الجامعة الإفتراضية السورية

أمن الشبكات

Network and Infrastructure Security

د. محمد العصورة

Dr. Mohammed Assora

دكتوراه في امن شبكات الحواسب

PhD. In Computer Network Security

Introduction to Network Security

Objectives of Lecture

- Understand why security should be a fundamental consideration when designing and operating networks.
- Understand the meaning of security policy and security life cycle.
- Examine the *primary enabling* threats and *fundamental* threats to security for networks.
- Introduce security *services* and *mechanisms*, and show how they can be used to counter threats.

Contents

Why Network Security? (1)

- A network is a system of interconnected computers.
- As everything is related to the internet and will continue to grow in coming years, security becomes an important part of it.
- As many people use online shopping and other banking services to transfer money. It becomes necessary that their privacy needs to be safe guarded in order to prevent data loss.
- Network security is just not related to data. Nowadays many countries control each and every means of transport system through their private network, like the airlines, traffic signals, electricity substation, etc.

Why Network Security? (2)

- Imagine if any hacker with a bad intention breaks into such systems and shuts down the system or alters the system
- Planes would crash, signals will not work. communication systems may go down, along with electricity blackouts.
- So in order to prevent such situations, network security is give more importance in every part of the world.
- Network security is the backbone of the network. If it fails the system goes down or gets compromised. Safeguarding one’s network is just as important as safeguarding one’s home.

