Network Security Essentials

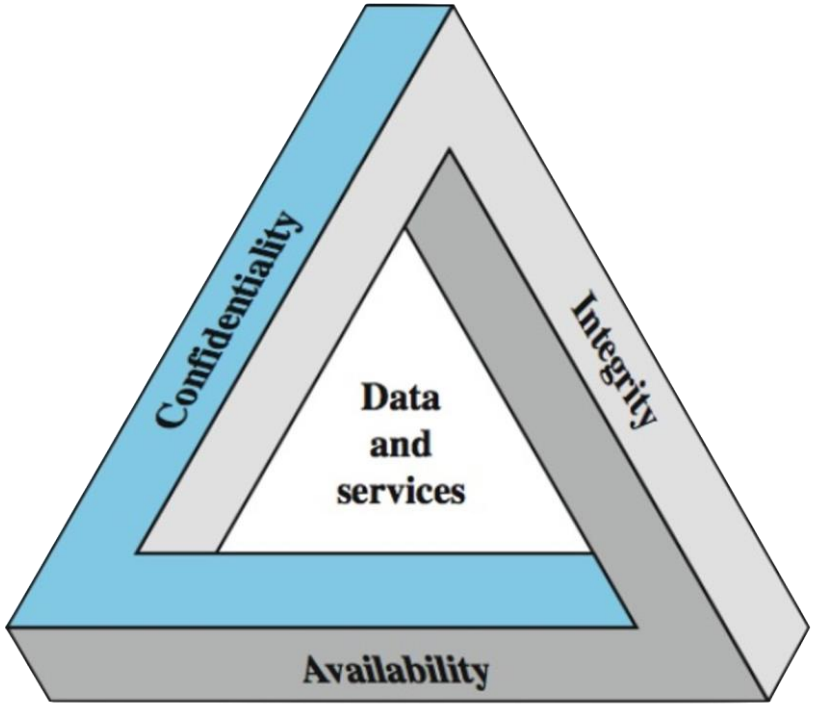
Kaminaga Yuma

Contents

1. Introduction

What is Computer Security?

- Protection provided to maintain the integrity, availability, and confidentiality of information system resources.

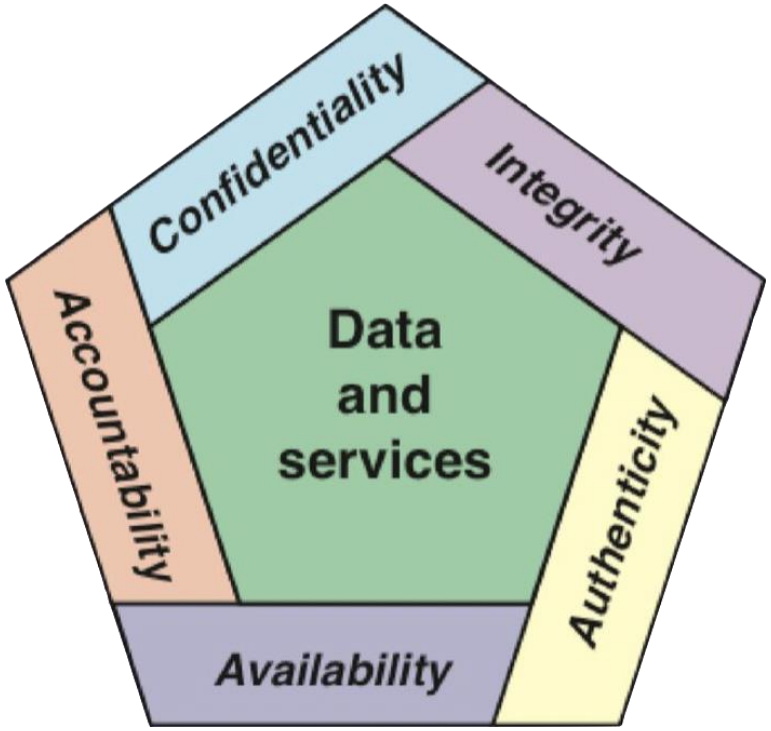


Three main goals of computer security

1. Confidentiality
   - Data confidentiality: Ensure that confidential information is not disclosed or disclosed to unauthorized individuals.
   - Privacy: To be able to control or influence the collection and storage of information that is relevant to you and to whom the information is disclosed.
2. Integrity
   - Data integrity: Ensures that data and programs are only modified in the manner specified
   - System integrity: Assurance that the system is protected and safeguarded from unauthorized searches without compromising its intended function
3. Availability
   - Ensure that the system operates quickly and does not interfere with the provision of services to legitimate users.

