Cryptology part 2 Keränen /Teeriaho (Ramk 2006)

11 Public key infrastructure PKI

Using public key cryptosystems for digital signatures and authentication requires an infrastructure, called *public key infrastructure (PKI)* with specialized key servers and standardisized procedures ,which are describes in the following.

1. Public key systems are not largely used for encryption, but they are needed for digital signatures (RSA) and key agreement (DH)

2. Public key are certified
   - certificate tells the owner of the public key
   - certificates cannot be forged, because they are digitally signed by the certificating authority
   - certificates are given by certification authorities (CA)
   - CA's form hierarchical structures

3. Certificates are kept distributedly

4. The public keys of root CA's are delivered manually

5. Certification Revocal List (CRL) is needed to prevent usage of outdated certificates

6. CA is sometimes called also TTP = Trusted Third Party

Why are certificates needed ?

When Alice wants to send an encrypted message to Bob, she has to get Bob's public key.
* Alice can phone Bob and ask for his key.

* Bob can send his trustee Tim to deliver the key to Alice

* Bob could send the key to Alice by email. This is risky, because of a possible Man In The Middle attack, where a third person may capture the message and alter it.

* Alice and Bob can save their keys to a public key server. This is also risky because of a Man In The Middle attack. Someone can pretending to be Bob send the server a false public key.

Key server system CA is however the best solution is some safety measures are taken:

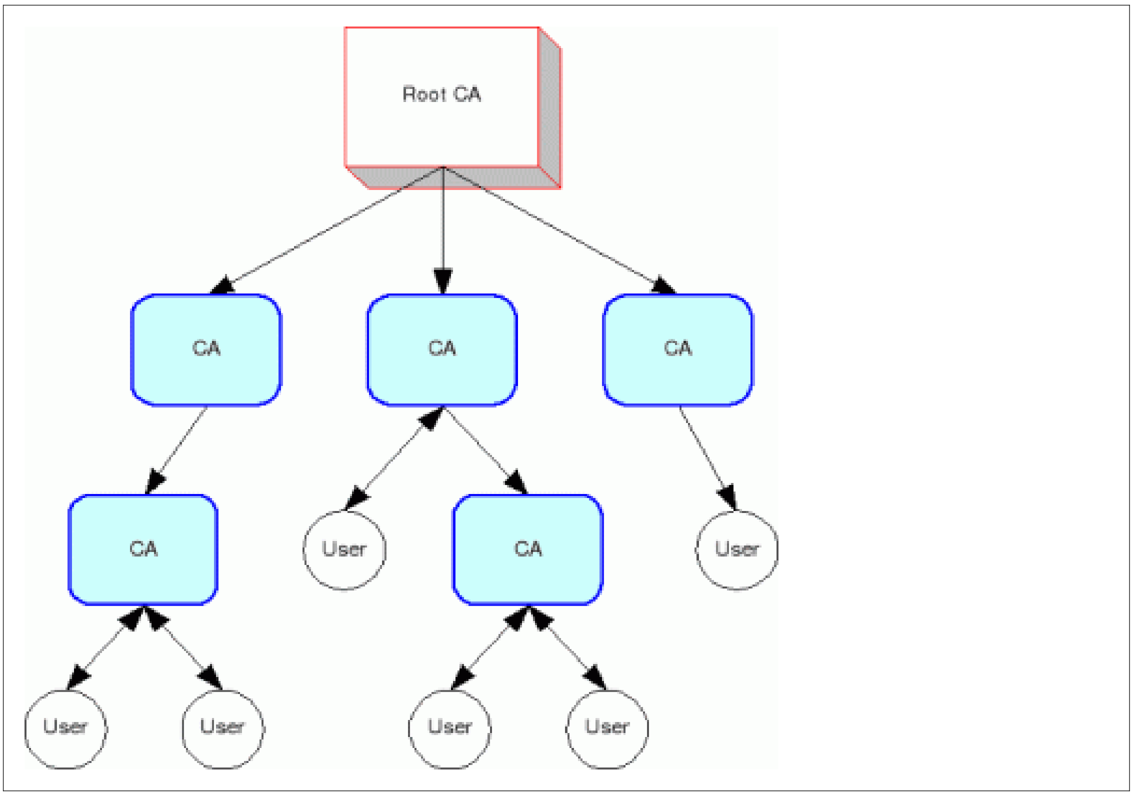
* Server should be maintained by 100% reliable party (bank, governement administration,...)

* Server should use storng public encryption when answering the requests of public keys.

* Server should send the public key in a specified standard format provided with the CA's digital signature.
CA's public key is delivered to all users manually.

