Public Key Infrastructure

Public Key Distribution

One of the most important applications of digital signatures:

- Distribution of public keys in a secure way

  The main idea:
- Public-key cryptography is used to distribute public keys
- Initial step: binding entities to public keys (certification)
- Later steps: using certified keys for further certification

Digital Certificates

- Suppose B has a key pair $(\mathrm{pk}_B, \mathrm{sk}_B)$ and C has a key pair $(\mathrm{pk}_C, \mathrm{sk}_C)$. A digital certificate for B's key issued by C is a signature

$$\mathrm{cert}_{C \to B} = \mathrm{Sign}_{\mathrm{sk}_C}(\text{“I certify that } B\text{'s public key is } \mathrm{pk}_B\text{”})$$

- Suppose B is identified by his full name or ID number or some other information
- Using C's public key, everyone who knows and trusts C can verify B's public key

Digital Certificates

Communication between A and B.

- Suppose B has a certificate $\mathrm{cert}_{C \to B}$
- Suppose A knows and trusts C and wants to communicate with B
- B sends $\mathrm{cert}_{C \to B}$ and pk_B to A
- A verifies the certificate with C's public key
- A now knows B really has the key
- Note that all communication between A and B can be in an insecure channel

Main question: How does A learn C's public key?

Public Key Infrastructure

A Public Key Infrastructure is a framework for securely distributing and managing public keys. A few models:

- Single certificate authority
- Multiple certificate authorities
- Delegation and certificate chains
- Web of trust

Single Certificate Authority

- Single certificate authority: company, agency or a department within a firm
- Certificate most commonly obtained physically (in person)
- Authentication: using ID card, passport etc.
- Certificate: USB key or QA code etc.
- Bootstrap: "relatively expensive", but happens only once
- Examples:
  - Employees on their admission
  - Bundled with products (OS, browser, hardware products)

Multiple Certificate Authorities

- Physical contact sometimes impossible
- Relying on only one authority has risks
- Handling multiple authorities, each party can decide
  - Which authorities to trust (the more we trust, the higher the risk)
  - Which certificates to obtain
- If A trusts any of the issuers that had certified B's public key, then she can decide to accept it
- Problem: it is more likely to find a corrupt one among many authorities

Delegation

- An authority A can issue certificates to secondary certifiers, e.g. B
- Such a certification can work as an authorization to issue further certificates
- Secondary certifiers certify the public key together with their own certification
- Problem: it is more likely to find a corrupt one among many authorities

Web of Trust

- There are no central authorities
- Trust and authentication are distributed
- Every participant decides on the level of confidence she has in the others
- The keys and certificates can be stored in a central database, e.g. PGP
- Mainly appropriate at the personal level, inappropriate at the organizational level

Expiration and Withdrawal of Certificates

Compromised private keys or changes in trust between parties require the possibility for invalidating a certificate

- Expiry date included in the signature
- Revocation list signed by the issuer

We demonstrate PKI and key management through examples

- Browsers and authority settings
- Pretty Good Privacy (PGP)
- Legal issues

NSA - NCSA

- The hungarian **NSA** (National Security Authority) was established in 1998.
- NSA is responsible for the protection of NATO, EU and National classified information.
- The Parliament of Hungary adopted Act CLV. Of 2009 on the Protection of Classified Information on December 14, 2009 by 332 yes votes against 17 no. According to the new law NCSA (National Crypto Security Authority) belongs to the HUN NSA.
- A new Government Decree was adopted: Decree on the protection of classified information in the communication information systems (INFOSEC): it covers Communication Security (Transmission, Emanation and **Crypto Security**) and Information System Security (Networks, Hardware, Software).

Rules...

- Several examples will be presented and discussed.
- Examples are originated from different vulnerability assessments and security hardening projects conducted by the National Security Authority of Hungary (NSA).
- This presentation is made with the authorization of the Hungarian NSA and is **not containing calssified infromation**.