CN02 Network Security

Professor Anh T. PHAM
Computer Communications Lab.

Contents

Lecture 1: Introduction to Network Security

- Information Security

  Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means.

- Computer Security

  the need for automated tools for protecting files and other information stored on the computer

- Network Security

  protect data during their transmission.

- Internet Security

1. What's Network Security (1)

1.1 Confidentiality

Data confidentiality: Assures that private or confidential information is not **made available** or **disclosed** to **unauthorized individuals**

Privacy: Assures that individual's control or influence

- what information related to them **may be collected** and/or **stored**,
- and **by whom and to whom** that information may be disclosed

❖ What is the "Loss of Confidentiality"?

Unauthorized collected and/or of information

Unauthorized disclosure of information

❖ Example?

Example

❖ Undisclosed grade information to individual other than the owner

❖ Secretly, without prior notice, collect personal information by social networks

❖ Unauthorized collect and sell personal information to advertisement companies

❖ Collect and sell personal medical data

1. What's Network Security (2)

1.2 Integrity

Data integrity: Assures that information and programs **are changed** only in a **specified and authorized manner**

System integrity: Assures that a system performs its intended function in an **unimpaired manner**, free from deliberate or inadvertent unauthorized manipulation of the system

❖ What is the "Loss of Integrity"?

Unauthorized modification or destruction of information

Unauthorized modify the system

Example

❖ Modify individual medical data: inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability

❖ The system is modified to work not as good as it was designed

❖ The system is modified to collect and send data to unauthorized parties

1. What's Network Security (3)

1.3 Availability

Assures that systems work promptly, and service is **not denied to authorized users**

❖ What is "Loss of availability"?

Disruption of access to the information

Disruption of access to the system itself

❖ Example

Slow connection to a website

Service denial to authentic users

1. What's Network Security (4)

1.4 Authenticity

Verifying that users are who they say they are and that each input arriving at the system came from a **trusted source**

1.5 Accountability

The security goal that generates the requirement for actions of an entity to be **traced uniquely to that entity**

This support

- Nonrepudiation: cannot be denied
- Fault isolation
- Intrusion detection & prevention

All systems and users must keep records of their activities

Network Security: 5 Requirements

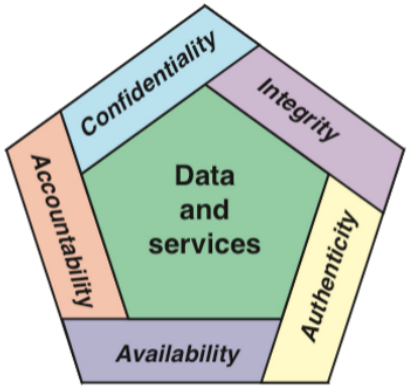


Figure 1.1 Essential Network and Computer Security Requirements

2. Breach of Security Levels: Low

❖ **Low:** The loss could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals

❖ **Examples:** limited adverse effect caused by confidentiality/integrity or availability may include

Prolong the work/operation a bit, but still functioning, effectiveness of the functions **is noticeably reduced**

Some minor asset damage

Minor financial loss

Minor harm to individual

Breach of Security Levels: Moderate

- **Moderate:** The loss could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals

- **Example:** serious adverse effect, the the loss might
  - a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but **the effectiveness of the functions is significantly reduced**
  - result in significant damage to organizational assets
  - result in significant financial loss
  - result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries

Breach of Security Levels: High

- **High:** The loss could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals

- Example: the loss might
  - cause a severe degradation in or loss of mission capability to an extent and duration that the organization **is not able to perform one or more of its primary functions**;
  - result in major damage to organizational assets;
  - result in major financial loss; or
  - result in severe or catastrophic harm to individuals involving loss of life or serious, life-threatening injuries

