Public Key Infrastructure

VE475 Project 1 Group

Zhang Leyang
Xu Jiaweng
Lu Mingxuan

2021.7.22

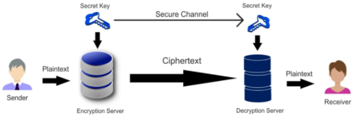
Outline

1. Introduction of Public-key Cryptosystem
   - Cryptosystem
     - Traditional and Public Cryptosytstem
   - RSA Method
2. Public-key Infrastructure
   - Basics
   - Structures of PKI
     - Flat Hierarchical Trust Model
     - Meshed Trust Model
3. Application and Future
   - Applications
   - Future Development

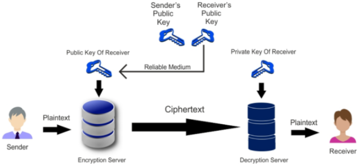
1.1 Cryptosystem

Cryptosystem:
A cryptosystem is a structure relying on general algorithms which are applied to particular randomly chosen parameters known as keys.

Traditional Public Cryptosystem:



Traditional



Public Cryptosystem

1.1.1 Traditional and Public Cryptosytstem

Traditional Cryptosytstem

Pros:

- Well-understood and lots of experience; security guaranteed.
- Computationally simple; Efficient, easy to implement.

Cons:

- Hard to maintain the keys secret
- large amount of key space

Public-Key Cryptosytstem

- Encryption key is public, open to everyone to generate
- Decryption key generated by the receiver, no need for transportation.

1.2 RSA Method

Key Generation

- Generate 2 large primes p and q. Let $n = pq$.
- Choose some e that has a multiplicative inverse d in the ring $\mathbb{Z}_n$.
  - Public Key: n, e
  - Private Key: d

Encryption

- $c = m^e \pmod{n}$.

Decryption

- $m = c^d \pmod{n}$.

2.1 Basics

Public-key Infrastructure
The public-key infrastructure, often abbreviated as *PKI*, consists of hardware or software elements that a trusted authority can use to verify the identities of the sender and the receiver.

Certification Authority
The trusted authority is often called certification authority (abbreviated CA) who confirms the identity of the sender and the receiver by issuing signed binary certificates.

2.1 Basics

Communication goes as follows:

(a) Alice requests a public key certificate from the CA.

(b) The CA verifies Alice's identity, computes a certificate consisting of hash of the content, signs the hash with k_2 in the published CA certificate, creates a new certificate by concatenating the certificate content and the signed hash, and makes the new certificate publicly available.

(c) The CA sends the certificate to Bob.

(d) Bob gets the certificate, decrypts the signed hash with k_1, computes a new hash of the certificate content, and compares the two hashes. If the hashes match, Bob can be sure that the message is indeed sent by Alice.

(e) Bob uses Alice's verified public key to encrypt a message to her.

(f) Alice uses her private key to decrypt the message from Bob.

2.2 Structures of PKI

There are several structuares of PKI:

- Hierarchical Trust Model
  - Flat Hierarchical Trust Model
  - Tiered Hierarchical Trust Model
- Meshed Trust Model

2.2.1 Flat Hierarchical Trust Model

The *flat hierarchical trust model* consists of a single CA, which issues certificates for multiple clients (senders and receivers). This kind of model is easy to supervise and manage, but any failure of the single CA would damage the whole system.

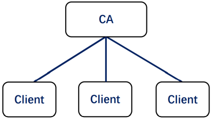


Figure 1: Example of flat hierarchical trust model

2.2.2 Tiered Hierarchical Trust Model

The *tiered hierarchical trust model* consists of multiple layers of CAs; usually there is one root CA, each middle layer CA(s) sign certifications of its children CAs and the CAs on the last level sign certifications.

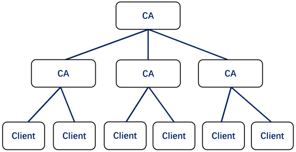


Figure 2: Example of flat hierarchical trust model

2.2.3 Meshed Trust Model

Another type of trust model is the *meshed trust model*. In this model, the client trusts the CA that issued their own certificate(s). The CAs have peer relationships and are subordinate to each other. Due to the multiple supervision, the structure is likely to be more secure than the ones above.

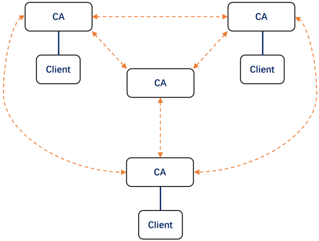


Figure 3: Example of meshed trust model

3.1.1 VPN

The IPSec protocol based on KPI technology has now become the basis for architected VPNs that can provide encrypted and authenticated communication between routers, firewalls, or between firewalls and routers.

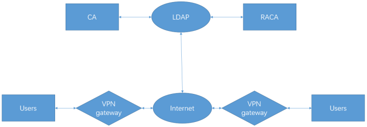


Figure 4: Illustration of procedures of VPN communication

3.1.2 Digital Notarization

The **time stamp** and **digital receipt** of the detailed report or document can not be modified by the submitter.
The **data** and **information** preserved by notarization has the legal evidential effect.

3.1.3 Code Signing

To solve the risk of software being imitated and tampered.
The software developer signs the software with the code signature certificate and puts it on the network. When the user downloads the software from the network, he will be prompted to make sure that the legitimate registered software is being used.

3.2 Future Development

Biometric Identification The introduction of biometric identification technology into KPI system will improve the development of KPI qualitatively.

Application in Wireless Communication Wireless communication, mobile commerce and so on all need security means, especially in the foreseeable future, the increase of wireless communication bandwidth and the improvement of mobile device performance

Thank you!