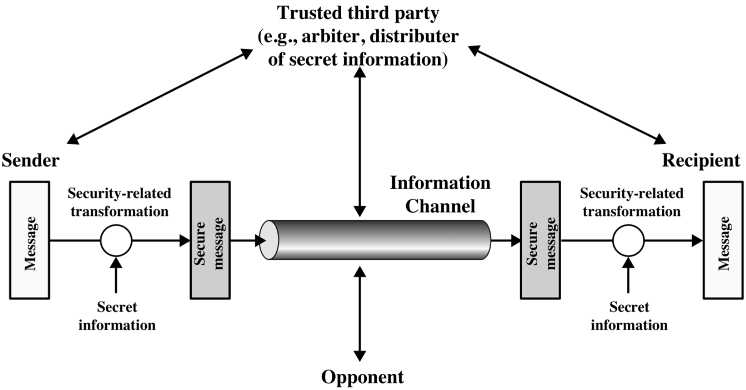


Figure 1.2 Model for Network Security

Source: Figure 1.2, Stallings 2014

Designing a Security Service

- Design an algorithm for performing the security-related transformation
- Generate the secret information to be used with the algorithm
- Develop methods for distributing and sharing the secret information
- Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service

Network Access Security Model

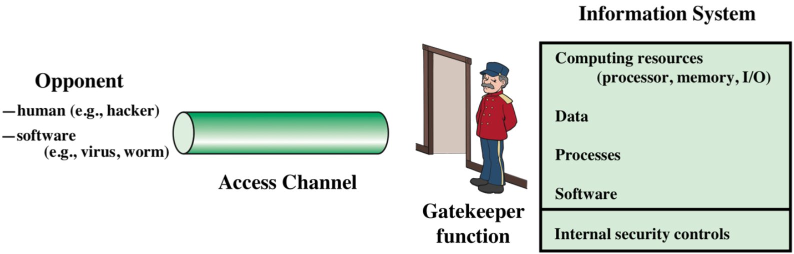


Figure 1.3 Network Access Security Model

Source: Figure 1.3, Stallings 2014