Using Public Key Cryptography

Key management and public key infrastructures

Key management and public keys

- Two aspects of key management relate to the use of public key cryptography.
  - Public key provides mechanisms for delivery and management of secret keys for symmetric cryptographic algorithms, such as DES, AES, or RC4.
  - Public key cryptography requires mechanisms for public key distribution, to guarantee authenticity of keys.

Distribution of public keys

- Public keys must be distributed in some trustworthy fashion.
  - Otherwise, Mallory may provide Bob with a fake public key for Alice, resulting in:
    - Failure to communicate with Alice
    - Improper release of confidential information to Mallory
    - Mallory being able to authenticate messages as if originated from Alice.
Distributing public keys

- Several mechanisms are available, such as:
  - public announcement
  - publicly available directory
  - active, online public key authority
  - public key certificates
  - general public key infrastructure

Public announcement

- Publicly announce your public key, by appending it to your website, or attaching it as a signature to e-mails, etc.
- Advantages:
  - Simple, cheap and convenient
- Disadvantages:
  - Hidden costs of off-band authentication; or lack of any authentication mechanism altogether.

Public directory

- An authoritative entity maintains a directory of (name, public key) entries.
- Periodically, the directory is updated if new keys are added or revoked.
- The directory could be a highly available electronic database—but then authentication of the data retrieved must be provided.
  - Since individual records can be changed/revoked, it is necessary in this case to have proof-of-current-membership
Online, active public authority

Off-line public authorities

• An online, active trusted party creates a host of difficult engineering issues:
  – High availability and high security are hard to combine successfully
  – Scalability: The trusted party can become a performance bottleneck
  – Denial-of-Service: The trusted party introduces a single point-of-failure in the security framework

Public key certificates

• Certificates are an off-line alternative mechanism to the online trusted party.
• When a user registers a new public key with the authority, it receives a digital signature on a document that includes both a *unique identifier for the user* as well as the public key.
  – Certificate: Binds the pair <identifier, key>
Certificate system

Certificate
Authority

PK_A, proof of identity

Cert_A = Sign_CA(ID_A||PK_A||Exp.time)

PK_B, proof of identity

Cert_B = Sign_CA(ID_B||PK_B||Exp.time)

Public Key Infrastructures

• In order for a certificate-based system to be functional (i.e., users accept each other certificates), there needs to be agreement on common certification authorities, certificate and signature formats, and the public keys of the certificate authorities need to be distributed securely.

• A framework that addresses all these issues is called a Public Key Infrastructure (PKI).

Examples of PKIs

• Anarchic
  – Based on peer trust and out-of-band verification mechanisms (e.g. PGP)

• Monopolistic

• Oligarchic
  – Internet e-business

• Name-constrained
  – Software package management
Oligarchic PKI

• Internet/E-business
  – E-business transactions are supported by the X.509 certificate format standard.
  – Public keys of trusted authorities are embedded in applications; commercial relationships between the dominant players ensure key distribution.

Your web browser’s keys