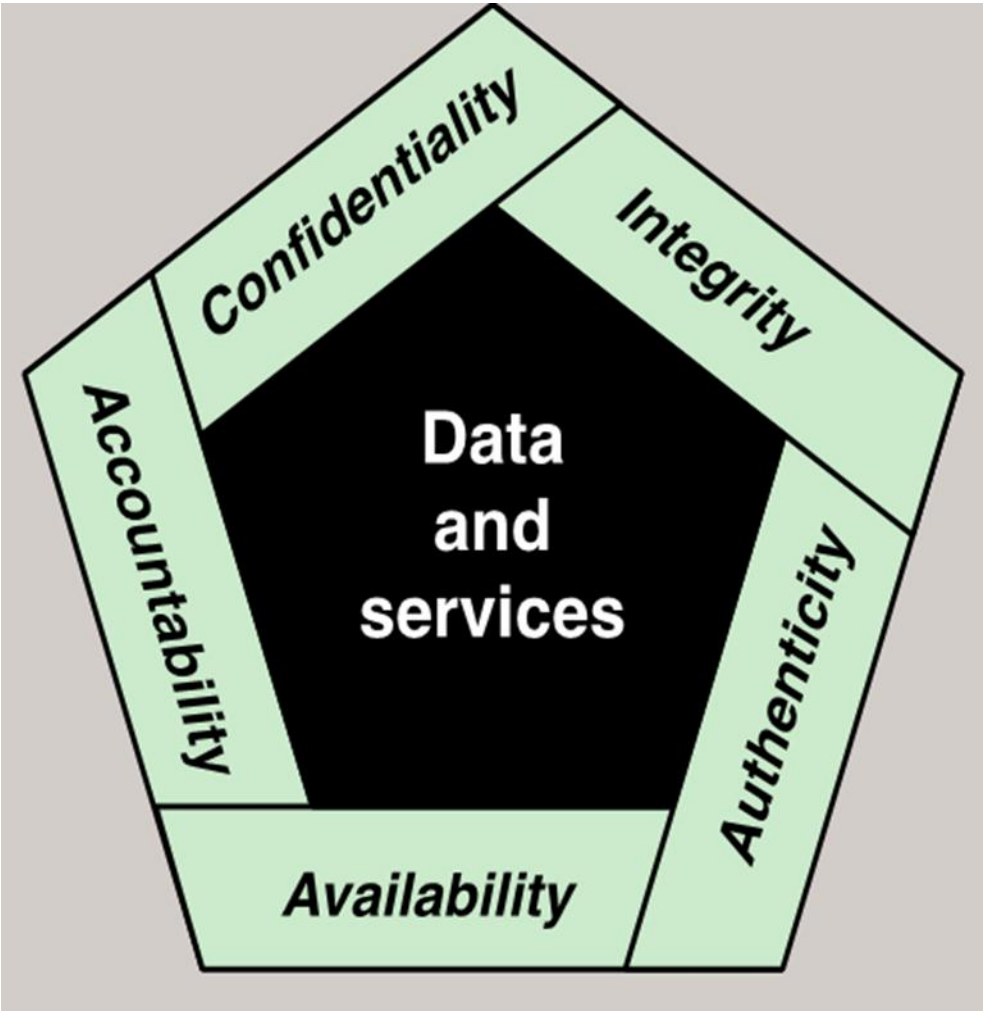
A Definition of Network Security

- Network security is the process of taking preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure.

- This definition introduces three key objectives that are at the heart of computer and network security: integrity, availability, and confidentiality. what is often referred to as the CIA triad.

- additional concepts are needed to present a complete picture: authenticity and Accountability.

Essential security requirements



Security Policies for Networks (1)

- When designing a secure system:
- The security domain is the scope of the system
- The security policy is the set of rules governing the security behavior of the system.

- A security policy is defined in ISO 7498-2 as ‘the set of criteria for the provision of security services’.

Security Policies for Networks (2)

- In more details the security policy for a network should:
  - Interpret the overall Information Security Policy in the context of the networked environment:
  - Defines what is the responsibility of the network and what is not.
  - Describes what security is to be available from the network.
  - Describes rules for using the network.
  - Describes who is responsible for the management and security of the network.

Types of security policy

- ISO 7498-2 distinguishes between 2 types of security policy:
  - identity-based: where access to and use of resources are determined on the basis of the identities of users and resources,
  - Rule-based: where resource access is controlled by global rules imposed on all users, e.g. using security labels.

The Security Life-Cycle

- A generic model for the security life-cycle is as follows:
  - define security policy,
  - analyse security threats (according to policy) and associated risks, given existing safeguards,
  - define security services to meet/reduce threats, in order to bring risks down to acceptable levels,
  - define security mechanisms to provide services,
  - provide on-going management of security.

Security terminologies (1)

- A threat is: a possible means by which a security policy may be breached.
- An attack is: a realization of a threat (e.g. stealing data, denial of service attack)
- Safeguards are: measures (e.g. controls, procedures) to protect against threats.
- Vulnerabilities are: weaknesses in safeguards.

Security terminologies (2)

- A Risk is: a measure of the cost of a vulnerability (taking into account probability of a successful attack).
- A security service is a measure which can be put in place to address a threat (e.g. provision of confidentiality).
- A security mechanism is a means to provide a service (e.g. encryption, digital signature).

Security attacks

- Security attacks can be defined as: Any action that compromises the security of information owned by an organization.

- Security attacks can be classified under two main categories, namely, passive attacks and active attacks.

Passive attacks

- The attacker does not make any effect on the exchanged data.
- The attacker only eavesdrops or monitors the transmission channel between the sender and the receiver.
- These types of attacks are very simple and normally they are always available.
- The goal of the attack is to obtain information about the transmitted data.

Active attacks (1)

- These types of attacks are more professional than passive attacks. The attacker can initiate connections, modify messages, deny messages and replay messages.

- The most important active attacks are:
- **Impersonation:** In this type of attack, the attacker pretends to be one of the legitimate parties (the sender or the receiver).

- **Modification of messages:** The attacker changes the exchanged data by insertion, deletion, reordering, delay or changing the content of the legitimate messages.

Active attacks (2)

- **Replay attack:** The attacker captures a message from a legitimate connection and replays the message again to produce unauthorized effect.

  Example of this attack is to capture the packet which contains the encrypted password from a user. The attacker replays this packet to have unauthorized access.

- **Denial of services:** The goal of these attacks is to prevent or degrade the network resources on the legitimate users.
- One example of denial of service attack is to bombard an Email server with so much spam that is not able to cope.