Standard X.509 certificate includes
* certificate version
* certificate serial number
* CA:s digital signature algorithm
* CA:s X.509 - name
* validity time
* X.509 - name of the owner of the requested public key
* requested public key
* digital signature of CA

Below is a picture of a typical CA -hierachy. On the top is the root certifier, which has given CA - status for other servers, which deliver public keys to the users.



12 Methods of cryptoanalysis

Cryptoanalysis developes methods for breaking ciphers

Passive and ja active attacks

Passive attacks

"Eavesdropping" and capturing a message does not effect the message, keys, or protocol. Therefore it is very difficult to detect. One must concentrate on preventive measures instead of detection or stopping this kind of action.

Active attacks

Changing messages and system files, or acting as another user in the network are active attacks

Attack types

Ciphertext only attack

* The analyst has in his possession many ciphertexts
* The goal is to reveal the decryption key.
* Most common form of attack, because it is easy to get ciphertexts

- **Known plaintext attack**

* The analyst has one or more corresponding plaintext ciphertext pairs in his possession.
* The goal is to reveal the decryption key.
* Is sometimes based on the fact that the sender uses always the same phrase in the beginning or end of the message.

- **Chosen plaintext attack**

* The analyst can in some extend influence the plaintext before it is encrypted
(For example the enemy sends to some employees a letter containing such an interesting information, that the empoyees will probably send the contents encrypted to their leadership. This way the enemy gets a pair of plaintext and its encryption)
* This method gives the analyst more possibilities to analyze the encryption method he wants to break.

- **Chosen ciphertext attack**

* The analyst can test the encryption algorithm with many chosen messages getting outputs from each of them.
This method is used when DES block cipher has been explored and finally broken.
* This attack also enables very effective methods like differential analysis, in which minor changed are made to the message and the changes in the ciphertext due to them are observed

- **Man in the Middle attack**

* For example Peter sends his public key to Alice. Eve captures the message and sends Alice his own public key instead. Alice does not know anything about the change.
* Eve captures the public key from message from Alice to Peter in the same way. This way Eve can be in the middle of Alice and Peter and read their correspondence.

* Using CA's prevents Man in The Middle attacks.

- **Dictionary attack**

The size of key space is significantly reduced, if the hacker uses a dictionary of most common passwords instead of complete search.

In practise a hacker may download the password file with user names and hash values of passwords. Then he may use a password dictionary and calculate the hash values of its words. If one of the hash values in the list match some of the hash values in the password file, he can access the system.
"Salting" passwords is one way to prevent or slow down this attack.

- **Replay attack**

In a distributed system this attack is a thread. The enemy captures data from teh channel and tries to use it in a login procedure. The captured data can be data from authentication process.
Uses of time stamps and serial numbers of packages are preventive measures against replay attack.

- **Side Channel attack**

This form of attack differs from others. Imagine that X can measure the emission of radiation of a computer at the moment when the computer performs RSA -decryption by $m = m^d$ mod n.
In fast exponentiationalgorithm the exponention is divided to n parts, the number of which depends on the magnitude of decryption exponent d . By measuring the emitted radiation of the computer X could possibly find out the value of d.

13 Secure protocols

Encryption algorithms work usually hidden inside a secure protocol. These protocols can often be configured to use several different encrytion algorithms. An ordinary user most often does even know what algorityms his software uses for encryption.

S-HTTP Secure Hypertext Transport Protocoll

* HTTP with additional security properties

* Offers a secure Internet cconnection

* The client application and serverillä have both a variety of prefer red encryption protocols . When the client contacts the server, the servers asks from the client on which encryption protocol this is configured. When encryption algorithm is agreed on, the client sends his public key to the server, which generates a session key and sends it in a digital envelope to the client.

S-HTTP is also able to calculate hash values , perform digital signatures and authentication. It support both public key and symmetric key encryption.

HTTPS

* When S-HTTP secures every message , HTTPS protects the channel between two computers using SSL and HTTP protocols.

SSL Secure Socket Layer

- used in banking software

* SSL is similar to S-HTTP. but protects the channel instead of individual messages.
* It uses public key encryption offering encryption, digital signature and two way atuthentication. In the beginning of the connection SSL forms the session key. Encryption is done with a symmetric block cipher.
* Channel is kept open until one of the parties ends the session.
* The browser must supprt SSL-protocol
* Protocol is between application layer and net layer in OSI model

SET Secure Electronic Transaction

* Credit card payment protocol introduced by Visa and Master Card
* A cryptographic protocol for transmission of credit card numbers in Internet
* It is more complex than SSL, which is more used

SSH Secure Shell

* A sort of tunneling mechanism which offers some kind of terminal use tunnel with the host.
* Provides authentication and secure data transfer in Internet
* SSH should replace the use of Telnet and FTP
* Diffie Hellman algorithm is used for key agreement

