Network Security Concepts

Learning Objective

After studying this chapter, you should be able to:

- 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.
- Study the provision of security services at different network layers in ISO7498-2.

1.Why Network Security

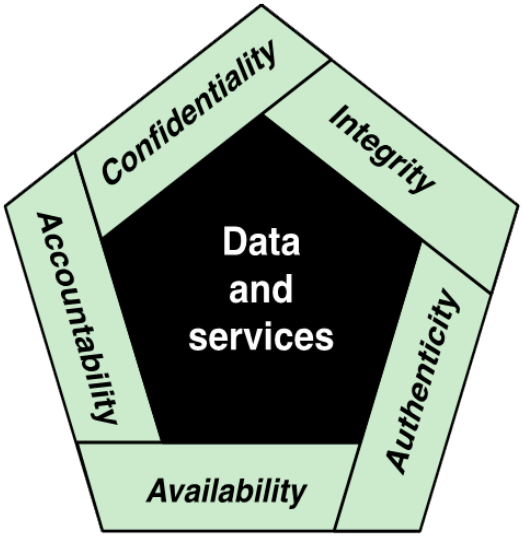
A network is a system of interconnected computers. Billions & trillions of bytes of data is sent back and forth over the internet every hour every day. As everything is related to the internet and will continue to grow in coming years, security becomes an important part of it. As many people use online shopping and other banking services to transfer money, without the need of going to the bank and standing in the long queues to save time, 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. So just imagine if any hacker with a bad intention breaks into such systems and shuts down the system or alters the system that may cause havoc in the vicinity. 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 given 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.

2. Definition of Network Security

According to the SANS Institute, 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. Implementing these measures allows computers, users and programs to perform their permitted critical functions within a secure environment.

This definition introduces three key objectives that are at the heart of computer and network security: integrity, availability, and confidentiality. These three concepts form what is often referred to as the CIA triad. Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture Figure(1.1). Two of the most commonly mentioned are: authenticity and Accountability.



Figure(1.1): Essential Security Requirements

3.Security Policy for Network

When designing a secure system, the scope of the system and the set of rules governing the security behavior of the system are of fundamental importance, these are the security domain and the security policy respectively.

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

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.

4.Security Life Cycle

A security program is not a static assessment or a finished product. Rather it requires constant attention and continual improvement. Security policy is the foundation to any component of a security plan. Therefore a generic model for the security life-cycle, including network security issues, is as follows:

- Define security policy.
- Analyze 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.

To explain the used terminologies:

A threat is: a possible means by which a security policy may be breached. in other words, a security threat is: a person, thing, event or idea which poses some danger to an asset (in terms of confidentiality, integrity, availability or legitimate use). An example of threats (information leakage, integrity violation, illegitimate use, …).

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.

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).

5.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.

5.1.Passive Attacks

In these types of 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.

5.2.Active Attacks

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 (or masquerade): In this type of attack, the attacker pretends to be one of the legitimate parties (the sender or the receiver).
- 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.
- Modification of messages: The attacker changes the exchanged data by insertion, deletion, reordering, delay or changing the content of the legitimate messages.
- 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.

By comparing active and passive attacks, it can be observed that passive attacks are difficult to detect but easy to prevent, normally by using cryptography. Active attacks can be detected but not totally prevented because of the wide variety of potential physical, software, and network vulnerabilities. Instead, the goal is to detect active

attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention. Normally, perfect security is not realistic and for business, “good enough security is good enough”.

6.Security Services

Security services are used to counter security attacks and to enhance the security of the data processing and data transfers of an organization. Security services implement security policies and are implemented by security mechanisms. Security services can be divided into five main categories, namely authentication, data integrity, data confidentiality, access control, and nonrepudiation.

6.1.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.

6.2.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.

6.3.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. If a violation of integrity is detected, then the service may simply report this violation, and some other portion of software or human intervention is required to recover from the violation.

6.4.Access Control

In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links, and this includes:

- 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.

6.5.Nonrepudiation

Nonrepudiation 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 misbehavior from the legitimate users. Therefore, in a case where an entity repudiates the action, a trusted third party is needed to solve the dispute.

7.Security Mechanisms

A security mechanism is the mechanism that is designed to achieve the security services and to detect, prevent or recover from security attacks. To achieve a security service or to prevent an attack more than one security mechanism can be used. Table(1.1) shows the relationships between security services and mechanisms. The most important security mechanisms are:

- Encipherment Mechanisms: encryption or cipher algorithms. Can provide data and traffic flow confidentiality. In addition, it can be basis of some authentication exchange mechanisms.
- Digital Signature Mechanisms: signing procedure (private), verification procedure (public). Can provide non-repudiation, entity an data origin authentication and data integrity services.
- 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.
- 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.
- Notarization 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.

