Armaan Shamsaasef

Public Key Infrastructure (PKI)

Notes: Public Key Infrastructure (PKI) (SY0-701 - 1.4)

Core Concept: Public Key Infrastructure (PKI) is the entire system of hardware, software, policies, and standards used to create, manage, distribute, use, store, and revoke digital certificates. It enables secure communication by binding public keys with respective user identities.

Key Components of PKI

1. Certificate Authority (CA)

- **Definition**: A trusted third-party entity that issues and signs digital certificates.
- **Role**: The root of trust for the entire PKI system. It verifies the identity of an entity (a person or device) and then vouch for them by issuing a certificate.
- Example: Global CAs like DigiCert, Let's Encrypt, or a company's own internal CA.

2. Digital Certificate

- **Definition**: An electronic document that uses a digital signature to bind a public key with an identity (e.g., a website's URL, a person's name, or a device).
- **Contents**: Contains information like the owner's name, the public key, the issuing CA, a serial number, and expiration dates.
- **Purpose**: To provide proof of identity and ownership of a public key.

3. Registration Authority (RA)

- **Definition**: A subordinate entity that handles the verification of certificate requests on behalf of the CA.
- **Role**: The RA is the "front office" that accepts requests, verifies the applicant's identity, and then tells the CA to issue the certificate. The CA itself is the "back office" that performs the actual signing.

4. Certificate Revocation

- **Purpose**: To invalidate a certificate *before* its natural expiration date.
- Why Revoke? The private key is compromised, an employee leaves the company, or a device is retired.
- Methods:
    - Certificate Revocation List (CRL): A list, published by the CA, of all certificates that have been revoked. Clients must check this list.
    - Online Certificate Status Protocol (OCSP): A real-time protocol that allows a client to query the CA about the status of a single specific certificate ("Is this certificate valid?").

The PKI Process in Action

Example: Securing a Website with HTTPS

1. **Request**: The website owner generates a public/private key pair and submits a Certificate Signing Request (CSR) to a CA.
2. **Verification**: The CA (and its RA) verifies that the requester actually owns the domain name.
3. **Issuance**: The CA creates a digital certificate for the website, binds the website's public key to its domain name, and signs the certificate with the CA's own private key.
4. **Trust**: Your web browser trusts the CA. It comes pre-loaded with the public keys of major CAs.
5. **Validation**: When you connect to the website, it presents its certificate. Your browser uses the CA's public key to verify the CA's signature on the certificate. If valid, it establishes a secure TLS connection.

Key Concepts

- **Chain of Trust**: A hierarchy where a root CA signs intermediate CAs, and intermediate CAs sign end-entity certificates. This allows the root CA to remain offline and highly protected.

- **Key Escrow**: A process where a copy of a private key is stored with a trusted third party. This is typically used for recovery purposes (e.g., if an employee leaves and encrypted data needs to be accessed).

Key Takeaway

PKI is the foundation for trust and security on the internet. It enables critical services like:

- Encryption (for confidentiality)
- Digital Signatures (for integrity and non-repudiation)
- Authentication (verifying the identity of websites, users, and devices)

Without PKI, secure e-commerce, online banking, and private communication would not be possible.