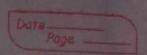
Raju Shrestha Roll No. 48



Write a report on the following topics:-

Certificates are the building blocks of PKIs, & they ultimately enable secure a scalable pKEs 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 (A) 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 a 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 a certification revocation 18st or CRI.

X.509 certificates contain the following fields:-

1) version number 11) Serial number 111) Signature algorithm ID 1v.) Issuer name v) validity period vi) Subject name (i.e. the certificate owner) vii) the certificate oconer's public key viil 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 e a private key. 1) key generation: The recepient generates a pair of keys: a public key a a private key. The private key is kept secret while the public key be shared with anyone. 11) Symmetric key generation: The sender generates a random symmetric key. This key will be used to encrypt the actual data. 111) Encryption of symmetric key! The sender encrypts the symmetric key using the recepient'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 a 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 lensures that only the recipient can access the a 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 a systems designed to facilitate the distribu - tion 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 oconership of public keys. centificate Hierarchies: - cas operates on hierarchial structure, with noot cas delegating trust to intermediate

Certificate Revocation: - Mechanisms like certificate Revocation lists & online certificate status protocol are used to manye revoked certificates. 11) Web Trust: ciser based trust: - User's 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 pks, 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 load their public keys to key servers, which are public repositories accessible over the internet. · Synchronization: - key servers often synchronize with leach other to ensure that public keys are coulddy available. · Searchable: - Users can search for public keys by email address or other identities. In manual distribution: · Pirect exchange: Public keye 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 AR codes for easy scanning of sharing. Print: - Sometimes public keys are printed in physical form & distributed in person. 5) Public Key Infrastructure of 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 with PKI play a crucial role in establishing & managing trust relationships. components of PKI: (cartificate Authority (cA):-Central to PKI, la CA issues digital certificates to validate the ownership of public keys. Root cas are the top of the hierarchy & can deligate trust to intermediate (As. 11) Regulation Registration Authority (RA) :-Acts as a verifier for the CA before a certificate is issued, ensuring that the entity requesting a certificate for legitimate. in Digital certificates: - Bind public keys to the identities of their owners, including information such as the oconer's name, the public key, the ca's signature, & the certificate's validity period.

14) 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 a managing cryptographic keys a certificates. Trust models: 1) Hierarchial Trust model (Tree model):-Organized in a tree like structure with single most cA at the - Trust is hierarchial & propagates down from the root (A to subordinate CAS. 11) Web of Trust model: - Decentralized model where trust is established through mutual endorgements by cusers. Users sign each other's public keys, creating a network of trust relationships. 111) Bridge CA Model: - Acts as a central point to connect multiple mot CAs. - facilitates interoperability between different pass be creating trust relationship among them. Ivy Mesh must model: Every ca trust every other ca directly without a



