CS 465 Computer Security

Public Key Certificates

Kent Seamons

Last update: Feb 21, 2006
Background

- A certificate was originally created to bind a subject to the subject’s public key
- Intended to solve the key distribution problem for public keys by narrowing the problem to the secure distribution of the CA public key
Figure 3.12 Public-Key Certificate Use
Definitions

- Certificate authority (CA) – Issuer
  - Certification Practice Statement (CPS) – statement of practices the CA employs to issue certificates
  - Registration Authority (RA) – entity that identifies and authenticates subjects, but does not issue certificates
- Expiration – Validity period of the certificate
- Certificate Revocation List (CRL)
  - Analogous to a list of lost or stolen credit card numbers
  - When is there a need to revoke a certificate?
- Relying party – Recipient of a certificate who relies on the information contained in the certificate
  - How does the relying party validate the certificate?
- Public Key Infrastructure (PKI)
  - Infrastructure necessary to deploy and use public key technology
Certificate Hierarchy

- Trusted root
- Certificate path
  - The subject of a parent certificate in the chain is the issuer of the child certificate
  - How would you verify a chain? Top-down or bottom-up?
- What if a Department certificate is revoked? How is the hierarchy repaired?
Steps to Certificate Verification

- What are the steps a web browser (relying party) might take to verify a certificate?
  - Integrity
  - Expiration
  - Revocation
  - Usage constraints
    - Basic constraints - Can the subject act as a CA?
      - Is there a limit to the length of a certificate chain?
    - Limitations on key usage
  - Ownership
    - Does the entity presenting the certificate own the associated private key?
Required Reading

- Ten Risks of PKI
  *C. Ellison and B. Schneier*
  - Who do we trust, and for what?
  - Who is using my key?
  - How secure is the verifying computer?
  - Which John Robinson is he?
  - Is the CA an authority?
  - Is the user part of the security design?
  - Was it one CA or a CA plus a Registration Authority?
  - How did the CA identify the certificate holder?
  - How secure are the certificate practices?
  - Why are we using the CA process, anyway?