3. Security Terminology

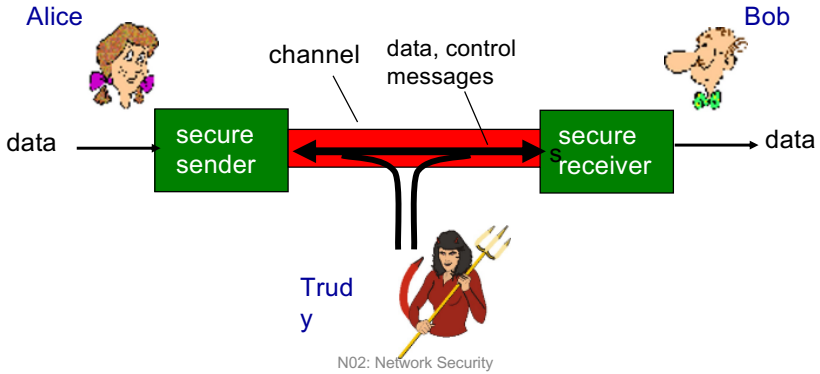
- **Security Attack:** Any action that **compromises** the security of information exchanges and systems

- **Security Service:** A service that **enhances** the security of information exchanges and systems. A security service makes use of **one or more security mechanisms**

- **Security Mechanism:** A mechanism that is designed to **detect, prevent, or recover** from a security attack

Friends and Enemies

- Well-known in network security world
- Bob, Alice (lovers!) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages



Who might Bob, Alice be?

- … well, real-life Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- On-line banking client/server
- DNS servers
- Routers exchanging routing table updates
- other examples?

4. Security Attacks

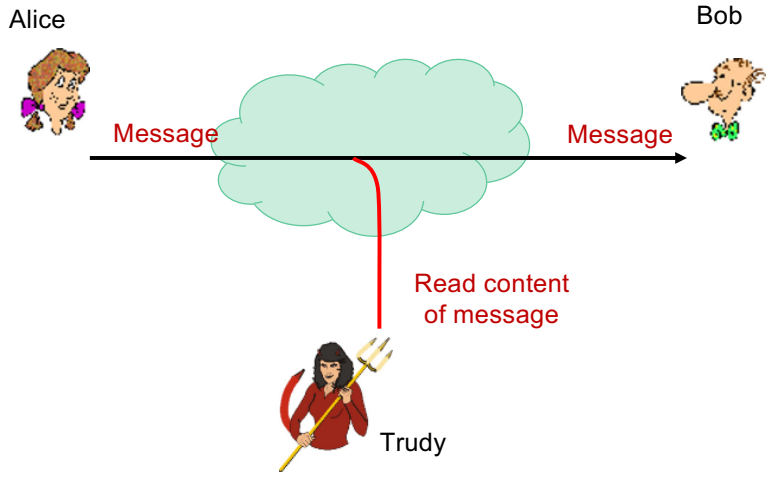
- Classification of security attacks
  Used in both ITU-T X.800 and RFC 4949
- Passive attacks
  Attempts to learn or make use of information, but does not affect the system resources
- Active attacks
  Attempts to alter system resources or affect their operation.

Security Attacks: Passive

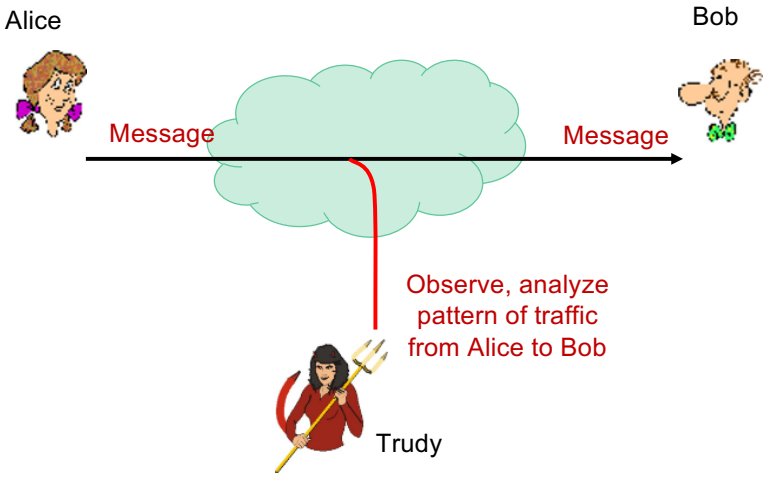
- Passive attacks: The goal of the opponent is to obtain information that is being transmitted.
- Two types of passive attack
  Release of message contents (eavesdropping)

