EBU7140

Tutorial 3

2020_21

1) What is a replay attack?

- It is when an attacker re-uses a valid sequence of data in order to access a particular service.

2) What is Kerberos? What does it provide?

- Kerberos is a centralised authentication service designed for use in a distributed environment.
- It makes use of a trusted third-party authentication service that enables clients and servers to establish authenticated communication. Also, it provides access control.

3) A simple way for a server to authenticate a client is to ask for a password. In Kerberos this authentication is not used, why? How does Kerberos authenticate the server and the clients?

- The main security weakness is that the password is transmitted. So anybody eavesdropping can get hold of it.
- A better way is: the client request from the server a “service granting ticket”. The client sends the request for using the server, and the user’s ID. The server, which knows the users password, creates a session key using the user’s password. Using this session key, the server sends the ticket granting a service. The client asks the user for his/her password, generates the session key and recovers the ticket. The password is never transmitted between server-client.

4) What are the four requirements for Kerberos? What mechanisms are used within Kerberos systems to achieve those requirements?

Requirement	Mechanism
Secure	Provided by the secure steps, mostly achieved by using conventional encryption. AUTHENTICATION is an alternative answer.
Reliable	Distributed architecture. Uses mirrored system backups.
Transparent	Limitation of user interaction to the authentication with the client (password, or other methods).
Scalable	Principle of Kerberos realms.

5) What is a public-key certificate?

It is used to authenticate public-keys of users.

A public-key certificate contains a public key, an identifier of the key owner and other information, is signed and acreated by a certificate authority, and is given to the participant. A participant conveys its key information to another by transmitting its certificate. Other participants can verify that the certificate was created by the authority.

6) Define the X.509 standard. How is an X.509 certificate revoked?

- X.509 defines a framework for the provision of authentication services by the X.500 directory to its users.
- The directory may serve as a repository of public-key certificates.
- the public key of a user and is signed with the private key of a trusted certification authority.
- In addition, X.509 defines alternative authentication protocols based on the use of public-key certificates.

- Each CA must maintain a certificate revocation list (CRL) consisting of all revoked certificates issued by that CA.
- The list is signed by the issuer and includes the issuer's name, the date the list was created, the date the next CRL is scheduled to be issued, and an entry for each revoked certificate. Each entry consists of the serial number of a certificate and revocation date for that certificate.
- The user could check the CRL list each time a certificate is received to determine the certificate is not revoked.

7) What is IPsec? Why is it significant?

- IPSec stands for IPSecurity as it protects IP packets
- It is vital for providing additional security at the IP layer, and protect security-ignorant applications
- It provides: confidentiality, authentication, or both for IP packets.

7) What are the two modes of operations in IPsec? How can they achieve protection against traffic analysis?

- Tunnel Mode: protects entire packet.
- Transport Mode: protects payload.

ESP provides protection against traffic analysis.

* In tunnel mode ESP provides protection against traffic analysis where the host on the internet networks use the Internet transport of data but do not interact with other Internet-based hosts.

* In Transport Mode, ESP only protects the payload, hence the IP header will not be hidden (limited protection against traffic analysis).

9) List the services provided by IPSec.

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
- Confidentiality (encryption)
- Limited traffic flow confidentiality

10) In IPSec, what is the domain of interpretation (DOI)?

- Contains values to relate the different specifications of the protocol;
- identifiers for encryption and authentication algorithms
- and operational parameters, key lifetimes, key exchange etc.

11) In IPSec, what is the difference between transport mode and tunnel mode?

- Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet.

- Tunnel mode provides protection to the entire IP packet.

12) What are the parameters used to characterise the nature of a particular SA?

- Sequence Number Counter.
- equence Counter Overflow.
- Anti-Replay Window.
- AH Information.
- ESP Information.
- Lifetime of this Security Association.
- IPSec Protocol Mode.
- Path MTU.

13) What are the roles of the Oakley key determination protocol and ISAKMP in IPsec?

ISAKMP by itself does not dictate a specific key exchange algorithm; rather, ISAKMP consists of a set of message types that enable the use of a variety of key exchange algorithms. Oakley is the specific key exchange algorithm mandated for use with the initial version of ISAKMP.