Security mechanisms will be addressed in details in the next chapters.

Service \ Mechanism	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Entity Authentication	Y	Y			Y			
Data Origin Authentication	Y	Y						
Access Control			Y				Y	
Confidentiality	Y						Y	
Traffic Flow Confidentiality	Y					Y		
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Table(1.1): Relationship Between Services and Mechanisms

8.Security Services and Layers

ISO 7498-2 lays down which security services may be provided in what parts of the OSI model. The information is summarized in Table(1.2), which indicates which services may be placed in which layers of the OSI model.

- Layers 1 and 2 are restricted to providing certain types of confidentiality services.
- Layers 3 and 4 can provide authentication, access control, confidentiality (layer 3 only) and integrity services.
- No security services can be provided in Layer 5 or Layer 6, although Layer 6 may contain facilities to support the provision of services at Layer 7.
- All security services may be provided at Layer 7.

There are good reasons for varying the position of security functionality within the OSI layer hierarchy depending on the type of network in use. For the maximum degree of traffic flow confidentiality, data encryption needs to be placed at the lowest possible layer (to hide the protocol addresses). Low level placement also offers

common security support for all the different applications running across the network. If end-to-end security is required, then the security services must be placed in Layer 3 or above. If application-specific security services are required, then the security must be placed in Layer 7.

Service / Layers	1	2	3	4	5	6	7
Entity Authentication			Y	Y			Y
Data Origin Authentication			Y	Y			Y
Access Control			Y	Y			Y
Confidentiality	Y	Y	Y	Y			Y
Traffic Flow Confidentiality	Y		Y				Y
Data Integrity			Y	Y			Y
Nonrepudiation							Y

Table(1.2): Service/ Layer

Exercises:

True or False

Question	True	False
1. Security attacks are classified as either passive or aggressive.		
2. Authentication protocols and encryption algorithms are examples of security mechanisms.		
3. The more critical a component or service, the higher the level of required availability.		
4. Thanks to years of research and development, it is now possible to develop security design and implementation techniques that systematically exclude security flaws and prevent all unauthorized actions.		
5. The field of network and Internet security consists of measures to deter, prevent, detect and correct security violations that involve the transmission of information.		
6. The OSI security architecture was not developed as an international standard, therefore causing an obstacle for computer and communication vendors when developing security features.		
7. Data origin authentication does not provide protection against the modification of data units.		
8. The emphasis in dealing with active attacks is on prevention rather than detection.		
9. All the techniques for providing security have two components: a security-related transformation on the information to be sent and some secret information shared by the two principals.		
10. The data integrity service inserts bits into gaps in a data stream to frustrate traffic analysis attempts.		

Multiple Choice Questions

1. A common technique for masking contents of messages or other information traffic so that opponents cannot extract the information from the message is _____ .
   A. integrity
   B. encryption
   C. analysis
   D. masquerade

2. _____ involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
   A. Disruption
   B. Replay
   C. Service denial
   D. Masquerade

3. A loss of _____ is the unauthorized disclosure of information.
   A. authenticity
   B. confidentiality
   C. reliability
   D. integrity

4. Verifying that users are who they say they are and that each input arriving at the system came from a trusted source is _____ .
   A. authenticity
   B. credibility
   C. accountability
   D. integrity

5. A _____ is any action that compromises the security of information owned by an organization.
   A. security attack
   B. security service
   C. security alert
   D. security mechanism

6. A _____ takes place when one entity pretends to be a different entity.
   A. replay
   B. masquerade
   C. service denial
   D. passive attack

7. _____ is the protection of transmitted data from passive attacks.
   A. Access control
   B. Data control
   C. Nonrepudiation
   D. Confidentiality

8. A(n) _____ service is one that protects a system to ensure its availability and addresses the security concerns raised by denial- of- service attacks.
   A. replay
   B. availability
   C. masquerade
   D. integrity

9. _____ threats exploit service flaws in computers to inhibit use by legitimate users.
   A. Information access
   B. Reliability
   C. Passive
   D. Service

10. A(n) _____ is a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm.

A. threat

B. attack

C. risk

D. attack vector

References

1. Stallings, W.: Cryptography and Network Security: Principles and Practice, 7th edn. Prentice Hall (2017).
2. Stallings, W.: Network Security essentials: application and standards, 6th edn. Pearson India Education Services Pvt. LTD (2017).
3. https://www.sans.org/network-security/.

Number of the Question	True	False
1		✓
2	✓	
3	✓	
4		✓
5	✓	
6		✓
7	✓	
8		✓
9	✓	
10		✓

Number of the Question	Answer
1	B
2	B
3	B
4	A
5	A
6	B
7	D
8	B
9	D
10	A