  Traffic analysis (monitoring)

Passive Attack: Eavesdropping



Passive Attack: Traffic Analysis (Monitoring)



Passive Security Attacks: Features

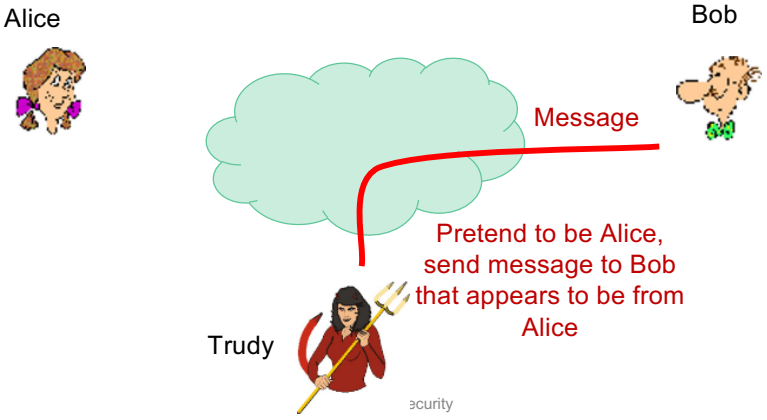
- Difficult to detect
  - Typically, the message traffic is sent and received in an apparently normal fashion, and
  - Neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern
- Prevention rather than detection
  - How? Encryption

Security Attacks: Active

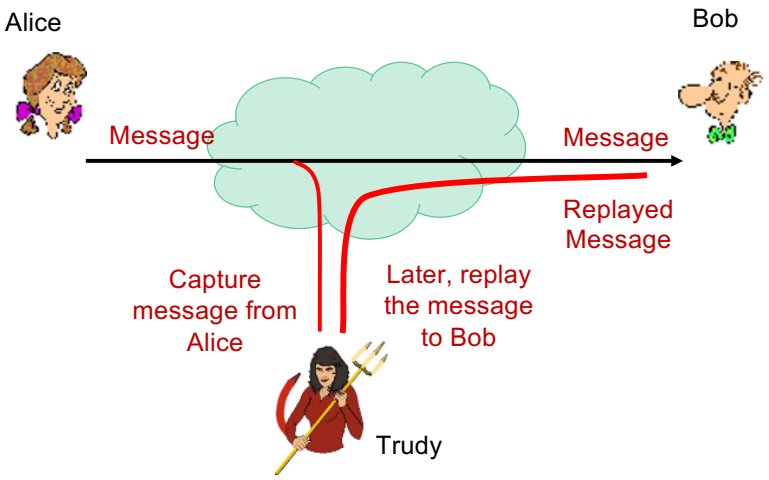
- Involve **some modifications** of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them
- Active attacks: four types
  - Masquerade (impersonate)
  - Replay
  - Message modification
  - Denial of Service

Masquerade

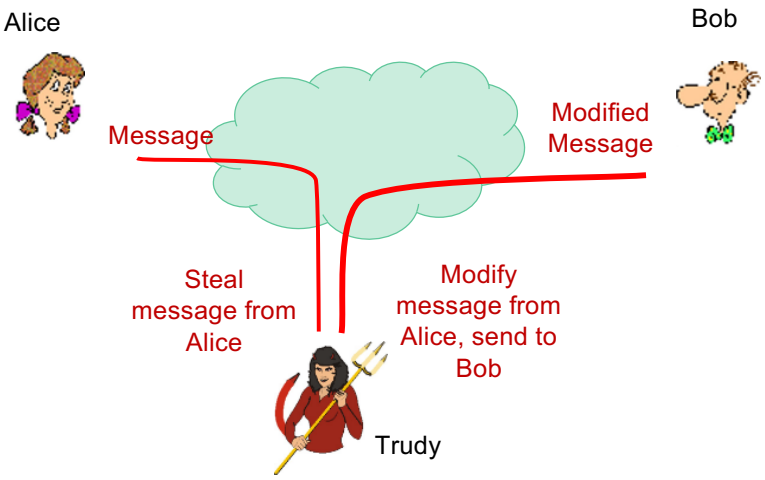
- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack



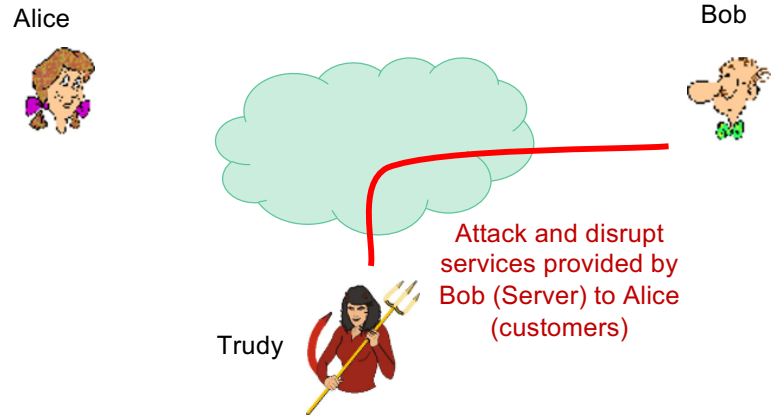
Replay



Message Modification



Denial of Service



5. Security Services

- Security Service (defined by X.800)
  - provided by protocol layer of communicating open systems
  - Ensures adequate security of the systems or data transfers
- X.800 groups services into 5 categories & 14 specific services

Security Services (cont.)

1. Authentication

   Assures communicating entity is the one that it claims to be

   Two services

   - Peer entity authentication: confidence in identity of the connected entities
   - Data-origin authentication: assurance of the data source

2. Access control

   The ability to limit and control the access to host systems and applications via communications links

   To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual

Security Services (cont.)

3. Data confidentiality: the protection of data from unauthorized disclosure, **in two senses**

   The protection of transmitted data from **passive attacks**

   - Broadest service protects all user data transmitted between two users over a period of time
   - Narrower forms of service include the protection of a single message or even specific fields within a message

   The protection of traffic flow **from analysis**: this requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Security Services (cont. 2)

4. Data integrity

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

5. Nonrepudiation (denied each other): prevents either sender or receiver from denying a transmitted message

   Nonrepudiation, Origin

   - Proof that the message was sent by the specified party.

   Nonrepudiation, Destination

   - Proof that the message was received by the specified party.

Security Services (cont. 3)

6. Availability Service

   The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system

6. Security Mechanisms

- X.800 also defines security mechanisms designed to **detect, prevent, or recover** from security attacks

- Grouped into two types

  Specific mechanisms: may be incorporated into **the appropriate protocol layer** in order to provide some of the security services

  Pervasive mechanisms: mechanisms that are **not specific to any particular security service or protocol layer**

Specific Mechanisms

*Specific mechanism: may be incorporated into **the appropriate protocol layer** in order to provide some of the security services*

- **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.

Specific Mechanisms (cont.)

- **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.

Pervasive Mechanisms

Pervasive mechanisms: *mechanisms that are **not specific to any particular security service or protocol layer***

- **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.

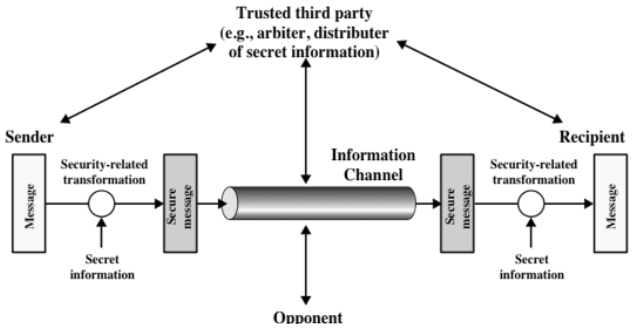
- **Security Recovery**

  Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Services vs Mechanisms

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			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

7. Secure Model: Components



All the techniques for providing security have two components

1. A security-related transformation on the information to be sent
   - encryption of the message
2. Some secret information shared by the two principals and, it is hoped, unknown to the opponent
   - encryption key used

That's all for today!