Concepts to be added to the Three main goals of computer security

1. Authenticity
   - Ensure that the message and sender are trustworthy.
   - Verifying that the user is who they say they are.
2. Accountability
   - Ensure that the entity behavior can be uniquely tracked.



2. The OSI Security Architecture

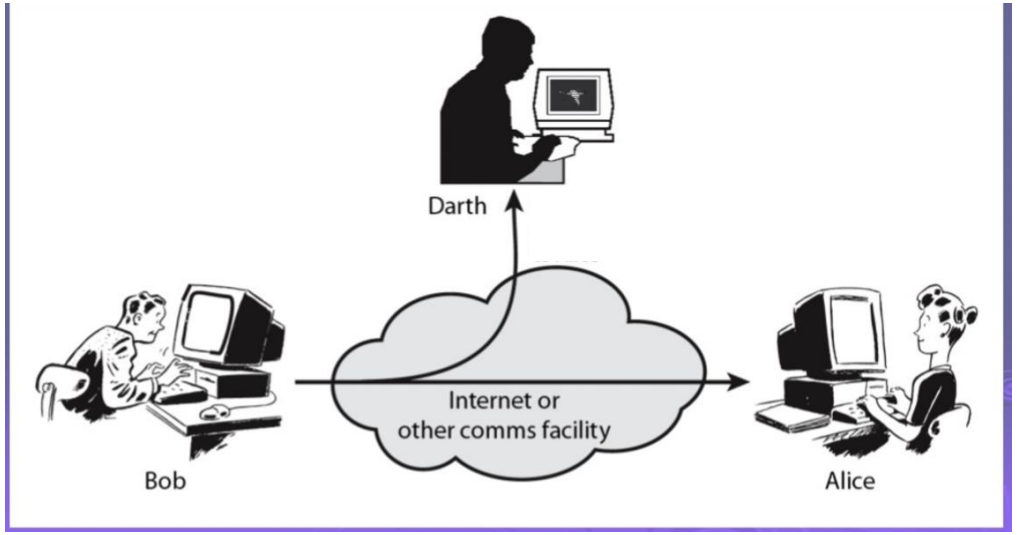
The OSI security architecture focuses

1. Security attack:
   - Violating the security of information owned by the organization
2. Security mechanism:
   - Processes designed to detect, prevent and recover from security attacks
3. Security service:
   - Processes or communication services that increase the security of an organization’s data processing system or information transfer