Active VS. passive attacks

- By comparing active and passive attacks
- Passive attacks are difficult to detect but easy to prevent, by using cryptography.
- Active attacks can be detected but not totally prevented.
- Normally, perfect security is not realistic and for business, “good enough security is good enough” .

Security Services and Mechanisms

- A security threat is a possible means by which a security policy may be breached (e.g. loss of integrity or confidentiality).

- A security *service* is a measure which can be put in place to address a threat (e.g. provision of confidentiality).

- A security *mechanism* is a means to provide a service (e.g. encryption, digital signature).

Security Service Classification

- Five main categories of security service:
  - Authentication (including entity authentication and origin authentication),
  - Access control,
  - Data confidentiality,
  - Data integrity,
  - Non-repudiation.

Authentication

- Authentication is the assurance that the communication entity is the one that it claims to be. The authentication can be applied to entities and information. Therefore, authentication can be divided into two services:
- **Entity authentication:** In a logical connection, the authentication provides a confidence that the identities of the entities connected are genuine.
- **Data origin authentication:** It provides assurance that the source of received data is as claimed. However, it does not provide any assurance of the integrity of the data.

- In computer systems, there are two types of authentication, firstly, client authentication, where only the user authenticates him/herself to the server. Secondly, mutual authentication, where the user and the server authenticate each other.

Access Control

- Provides protection against unauthorised use of resource, including:
  - use of a communications resource,
  - reading, writing or deletion of an information resource,
  - execution of a processing resource.

- 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.

Data Confidentiality

- Confidentiality (or privacy) is a service used to keep the content of information secret from all but those authorized to have it.

- The main attacks on data confidentiality are the passive attacks. Therefore, the main focus is to prevent the attacks and this can be achieved in many ways, ranging from physical security to the use of cryptography.

Data Integrity

- Data integrity is a service which addresses the unauthorized alteration of data.
- For example, the integrity of transmitted messages assures that the messages are received as sent i.e. no modification, insertion, deletion, replays, or reordering has been carried out on these messages.
- The main attacks on data integrity are the active attacks. Therefore, the main focus is to detect the attacks.

Non-repudiation

- Non-repudiation is a service which prevents an entity from denying previous commitments or actions.

- Thus, the sender has irrefutable proof that the receiver received the message and the receiver has irrefutable proof that the sender sent the message.

- Repudiation is not an attack, but rather, it can be constructed as misbehaviour from the legitimate users. Therefore, in a case where an entity repudiates the action, a trusted third party is needed to solve the dispute.

Security Mechanisms

- Eight types:
  - encipherment,
  - digital signature,
  - access control mechanisms,
  - data integrity mechanisms,
  - authentication exchanges,
  - traffic padding,
  - routing control,
  - notarisation.

Security Mechanisms (1)

- Encipherment mechanisms = encryption algorithms.
  - Can provide data and traffic flow confidentiality.
  - Covered in detail in the next chapters
- Digital signature mechanisms
  - signing procedure (private),
  - verification procedure (public).
  - Can provide non-repudiation, origin authentication and data integrity services.
  - Also addressed in detail in the next chapters
- Both can be basis of some authentication exchange mechanisms.

Security Mechanisms (2)

- Access Control mechanisms
  - A server using client information to decide whether to grant access to resources
    - E.g. access control lists, capabilities, security labels.
- Data integrity mechanisms
  - Protection against modification of data.
    - Provide data integrity and origin authentication services. Also basis of some authentication exchange mechanisms.
- Authentication exchange mechanisms
  - Provide entity authentication service.

Security Mechanisms (3)

- Traffic padding mechanisms
  - The addition of ‘pretend’ data to conceal real volumes of data traffic.
  - Provides traffic flow confidentiality.
- Routing control mechanisms
  - Used to prevent sensitive data using insecure channels.
  - E.g. route might be chosen to use only physically secure network components.
- Notarisation mechanisms
  - Integrity, origin and/or destination of data can be guaranteed by using a 3rd party trusted notary.
    - Notary typically applies a cryptographic transformation to the data.