1. **Security in distributed systems may be considered as consisting of two parts. Describe each of these parts.**

Security in distributed systems consists of two parts:

• Communication security - concerns communication between users/processes (principal mechanism - secure channel)

• Authorization security - concerns processes only getting those access rights to resources they are entitled to (principal mechanism - access control).[1]

1. **What is communication security concerned with?**

Communication security concerns communication between users/processes (principal mechanism - secure channel).

1. **What is authorisation security concerned with?**

Authorisation security concerns processes only getting those access rights to resources they are entitled to (principal mechanism - access control).

1. **Describe what is meant by a security incident and a security threat. In doing so describe the relationship between both concepts.**

A security incident is an event that occurs when an organization’s systems or data is compromised. And a security threat is a potential cause of a security incident.

1. **Describe three types of security threats.**

There are four types of security threats to consider:

Interception - unauthorized party gains access to a service or data.

Interruption - services or data become unavailable, unusable, destroyed etc.

Modification - unauthorized changing of data or tampering with a service so that it no longer adheres to its original specifications.

Fabrication - additional data or activity are generated that would normally not exist.

1. **What is a security policy? How may a security policy be enforced?**

A security policy describes the actions entities in a system are allowed to take and which are prohibited, here entities include users, services, data, machines, etc.

We usually use security mechanisms to enforce security policies to reduce security threats.

1. **Describe three important security mechanisms in the context of distributed systems.**

Important security mechanisms are:

Encryption - transforms data into something an attacker cannot understand.

Authentication - used to verify the claimed identity of a user, client, server, host, or other entity.

Authorization - check whether a client is authorized to perform the action requested.

Auditing - used to trace which clients accessed what, and in which way (does not provide protection but is useful).

1. **What do the terms plaintext and ciphertext refer to in the context of cryptography? How are these terms related?**

Plaintext: the original form of the message sent.

Ciphertext: encrypted form of the message sent.

Encryption and decryption are accomplished by using cryptographic methods parameterized by keys.

1. **A cryptosystem consists of three algorithms. What are these algorithms?**

• A cryptosystem consists of three algorithms:

• One for key generation.

• One for encryption.

• One for decryption.

1. **Describe how a symmetric (secret-key) cryptosystem works.**

In a symmetric (secret-key) cryptosystem, the same key is used to encrypt and decrypt a message:

P=Dk(Ek(P))

Recall, Ek denotes encryption with key K, Dk denotes decryption with key K and P denotes the plaintext. Sender and receiver required to share the same key and this shared key must be kept secret.

1. **Describe how an asymmetric (public-key) cryptosystem works.**

In an asymmetric (public-key) cryptosystem, the keys are different but form a unique pair:

P=Dkd (Eke(P))

Here key pair ke and kd are used for encryption and decryption respectively. One of the keys in an asymmetric cryptosystem is kept private; the other is made public. Which one of the encryption or decryption keys that is actually made public depends on how the keys are used.[1]

1. **What is the main difference between a symmetric (secret-key) cryptosystem and an asymmetric (public-key) cryptosystem?**

In a symmetric (secret-key) cryptosystem, the same key is used to encrypt and decrypt a

message. In an asymmetric (public-key) cryptosystem, the encryption and decryption keys are different but form a unique pair.

1. **How may one send a confidential message using an asymmetric (public-key) cryptosystem?**

Sending a confidential message using an asymmetric sryptosystem can be explained by an example as below:

If sender wants to send a confidential message to the other one, He uses the receiver’s public key to encrypt the message and the receiver is the only one holding the associated and private decryption key. Therefore, receiver is the only person that can decrypt the message.

1. **How may one perform message authentication using an asymmetric (public-key) cryptosystem?**

If a person wants to know for sure that the message he just received actually came from the sender. That is, perform message authentication. sender can keep his encryption key private to encrypt the messages he sends. If receiver can decrypt a message using sender’s public key the message must have come from sender, because the decryption key is uniquely tied to the encryption key.

1. **What is a digital signature?**

Digital signatures which maybe be implemented using a public key cryptosystems is uniquely tied to its content.

//TODO

1. **Provide a real world application of digital signatures.**

Digital signatures which maybe be implemented using a public key cryptosystems is uniquely tied to its content.

//TODO

1. **What is the purpose of access control?**

The purpose of access control is to prevent or control user or system that are not allowed from communicating and interacting. Access control manages access to computer systems, networks, Web servers, additional networks, and various other systems and devices. Access control protects the system from illegal access, and in most cases determines the appropriate level of authority for users or systems that have been confirmed by the identity authentication system.

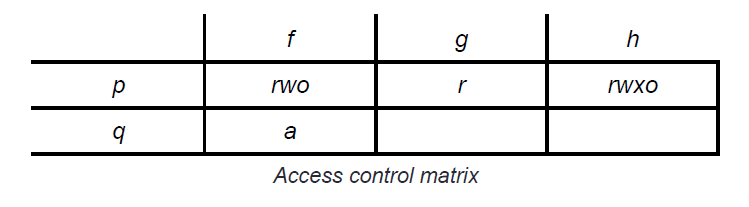
1. **What is the purpose of a reference monitor in the context of access control?**

The purpose of a reference monitor is recording which subject may do what. And deciding whether a subject is allowed to have a specific operation carried out.

1. **Explain how access control may be implemented using an access control matrix.**

Each subject is represented by a row in this matrix, and each object is represented by a column. Given a matrix M, the entry M[s,o] lists operations subject s can request to be carried out on object o. And many entries in the matrix will be empty; a single subject will have access to relatively few objects.[1]

For example, in this access control matrix:



p and q are subjects.

f, g and h are objects.

r, w, x, a, o are operations.

1. **Describe the purpose of a firewall in a distributed system**

The purpose of a firewall is acting as a reference monitor between a distributed system and other distributed systems. All messages are routed through the reference monitor

and inspected before they are passed through. Unauthorized traffic is discarded and not allowed to continue.

1. **Explain why mobile code introduces a number of security threats** **Describe a security mechanism which may be used to deal with such a threat.**

Mobile code poses many security threats because it is difficult for mobile code developers to control the environment in which their code runs, so it brings special security issues. One of the biggest threats is the risk that mobile code runs side by side with other potentially malicious mobile code, and those malicious code may corrupt its host. The solution is that we can execute code in a restricted environment called a sandbox, only in this way the malicious code cannot corrupt other area.