3. Security Attacks

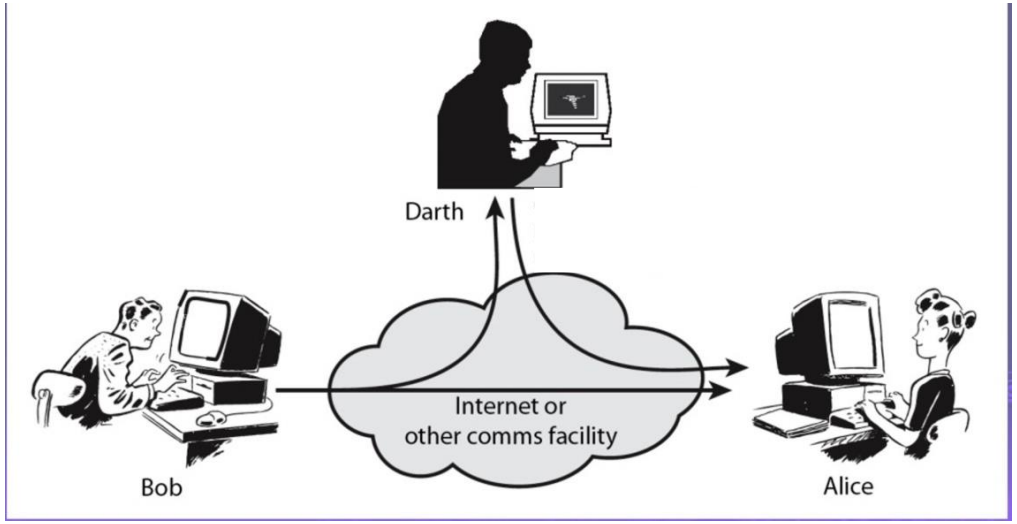
Passive Attacks

1. Release of message content
   - Obtaining confidential information such as telephone conversations, emails, or transferred files
2. Traffic analysis
   - Obtaining patterns, frequency and length of messages, and the location and identity of communicating hosts



Active Attacks

1. Masquerade
   - Occurs when one entity pretends to be another entity
2. Replay
   - Capturing data and then re-transmitting it to produce illicit effects
3. Modification of messages
   - Altering part of a legitimate message.
   - Delaying or re-ordering
4. Denial of service
   - Interference with telecommunication facilities
   - Disables or overloads the network, degrading performance



4. Security Services

Authentication

1. Peer entity authentication
   - Provided to verify the identity of peer entities during collaboration.
   - Provides confidence that the entity is not impersonating or illegally retransmitting a previous connection.
2. Data origin authentication
   - Provided to verify the source of the data unit.
   - Support applications where there is no prior interaction between communicating entities, such as e-mail.

Access Control

- Controls who can access resources, under what conditions access is granted, and what the person accessing the resource is authorized to do

Data Confidentiality

- Protecting transmitted data from passive attacks
- Require that an attacker be unable to observe characteristics such as the source and destination of communications.

Data Integrity

- Defense against active attacks.
- If a violation is detected, human intervention is required for the software to recover from the violation. Alternatively, there are mechanisms to recover automatically.

Nonrepudiation

- Prevent the sender or receiver from denying the message sent.

Availability Service

- Services to protect system availability
- The property of being accessible and usable on demand by authorized system entities

5. Security Mechanisms

Specific Security Mechanisms

1. Encipherment
   - Transforming data into a form that is not easily understood
2. Digital Signature
   - Allows the recipient to prove the origin and integrity of the data and protect it from counterfeiting
3. Access Control
   - A variety of mechanisms that enforce access rights to resources.
4. Data Integrity
   - Mechanisms used to ensure integrity.

Specific Security Mechanisms

5. Authentication Exchange
   - Ensuring the identity of the entity through the exchange of information.
6. Traffic Padding
   - Inserting bits into gaps in the data stream to interfere with traffic analysis.
7. Routing Control
   - Ensure that a secure route can be selected in the event of a suspected security breach.
8. Notarization
   - A trusted third party can be used to guarantee the characteristics of the data exchange.

Pervasive Security Mechanisms

1. Trusted Functionality
   - What is perceived to be correct with respect to a given criterion.
2. Security Label
   - Indicates the security attributes of a resource. (e.g., confidential, public, etc.)
3. Event Detection
   - Detection of security-related events
4. Security Audit Trail
   - A collection of data from system records and activities that are used to perform security audits
5. Security Recovery
   - Addressing security problems that occur in a system and returning the system to a normal state

6. A Model for Network Security

- A message is transmitted from sender to recipient via some Internet service. An information channel defines the route from the sender to the recipient and is established using a communications protocol (such as TCP/IP).

- The security aspect serves to protect the information channel from potential threat actors when exposed to threats.

