Computer Science Basics
Public Key Infrastructure

Fall Term 2023/2024

Emmanuel Benoist | BFH-TI

Public Key Infrastructure

Problem

Problem: Key exchange

How to know the public key

- Alice or Bob can give themselves the public keys physically
- publish the keys on public servers
- send the keys by email
- Attach the keys to their messages **Problem:** how to know if it's the right key

Trusted Third Party

- A Certificate Authority (CA) will "validate" a certificate
- Alice and Bob must have confidence in this Certificate Authority
- Alice and Bob must know the public key of the CA

The CA will certify the relationship between an "identity" and a public key

- A certificate is signed by the CA for Alice and Bob
- Contains Alice's (resp. Bob) identity and public key, all signed by the CA.

Public Key Infrastructure

PKI Architecture

Public Key Infrastructure (PKI)

- Allows a secure key exchange
- A prerequisite for the use of public key cryptography

Central role: the Certificate Authority (CA)

- Everyone knows their public key
- Uses their private key to sign new certificates

A certificate

- The identity of the holder.
- The holder's public key.
- The identity of the CA.
- The signature made by the CA.

Alice and Bob

- Can exchange their certificates;
- test the validity of these certificates (i.e. public keys);
- trust the other's certificate.

Certificate Information

X509 certificates

- Used by websites to ensure the "handshake" of TLS.
- TLS is used by https, sftp, …

At least

- Server name
- Public key
- identity of the Certificate Authority
- Protocols used for signature

Supplementary information

- Identity of the holder
- Physical address of the holder

Google.com certificate

DEMO

`https://www.google.com`

TLS

Transport Layer Security (TLS)

Internet protocols for secure connections

- Base for HTTPS, SFTP, ...

Goal: communicate securely with a server

- Be sure to communicate with the right server
- Make sure only the server can read what you send.
- I'm sure what we're receiving is coming from the server

Means

- A PKI architecture
- The server certificate

Problems

- Public key cryptography: very slow and consumer of computation time.
- secret key cryptography (symmetrical) : fast, but requires knowing each other.

TLS Handshake

Use public key cryptography (asymmetric)

- We download the certificate from the server
- We're checking this certificate
- We establish an encrypted communication with the server
- Together we define a secret key (new one that only serves once)

The protocol continues with this secret key

- Symmetric cryptography, much more efficient

Principle

- First of all, we don't know each other,
- We exchange business cards (and check them)
- Then we know each other and we can talk faster

Problems with TLS

TLS is often used as single security measure

- Often rely only on the certificate of the server
- Can be configured to use 2 certificates (1 for client, 1 for server).

List of Certificate Authorities

- Which ones are trusted?

How to update certificates for CAs

- Not an easy task,
- Very sensitive.

What if a certificate is corrupt?

Certificate can be corrupt if private key is stollen

- Stollen by an employee
- Hacked on the server
- Brute forced by an attacker
- Not considered secure anymore

Need to limit the validity of a certificate

- Certificates must contain a validity date

Revocation Lists

- Certificate authorities provide lists of revoked certificates : *Revocation Lists*.

Application should

- Have a list of valid CAs (the ones we trust)
- Should check for the revocation list
- Should not accept a certificate issued by a not trustworthy CA.

Conclusion

Conclusion

Cryptography

- Public Key cryptography (asymmetric)
- Secret Key cryptography (symmetric)

Protocols

- Mix both systems
- Asymmetric crypto to start (using Diffy-Hellman for instance).
- Then symetric crypto to send payload (data).

Public Key Infrastructure

- To transmit public key.
- To be certain the public key belongs to one person (or identifier).