Systems' Security | *Segurança de Sistemas*

Introduction – Computer Security Concepts

Miguel Frade

POLITÉCNICO DE LEIRIA
ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Overview

Introduction

The OSI security Architecture

- **Security attack** – any action that compromises the security of information owned by an organization;

The OSI security Architecture

- **Security attack** – any action that compromises the security of information owned by an organization;
- **Security mechanism** – a process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack;

The OSI security Architecture

- **Security attack** – any action that compromises the security of information owned by an organization;
- **Security mechanism** – a process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack;
- **Security service** – a processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service;

Types of Security attacks:

- **Passive attacks** – The goal of the opponent is to obtain information that is being transmitted and is in the nature of eavesdropping on, or monitoring of, transmissions. There are two types:
  - release of message contents
  - traffic analysis – observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Types of Security attacks (continuation):

- **Active Attacks** – involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:
  - **masquerade** – when one entity pretends to be a different entity and usually includes one of the other forms of active attack;
  - **replay** – passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect;
  - **modification of messages** – some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect
  - **denial of service** – prevents or inhibits the normal use or management of communications facilities;

Security Services

Security service

a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.

Security Services:

1. **Availability** – it's a service that protects a system to ensure its availability and assure that systems work promptly and service is not denied to authorized users;

Security Services:

1. **Availability** – it's a service that protects a system to ensure its availability and assure that systems work promptly and service is not denied to authorized users;
2. **Data Confidentiality** – it's a service to assure that private or confidential information is made available or disclosed **only** to authorized entities (person, organization, or computer):
   - **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;

Security Services (continuation):

3. **Data Integrity** – it's a service to assure that data received is exactly as sent by an authorized entity:
   - 3.1 **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, with recovery attempted;
   - 3.2 **Connection Integrity without Recovery** – as above, but provides only detection without recovery;
   - 3.3 **Selective-Field Connection Integrity** – provides for the integrity of selected fields within the user data of a data block transferred over a connection and detects whether the selected fields have been modified, inserted, deleted, or replayed;
   - 3.4 **Connectionless Integrity** – provides for the integrity of a single connectionless data block and may take the form of detection of data modification.
   - 3.5 **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;

Security Services (continuation)

4. **Authentication** – it's a service to assure that an entity (person, organization, or computer) is the one she 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;

Security Services (continuation)

4. **Authentication** – it's a service to assure that an entity (person, organization, or computer) is the one she 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;

5. **Access Control** – it's a service to prevent the unauthorized use of a **resource**;

Security Services (continuation)

4. **Authentication** – it's a service to assure that an entity (person, organization, or computer) is the one she 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;

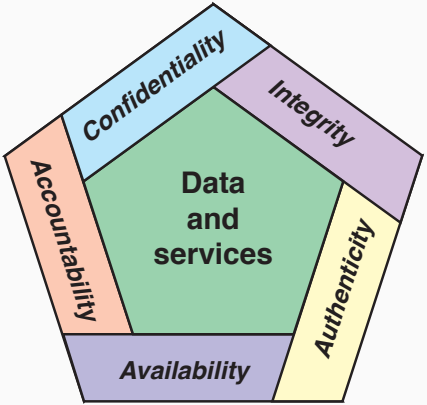
5. **Access Control** – it's a service to prevent the unauthorized use of a **resource**;

6. **Non-repudiation** – it's a service to assure that an entity can not deny its participation in all or part of a communication:
   - **Source non-repudiation** – Proof that the message was sent by the specified party;
   - **Destination non-repudiation** – Proof that the message was received by the specified party;

Not part of the X.800 standard, but important:

7. **Accountability** – it's a service to assure that generates the requirement for actions of an entity to be traced uniquely to that entity:
   - this supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action;
   - because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party;
   - systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes;

Esssential Network and Computer Security Requirements



Security Mechanisms

Security Mechanism

Security mechanisms are technical tools and techniques that are used **to implement security services**. A mechanism might operate by itself, or with others, to provide a particular service.

Security Mechanisms:

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

Security Mechanisms:

- **Specific security mechanisms** – may be incorporated into the appropriate protocol layer in order to provide some of the security services;
- **Pervasive security mechanisms** – mechanisms that are not specific to any particular security service or protocol layer;

List of **Specific Security Mechanisms**:

- **Encipherment** – use of encryption algorithms;

List of **Specific Security Mechanisms**:

- **Encipherment** – use of encryption algorithms;
- **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);

List of **Specific Security Mechanisms**:

- **Encipherment** – use of encryption algorithms;
- **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 (*i. e.* firewalls);

List of **Specific Security Mechanisms**:

- **Encipherment** – use of encryption algorithms;
- **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 (*i. e.* firewalls);
- **Data Integrity** – a variety of mechanisms used to assure the integrity of a data unit or stream of data units;

List of **Specific Security Mechanisms** (continuation):

- **Authentication Exchange** – a mechanism intended to ensure the identity of an entity by means of information exchange;

List of **Specific Security Mechanisms** (continuation):

- **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;

List of **Specific Security Mechanisms** (continuation):

- **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;

List of **Specific Security Mechanisms** (continuation):

- **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;

List of **Pervasive Security Mechanisms**:

- **Trusted Functionality** – that which is perceived to be correct with respect to some criteria (e.g., as established by a security policy;

List of **Pervasive Security Mechanisms**:

- **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;

List of **Pervasive Security Mechanisms**:

- **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;

List of **Pervasive Security Mechanisms**:

- **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;

List of **Pervasive Security Mechanisms**:

- **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;

Relationship Between Security Services and 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			

Attack Surfaces

Attack Surfaces

An attack surface consists of the reachable and exploitable vulnerabilities in a system.

Attack Surfaces

An attack surface consists of the reachable and exploitable vulnerabilities in a system.

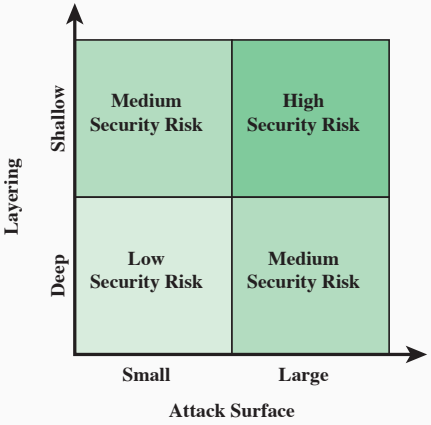
Attack surfaces can be categorized as follows:

- **Network attack surface** – vulnerabilities over an enterprise network, wide-area network, or the Internet.
- **Software attack surface** – vulnerabilities in application, utility, or operating system code.
- **Human attack surface** – vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

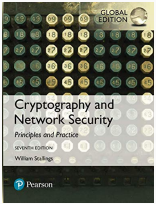
Examples of attack surfaces:

- Open ports on outward facing Web and other servers, and code listening on those ports
- Services available on the inside of a firewall
- Code that processes incoming data, email, XML, office documents, and industry specific custom data exchange formats
- Interfaces, SQL, and Web forms
- An employee with access to sensitive information vulnerable to a social engineering attack

Defense in depth versus attack surface



Questions?



Chapter 1 of
William Stallings, Cryptography and Network Security: Principles and Practice, Global Edition, 2016