HTTPS (or TLS/SSL) uses PKI (public key infrastructure) and certificates to ensure security. A certificate contains an identity, a public key, and the signatures of CAs (certification authorities). Other fields that may be present include the organization (for example, university, company, or government) to which that identity belongs and perhaps suborganizations (college, department, program, branch, office).

1) Explain what security purpose these fields serve.

2) Describe two uses of certificates.

1. **Security Purposes of Certificate Fields:**
   * **Identity**: This field uniquely identifies the entity (user, organization, server, etc.) associated with the certificate. In security terms, it establishes the principle of 'authentication', ensuring that an entity is who it claims to be.
   * **Public Key**: The inclusion of a public key in the certificate is fundamental to the principle of 'confidentiality'. It enables secure communication, allowing others to encrypt messages that only the holder of the corresponding private key can decrypt.
   * **Signatures of Certification Authorities (CAs)**: The CA's signature underpins the 'trust model' in PKI. It assures that the binding between the public key and the entity's identity is verified and trustworthy. This is essential for maintaining the integrity and trustworthiness of communications in a network.
   * **Organizational Details**: These details (like the university, company, department, etc.) are crucial for 'authorization' and 'access control'.

They help in determining the scope and legitimacy of the certificate, outlining the entity's role or jurisdiction within a larger organization.

1. **Uses of Certificates:**

**1)Secure Web Communications**: In the context of HTTPS, certificates authenticate the identity of web servers, establishing a trust basis for secure, encrypted communications between a web server and a client (e.g., a browser). This process mitigates the risk of man-in-the-middle attacks and eavesdropping.

2)**Digital Signatures:** Certificates play a crucial role in the process of digitally signing documents or software. They provide a means to associate a public key with the identity of the signer, such as a software developer. When a developer signs their software, they use their private key to create a digital signature, which is unique to both the software and their private key. The corresponding public key, needed to verify this signature, is part of the developer's certificate. This certificate, issued by a trusted Certification Authority (CA), confirms the identity of the signer and the authenticity of the public key. Thus, when users receive the signed software along with the developer’s certificate, they can use the public key within the certificate to verify the digital signature. This verification process ensures that the software indeed originates from the stated developer and that its integrity has not been compromised since signing.

In this manner, certificates in a PKI setup play a pivotal role in ensuring the foundational security principles of authentication, confidentiality, integrity, and authorization in digital communications and transactions.

2) Below are four pairs of concepts/threats/tools. For each pair, define both terms and explain the relationship between them. Then describe how the two terms can be used together to achieve a common goal, for example, to harm or protect one or several security properties, or ensure privacy. Structure each of your answers with the headings “Definition”, “Relationship”, and “Description”. Your answers to each part should show your deep understanding of the concept. The definition

relationship and description should be described or explained with care; they must not just be copied from the book/documents. Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem.

1. Reference monitor and incomplete mediation

2. Access control and IDS (Intrusion Detection System)

3. TCB (Trusted Computing Base) and memory protection

4. Viruses and worms

**1. Reference Monitor and Incomplete Mediation**

**Definition**

* **Reference Monitor**: An abstract machine that mediates all access to objects by subjects, ensuring that these accesses are consistent with the defined security policy. It is characterized by being tamper-proof, always invoked, and small enough to be subject to analysis and tests, the completeness of which can be assured.
* **Incomplete Mediation**: A security vulnerability that occurs when a software system fails to consistently enforce security controls on every access to a protected resource or object.

**Relationship**

* The relationship between a reference monitor and incomplete mediation is foundational in system security. The reference monitor is designed to prevent incomplete mediation by ensuring that all accesses to a resource are checked for security policy compliance.

**Description**

* When implemented effectively, a reference monitor can significantly reduce the risk of incomplete mediation. It acts as a gatekeeper, ensuring that every access request to sensitive resources is verified for permissions. In contrast, incomplete mediation arises when parts of the system bypass this security check, potentially leading to unauthorized access. Therefore, ensuring a robust reference monitor is crucial to prevent security breaches due to incomplete mediation.

**2. Access Control and IDS (Intrusion Detection System)**

**Definition**

* **Access Control**: A method by which systems determine who can access resources, when they can access them, and what actions they can take on them.
* **Intrusion Detection System (IDS)**: A tool or software used to detect unauthorized access or anomalies in network traffic or computer systems.

