Public Key Infrastructure

BIL 448/548
Internet Security Protocols
Ali Aydin Selçuk

• A system to securely distribute & manage public keys.
• Important for wide-area trust management (for e-government, e-commerce, e-mail, etc.)
• Ideally consists of
  – a certification authority
  – certificate repositories
  – a certificate revocation mechanism (CRLs, etc.)
• Many models possible: monopoly, oligarchy, anarchy, etc.

Monopoly Model

• Single organization is the CA for everyone
• Shortcomings:
  – no such universally-trusted organization
  – requires everyone to authenticate physically with the same CA
  – compromise recovery is difficult (due to single embedded public key)
  – once established, CA can abuse its position (excessive pricing, etc.)
  – requires perfect security at CA

Monopoly with Registration Authorities

• CA trusts other organizations (RAs) to check identities, do the initial authentication
• Solves the problem of physically meeting the CA. Other problems remain.
• RAs can be incorporated into other models too
Delegated CAs

- Root CA certifies lower-level CAs to certify others
- All verifiers trust the root CA & verify certificate chains beginning at the root (i.e., the root CA is the trust anchor of all verifiers)
- E.g., a national PKI, where a root CA certifies institutions, ISPs, universities who in turn certify their members
- Limitations are similar to monopoly with RAs

Oligarchy

- Many root CAs exists trusted by verifiers
- The model of web security
- Solves the problems of single authority (e.g., excessive pricing)
- Disadvantages:
  - n security-sensitive sites instead of one. Compromise of any one compromises the whole system
  - users can easily be tricked into trusting fake CAs. (depending on implementation)

Anarchy

- Each user decides whom to trust & how to authenticate their public keys
- Certificates issued by arbitrary parties can be stored in public databases, which can be searched to find a path of trust to a desired party
- Works well for informal, not-so-sensitive applications (e.g., PGP)

Revocation

- Mechanisms to cancel certificates compromised before expiration
- Certificate Revocation List (CRL): list of revoked certificates, published periodically by the CA
- Delta CRLs: Only the changes since the last issue are published
- Online Revocation Servers: No CRL is published. Verifier queries a central server to check if a certificate has been revoked.
Finding Certificate Chains

• Can be sent by the subject sending its public key to the verifier (e.g., SSL)

• A directory naming structure can be followed (e.g., LDAP, DNSsec)

X.509 Certificates

• Common standard for certificate format
• PKIX: Internet standard for X.509-based PKI
• Fields (X.509 v3):
  – version
  – serial number
  – signature algorithm identifier
  – issuer
  – validity period
  – subject
  – subject public key information
  – signature
  – standard extensions (key usage limitation, etc.)
  – other extensions (application & CA specific)