IP-Sec Internet Protocoll Security

* Method for crating a secure channel for data transfer between two computers.
* Uses strong encryption and strong authentication

S-MIME Secure Multipurpose Internet Mail Extension

* standard for email encryption and digital signature
* User can choose encryption- and hash - algorithms.
* Provides ancryption, digitaal signaturen, authentication with X.509

PEM Privacy- Enchanged Mail

* like previous, uses DES for encryption, RSA for key agreement

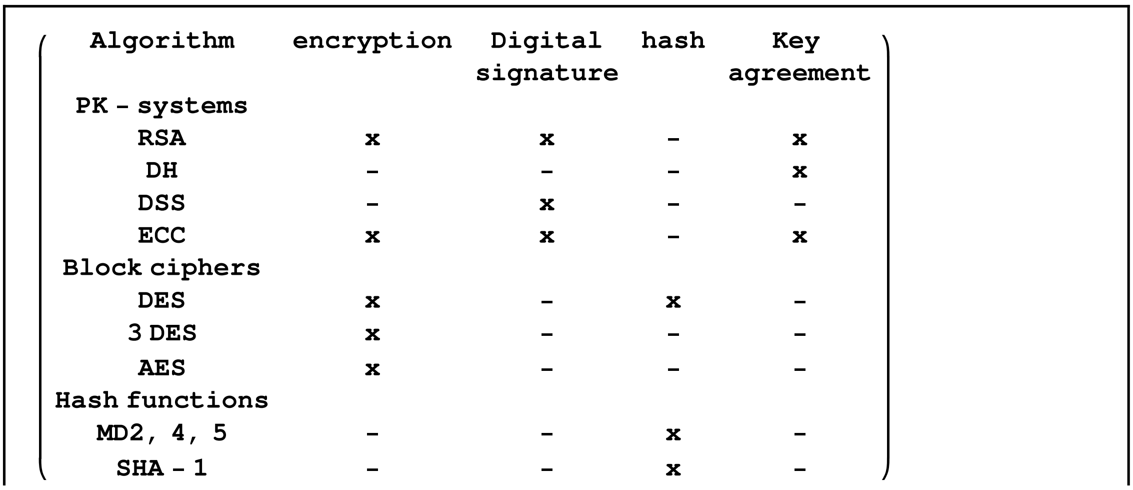
PGP freeware from 1991

* the most popular cryptosystem in the world
* originally uses IDEA block cipher for encryption, today more choices
* hash algorithm originally MD5 , today more choices
* key agreement with RSA
* uses peer ring in certifying public keys
* Community of users which trust each other (no CA's needed)

See pages *www. pgpi.org*.

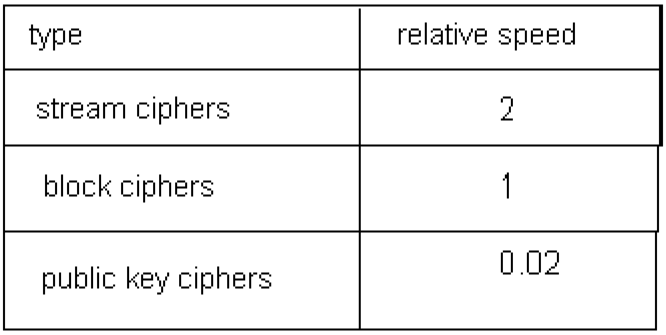
14 Summary of algorithms and applications

- **Table of algorithms and their uses**



Algorithm	encryption	Digital signature	hash	Key agreement
PK - systems				
RSA	x	x	-	x
DH	-	-	-	x
DSS	-	x	-	-
ECC	x	x	-	x
Block ciphers				
DES	x	-	x	-
3 DES	x	-	-	-
AES	x	-	-	-
Hash functions				
MD2, 4, 5	-	-	x	-
SHA - 1	-	-	x	-

■ Relative speeds



type	relative speed
stream ciphers	2
block ciphers	1
public key ciphers	0.02

■ Key sizes

* For block ciphers minimum key length is 128 bits

* In asymmetric algorithms like RSA and Diffie Hellman , minimum key size is 1024 bits. Within five years this may be too short and the key length should be 2048 bits. (Lenstra)

* In hash functions there are lots of problems. SHA-1 and RD5 are both broken. Recommendation is now SHA-2.

■ NESSIE project

New European Schemes for Signatures, Integrity, and Encryption

In 1999 has European Union started an own project for establshment of European encryption standards and recommendations. The intermediate report - written by the best experts of Europe - is published in 2004. In the web this document is found at www.cryptonessie.org