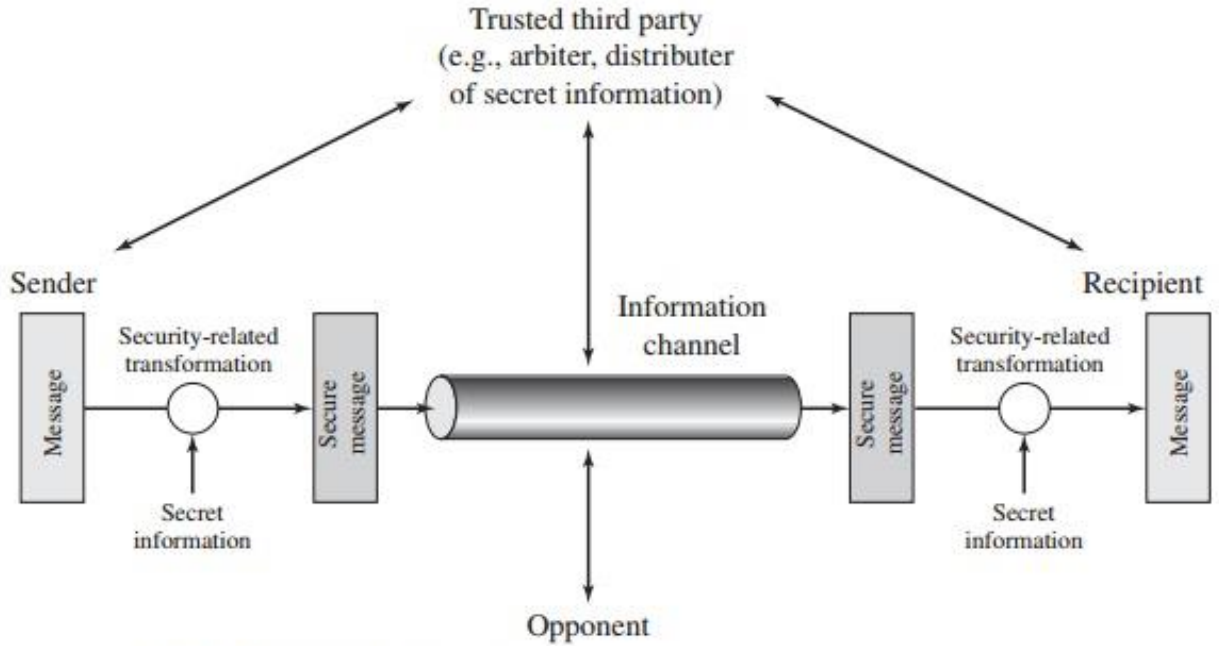


Figure 1.4 Model for Network Security

Technical elements to provide security

1. Security transformation of transmitted information
   - Encrypting messages or adding code based on message content.
2. Sharing of confidential information
   - Encryption keys, etc. Used to encrypt a message and decrypt it upon reception.

