Cryptography Concepts

Plain Text >> Encryption Algorithm >> Cipher Text

Two Type Of Encryption Algorithms

1. Symmetric Algorithm
    Data Encryption Standard (DES)
    - Key size 56 bit
    Triple DES
    Advanced Encryption Standard (AES) - key size 128 bits
    Hash Algorithm
    Md5 - Hash Length 128 bit
    SHA - Hash Length 160 bit SHA-2 Hash Length 224,256,384,512
    RIPEMD ..... Hash Length 128, 160, 256, 320 with one key
    only one key is used for encrypting and decryption
2. Asymmetric Algorithm
    Digital Signature With Public and Private key
    Used two keys for encryption and decryption
    Example: RSA - (Rivest-Shamir-Adleman)

(Public Key for Decryption and Private Key for Encryption)
    key size - 1024,2048,3072,4096 .. ..

Digital Certificates are generated by ROOT CA and Intermediate CA

- also include private in ROOT Server, public and hash algorithm, Details of Key Owner
- Generated by Third Party Certificate Authority Repo Server.

Certificate Authority
    - generate, issue and distribute public key certificates.
    - Distribute CA Certificates.
    - Generate and publish certificate status information
    - Revoke public key certificates.

Certificates must include Name, Public key, Name of issuer, Digital Signature of issuer, Serial Number, and Expiration Date.

Registration CA <<>> Intermediate CA <<>> ROOT CA (always offline for seCX purpose)
---------- publicity accessible Database storing CA Entities store in ----------

Certification Revocation List (CRL)
- Certificate no longer used
- Details of the certificates have changed
- Private key has been lost or stolen

Online Certification Status Protocol (OCSP)

- To check the certification status

Domain Digital Certificates (Web Server)

1. To ensure the authenticity of the web server is right.
2. To ensure the cryptography and secure

- Domain Validation,
- Extended Validation (legal or illegal)
- Wild Card Validation - Main Domain, Sub Domains Validation
Example: (*.blabla.com) * = app, www, mm, etc...
- Subject Alternative Name (SAN)

Hardware & Software Digital Certificates

- Machine digital certificates (Printer, Network Card, etc..
- Code Signing Digital Certificates. (Software Dev to prove the programs come from Authorize Entities)
- Email Digital Certificates

Public Key Infrastructure (PKI)

One CA Holder can't handle all of CA
A framework for all entities involved in digital certificates Authority.

In PKI, We have trust models.

Hierarchical Trust Model
Distributed Trust Model
Bridge Trust Model

Certificate Policy

- Operation of PKI
- Baseline Security Requirement
- CA obligations
- Users obligations

Life Cycle

- Creation
- Suspension
- Revocation
- Expiration

----------Finished part of Asymmetric Algorithm ----------

Diffie-Hellman Key Exchange

Diffie-Hellman is an algorithm for key exchange

_0_ User Alice
0

^

SSL/TLS Protocol Explain

Secure Socket Layer, Transport Layer Security.
SSL V3 is basic of TLS V1. Example: Https

SSL Communication Between Client & Server.

Client >> SSL Protocol Version, Random, Session ID, Cipher Suite, Compression Method >> Server

Diffie - Hellman Algorithms is just symmetric algorithms for key exchange

RSA and SSH Protocol
