Sanjivani Rural Education Society's

Sanjivani College of Engineering, Kopargaon-423603

(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

NAAC 'A' Grade Accredited, ISO 9001:2015 Certified

Department of Information Technology

(NBA Accredited)

Cryptography and Cyber Security [IT311]

Mrs. Kanchan D. Patil

Assistant Professor

Unit 3: Message Digest & Key Management

- Hash Algorithms: SHA-1, MD5, Key Management: Introduction, Key Management: Generations, Distribution, Updation, Digital Certificate, Digital Signature, Kerberos 5.0.

Key Management

- Public Key Management
  - Refer Unit 2 PPTs
- Private Key Management

Private Key Management

- In many situations, The private key of the user required to be transported from one location to another.
- The cryptographic standard name PKCS#12 allows user to export digital certificate and private key in the form of a computer file.
- The certificate and private key must be protected.
- PKCS#12 standard ensures that they are encrypted using a symmetric key.

Private Key Management

- **Multiple Key pairs**

- Users can process multiple digital certificates in various applications which is also called as multiple key pairs
- The need is
  - One can be used for signing
  - Another can be used for encryption
- This ensures that the loss of one of the private keys does not affect the complete operations of the user.

Multiple Key Pair Guidelines

- **Guideline 1:**
  - The private key used for signing must not be backed up or achieved after it expires.
  - It must be destroyed.
  - This ensures that this will not be used by someone else on behalf of the person in future

- **Guideline 2:**
  - In contrast, the private key used for encryption/decryption must be backed up after its expiry so that encrypted information can be recoved later

Key Update

- Key pairs must be updated periodically because over the time keys become susceptible to cryptanalysis attacks.
- The key update process can be handled as follows:
  - The end user has to detect that the certificate about to expire and request the CA to issue a new one
  - The expiry date of the certificate is automatically checked by every time it is used and as soon as it is about to expire, its renewal request is sent to the CA.

Mechanisms to protect Private Key

- **Password Protection**
  - This is the simplest and most common mechanism to protect a private key
  - The private key is **stored on the hard disk** of the user's computer as a disk file.
  - This file can be accessed only with the help of a **password or a Personal Identification Number (PIN).**
  - Since anyone who can guess the password correctly can access the private key, this is considered as the **least secure method** of protecting a private key.

Mechanisms to protect Private Key

- **PCM/CIA Cards**
  - The Personal Computer Memory Card International Association (PCMCIA) cards are actually **chip cards.**
  - The private key is stored on such a card, which means that it need not be on the user's hard disk.
  - **This reduces the chances of it being stolen.**
  - However, for a cryptographic application such as signing or encryption, the key must travel from the PCMCIA card to the memory of the user's computer.
  - Therefore, there is still scope for it being captured from there by an attacker.

Mechanisms to protect Private Key

- **Tokens**
  - A token stores the private key in an **encrypted format.**
  - To decrypt and access it, the user must provide a one-time password We
  - This is a **more secure** method.

- **Biometrics**
  - The private key is associated with a **unique characteristic of an individual** (such as fingerprint, retina scan or voice comparison).
  - This is similar in concept to the tokens, but here the user need not carry anything with him, unlike the token.

Mechanisms to protect Private Key

- **Smart Cards**
  - In a smart card, the private key of the user is stored in a tamperproof card
  - This card also contains a computer chip, which can perform cryptographic functions such as signing and encryption.
  - The biggest benefit of this scheme is that the **private key never leaves the smart card.**
  - Thus, the scope for its compromise is tremendously reduced.
  - The **disadvantage** of this scheme is that the **user needs to carry the smart card** with her and **compatible smart card readers must be available** to access it.

References:

- Atul Kahate,”Cryptography and Network Security”, second edition, Tata McGraw Hill