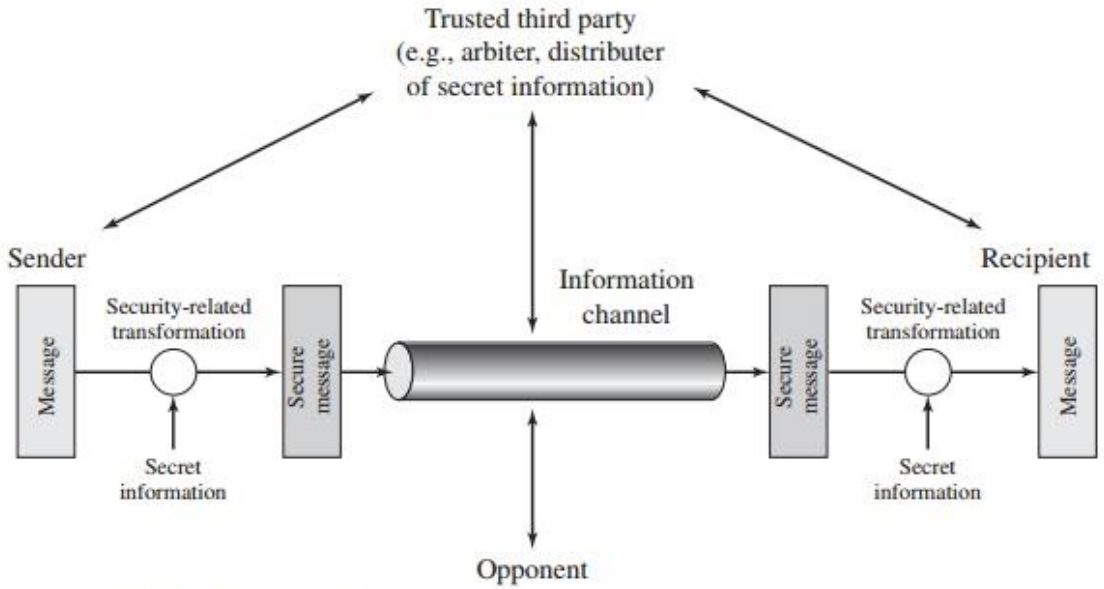


Figure 1.4 Model for Network Security

Design of security services

1. Algorithm Design
   - Design security algorithms that prevent attackers from achieving their objectives.
2. Generation of secret information
   - Generate secret information to be used with the algorithm.
3. Develop methods of distributing secret information
   - Develop a method to securely share secret information.
4. Specify protocols
   - Specify protocols for use of algorithms and secret information

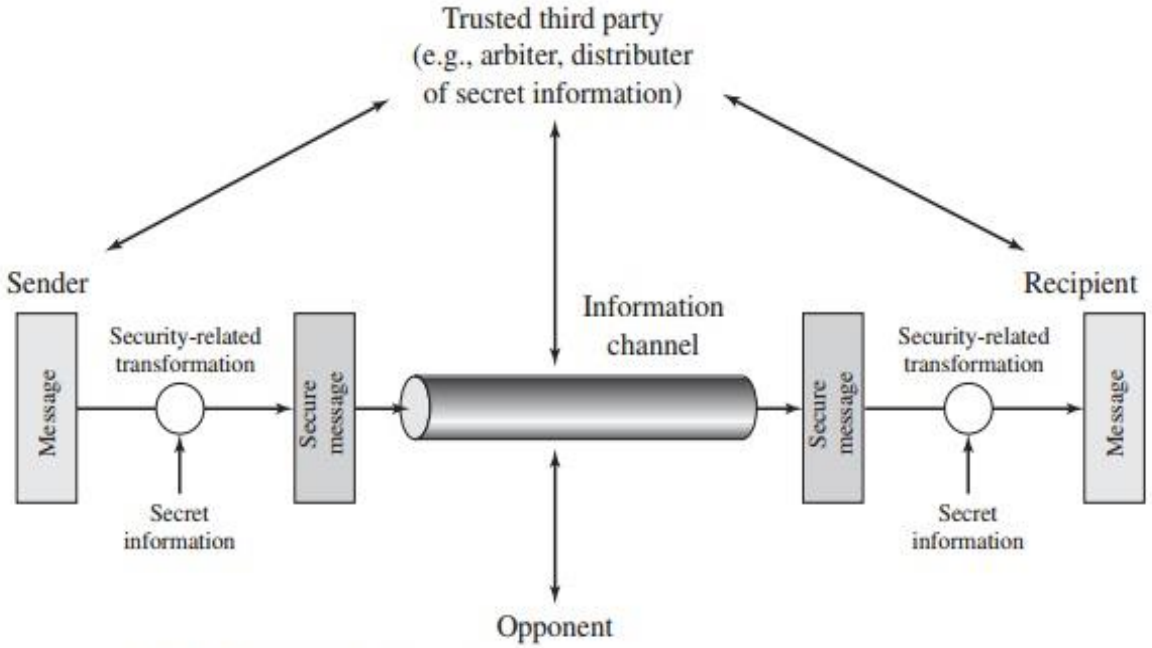


Figure 1.4 Model for Network Security

System protection and Security mechanisms

Threats

1. Information Access Threats
   - Unauthorized users intercepting or altering data
2. Service Threats
   - Taking advantage of service flaws to prevent legitimate users from using the service

Security mechanisms

1. Gatekeeper Functions
   - Password-based login procedures, detecting and eliminating viruses, etc.
2. Internal Controls
   - Those that monitor activity and analyze information to detect unauthorized intruders

Thank you for listening