SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE NAME : 19EC625 – CYBER FORENSIC AND DATA SECURITY

III YEAR / VI SEMESTER

Unit I- NETWORK LAYER SECURITY &TRANSPORT LAYER SECURITY

Topic : Key Management Protocol for IPSec

Introduction

- Key management refers to the processes and procedures involved in generating, storing, distributing, and managing cryptographic keys used in cryptographic algorithms to protect sensitive data. It ensures that keys used to protect sensitive data are kept safe from unauthorized access or loss. Good key management helps maintain the security of encrypted information and is important for protecting digital assets from cyber threats.

How Cryptographic Keys Works?

•Cryptographic keys are special codes that protect information by locking (encrypting) and unlocking (decrypting) it.

•In **symmetric key cryptography**, a single shared key does both jobs, so the same key must be kept secret between users.

•In **asymmetric key cryptography**, there are two keys: a public key that anyone can use to encrypt messages or verify signatures, and a private key that only the owner uses to decrypt messages or create signatures.

Types of Key Management

There are two aspects of Key Management:

Distribution of public keys.

Use of public-key encryption to distribute secrets.

Distribution of Public Key

The public key can be distributed in four ways:

- Public announcement
- Publicly available directory
- Public-key authority
- Public-key certificates.

Key Management

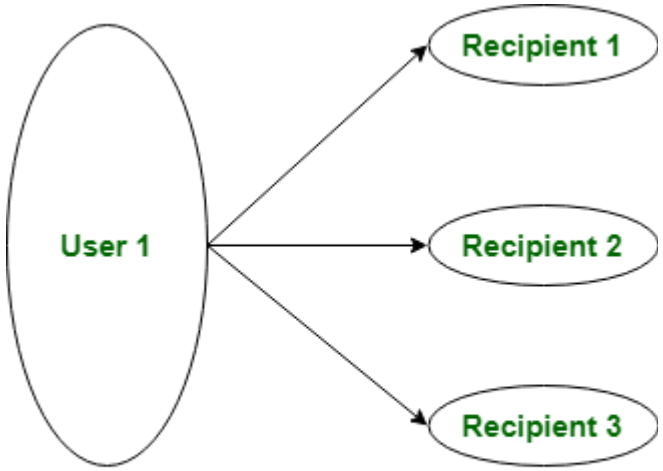
1. **Public Announcement:** Here the public key is broadcast to everyone. The major weakness of this method is a forgery. Anyone can create a key claiming to be someone else and broadcast it. Until forgery is discovered can masquerade as claimed user.

2. Publicly Available Directory: In this type, the public key is stored in a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like {name, public-key}. Directories can be accessed electronically still vulnerable to forgery or tampering.

3. Public Key Authority: It is similar to the directory but, improves security by tightening control over the distribution of keys from the directory. It requires users to know the public key for the directory. Whenever the keys are needed, real-time access to the directory is made by the user to obtain any desired public key securely.

4. Public Certification: This time authority provides a certificate (which binds an identity to the public key) to allow key exchange without real-time access to the public authority each time. The certificate is accompanied by some other info such as period of validity, rights of use, etc. All of this content is signed by the private key of the certificate authority and it can be verified by anyone possessing the authority's public key.

First sender and receiver both request CA for a certificate which contains a public key and other information and then they can exchange these certificates and can start communication.



Public Key Announcement

Key Management Lifecycle

The **key management lifecycle** outlines the stages through which cryptographic keys are generated, used, and eventually retired or destroyed. Proper management of these keys is critical to ensuring the security of cryptographic systems. Here's an overview of each stage:

1. Key Generation:

Creation: Keys are created using secure algorithms to ensure randomness and strength.

Initialization: Keys are initialized with specific parameters required for their intended use (e.g., length, algorithm).

2. Key Distribution:

Sharing: For symmetric keys, secure methods must be used to share the key between parties.

Publication: For asymmetric keys, the public key is shared openly, while the private key remains confidential.

3. Key Storage:

Protection: Keys must be stored securely, typically in hardware security modules (HSMs) or encrypted key stores, to prevent unauthorized access.

Access Control: Only authorized users or systems should be able to access keys.

4. Key Usage:

Application: Keys are used for their intended cryptographic functions, such as encrypting/decrypting data or signing/verifying messages.

Monitoring: Usage is monitored to detect any unusual or unauthorized activities.

Key Management Lifecycle

5. Key Rotation:
Updating: Keys are periodically updated to reduce the risk of exposure or compromise.
Re-Keying: New keys are generated and distributed, replacing old ones while ensuring continuity of service.
6. Key Revocation:
Invalidation: Keys that are no longer secure or needed are invalidated.
Revocation Notices: For public keys, revocation certificates or notices are distributed to inform others that the key should no longer be trusted.
7. Key Archival:
Storage: Old keys are securely archived for future reference or compliance purposes.
Access Restrictions: Archived keys are kept in a secure location with restricted access.
8. Key Destruction:
Erasure: When keys are no longer needed, they are securely destroyed to prevent any possibility of recovery.
Verification: The destruction process is verified to ensure that no copies remain.

Any Query????

Thank you……