**Relationship**

* Access control and IDS are complementary in protecting system security. Access control restricts access based on policies, while IDS monitors and analyzes for signs of violations or suspicious activities.

**Description**

* In combination, access control mechanisms and IDS can provide a more robust security posture. Access control proactively prevents unauthorized access, while IDS acts as a reactive measure to detect and alert on any breach attempts or policy violations. This dual-layered approach ensures not only preventive security measures but also active surveillance for potential security incidents.

**3. TCB (Trusted Computing Base) and Memory Protection**

**Definition**

* **Trusted Computing Base (TCB)**: The set of all hardware, software, and firmware components critical to a system's security, responsible for enforcing a security policy.
* **Memory Protection**: Techniques and mechanisms to control access to memory in a computer system, aimed at preventing unauthorized processes from accessing or altering memory spaces allocated to other processes.

**Relationship**

* TCB relies on memory protection as a foundational element to ensure its integrity and secure operation. Memory protection is crucial for isolating sensitive parts of the TCB from unauthorized access or modification.

**Description**

* In a secure system, the TCB utilizes memory protection to safeguard its critical components. Effective memory protection mechanisms ensure that the TCB operates in a secure and isolated environment, free from external interference or tampering. This relationship underscores the importance of maintaining the integrity of the TCB to uphold system security.

**4. Viruses and Worms**

**Definition**

* **Viruses**: Malicious software that requires user intervention to replicate and spread, often attaching itself to a file or document.
* **Worms**: Standalone malicious software that replicates itself and spreads across networks without requiring user intervention or attaching to a specific file.

**Relationship**

* Viruses and worms are related in their methods of propagation and the harm they cause. Both are types of malware but differ in how they spread: viruses require human action, while worms are more autonomous.

**Description**

* In a malicious context, viruses and worms can be used to compromise system security, steal data, or cause system damage. Viruses might be spread through infected files shared by users, while worms can exploit network vulnerabilities to spread rapidly. Understanding these threats is key to developing effective security measures, such as antivirus software and network security protocols, to detect and mitigate their impact.

Compare and contrast symmetric and asymmetric encryption. Discuss the advantages and disadvantages of symmetric and asymmetric encryption methods when securing web services.

Symmetric encryption

The idea behind symmetric encryption is that, in contrast with asymmetric encryption, the same cryptographic key is used to both encrypt and decrypt a message. To do that, both parties in an exchange need to share a key. Since it should remain secret, it also acts as an authentication method. Advantages - fast and easy to compute.

Disadvantages - key distribution - a new key is required for every new pair of users, which may introduce problems when keeping track of many keys - limited, algorithm dependant lenght, which may limit the possibilities of developing new algorithms (which might be needed in the future, computing power keeps growing which might eventually lead to current secure encryption algorithms being broken in the future) - requires a secure way to share the key with the receiver without compromising its secrecy Asymetric encryption When it comes to assymetric encryption, a pair of mathematically related keys is generated. One of them serves as the public key, and the other as the private key, to be kept secret from everyone else. Either of them can serve any of the two possible roles, but once it has been decided, which one is public and which one is private needs to remain unchanged - doing otherwise would compromise the secrecy of the encryption process. Assymetric encryption be used for both confidentiality and integrity checks, depending on which key is used to encrypt the messege. When confidentiality is the priority, the sender uses the public key of the recipient to encrypt the messege and the recipient uses their private key (which, presmebly, only they have access to to decrypt it. However, if we want to ensure the integrity and verify that it was indeed the sender who has sent the messege, sender A would use their private key to encrypt the messege and recipient B would use A's public key to decrypt it, thus verifying that it has indeed come from A. This technique is used in digital signatures. Advantages -solves the key distribution problem posed by symmetric encryption (public key can be shared freely) - unlimited lenght (the longer the key, the harder it is to break) Disadvantages - requires a working public key infrastructure - requires a trusted directory service Both types of encryption are often used in combination to establish trust when two parties want to exchange their public keys in a secure manner - they are exchanged via assymetric encryption and after that the communication continues with the use of shared private keys.