

Write a report on the following topics:-

1.) Certificates:-

- Certificates are the building blocks of PKIs, & they ultimately enable secure & scalable PKIs to be built from them. A certificate binds an identity to a public key. This is usually done by having a trusted authority (i.e. a certification authority, denoted as CA) sign the information on a certificate, it is generally assumed that everyone has access to an authentic copy of the public key of the CA. Hence, a CA's signature on a certificate can be verified, which allows the information on the certificate to be authenticated.

2.) X.509 Version 3 :-

- X.509 is an international telecommunication union standard defining the format of public key certificates. X.509 certificates are used in many internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing web. They are also used in offline applications like electronic signatures.

X.509 version 3 certificate was released in 1996 & defines the formatting used for certificate extensions. It also was used by the internet engineering task force in the development of its own X.509 public key infrastructure certificate & certification revocation list or CRL.

X.509 certificates contain the following fields:-

- i.) version number
- ii.) Serial number
- iii.) Signature algorithm ID
- iv.) Issuer name
- v.) validity period
- vi.) Subject name (i.e. the certificate owner)
- vii.) the certificate owner's public key
- viii.) optional fields
- ix.) the CA's signature on all the previous fields.

3.) Distribution of symmetric key using Asymmetric Encryption:-

- The distribution of a symmetric key using asymmetric encryption involves using a pair of keys: a public key & a private key.

i.) Key generation:-

The recipient generates a pair of keys: a public key & a private key. The private key is kept secret while the public key is shared with anyone.

ii.) Symmetric key generation:-

The sender generates a random symmetric key. This key will be used to encrypt the actual data.

iii.) Encryption of symmetric key:-

The sender encrypts the symmetric key using the recipient's public key. Asymmetric key is used

here. Since, public key is available to anyone, the sender can securely encrypt the symmetric key.

iv.) Sending the encrypted key & data:-

The sender then sends the recipient two items: the data encrypted with the symmetric key & the symmetric key itself encrypted with the recipient's public key.

v.) Decryption by the recipient:-

- The recipient first uses their private key to decrypt the encrypted symmetric key. This step ensures that only the recipient can access the symmetric key.
- The recipient use the decrypted symmetric key to decrypt the actual data.

A.) Distribution of public keys:-

- The distribution of public keys is a critical aspect of ensuring secure communication & authentication. There are several methods & systems designed to facilitate the distribution of public keys.

1.) Public Key Infrastructure (PKI):-

- Certification Authorities (CAs):- PKI relies on trusted third-party organizations called certification authorities to issue digital certificates. These certificates verify the ownership of public keys.
- Certificate Hierarchies:- CAs operates on hierarchical structure, with root CAs delegating trust to intermediate CAs.

- Certificate Revocation :- mechanisms like certificate Revocation lists & online certificate status protocol are used to manage revoked certificates.

11) Web Trust :-

- user based trust :- Users sign each other's public key, building a network of trust relationships.
- Key signing parties :- These are events where users physically meet to verify each other's identities & sign public keys.
- Decentralized approach :- Unlike PKI, the web of trust does not rely on a central authority but rather on the collective trust of the community.

111) Key Servers :-

- public repositories :- Users ^{upload} their public keys to key servers, which are public repositories accessible over the internet.
- Synchronization :- Key servers often synchronize with each other to ensure that public keys are widely available.
- Searchable :- Users can search for public keys by email address or other identities.

12) Manual distribution :-

- Direct exchange :- Public keys can be exchanged directly between parties, such as through email, physical media or secure messaging apps.

- QR codes:- Public keys ~~are~~ can be encoded in QR codes for easy scanning & sharing.
- Print:- Sometimes public keys are printed in physical form & distributed in person.

S> Public Key Infrastructure & Trust models:-

- Public Key Infrastructure (PKI) is a comprehensive framework used to manage digital keys & certificates, ensuring secure & trusted communications in a cryptographic system. Trust models withⁱⁿ PKI play a crucial role in establishing & managing trust relationships.

Components of PKI:-

i> Certificate Authority (CA):-

- Central to PKI, a CA issues digital certificates to validate the ownership of public keys.
- Root CAs are the top of the hierarchy & can delegate trust to intermediate CAs.

ii> ~~Regulation~~ Registration Authority (RA):-

Acts as a verifier for the CA before a certificate is issued, ensuring that the entity requesting a certificate is legitimate.

iii> Digital certificates:-

- Bind public keys to the identities of their owners, including information such as the owner's name, the public key, the CA's signature, & the certificate's validity period.

iv.) Certificate Revocation lists (CRLs) & online certificate status protocol (ocsp):-

- mechanisms to manage & disseminate information about revoked certificates.

v.) Key management systems:-

- Systems for generating, storing, distributing & managing cryptographic keys & certificates.

Trust models:-

i.) Hierarchical Trust model (Tree model):-

- Organized in a tree like structure with single root CA at the top.
- Trust is hierarchical & propagates down from the root CA to subordinate CAs.

ii.) Web of Trust model:-

- Decentralized model where trust is established through mutual endorsements by users.
- Users sign each other's public keys, creating a network of trust relationships.

iii.) Bridge CA Model:-

- Acts as a central point to connect multiple root CAs.
- Facilitates interoperability between different PKIs by creating trust relationship among them.

iv.) Mesh Trust model:-

- Every CA trust every other CA directly without a

central authority.

- Trust is fully distributed among CAs. //