CS 465

Certificates

Last Updated: Oct 8, 2012

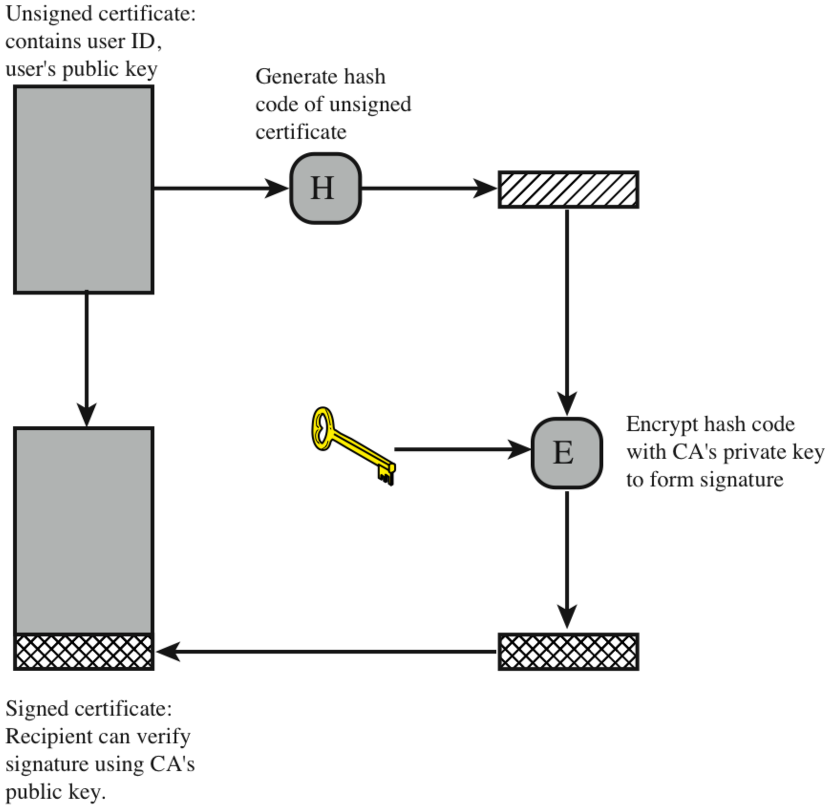
Background

- 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

Certificate Generation

- Who generates the subject's key pair?


Unsigned certificate: contains user ID, user's public key
Generate hash code of unsigned certificate
H
E
Encrypt hash code with CA's private key to form signature
Signed certificate: Recipient can verify signature using CA's public key.

Source: Stallings, Network Security Essentials

Terminology

- Certificate Authority (CA) – Issuer
  - Certification Practice Statement (CPS)
    - A statement of the practices employed by the CA to issue certificates
  - Registration Authority (RA)
    - Entity that identifies and authenticates subjects
    - Does not issue certificates
  - Trusted Third Party (TTP)
- Expiration
  - Valid lifetime of the certificate
- Certificate Revocation List (CRL)
  - Analogous to a list of lost or stolen credit card numbers
  - When do certificates need to be revoked?
- Relying party
  - Recipient of a certificate that relies on the information it asserts
  - How does the relying party validate the certificate? (5 steps)
- Public Key Infrastructure (PKI)
  - Infrastructure necessary to deploy and use public key technology
  - The infrastructure needed to recognize which public key belongs to whom

Certificate Verification

- What steps should a relying party (e.g., web browser) 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 the certificate chain?
      - Limitation on key use
  - Ownership
    - Does the entity presenting the certificate have access to the associated private key?

PKI Reality

- Names – how to identify subjects?
- Authority – no universal authority
- Trust – who do we trust as the CA?
- Revocation – hardest PKI problem to solve
  - CRL
  - Fast expiration
  - Online certificate verification (OCSP)
- PKI vs. key server
  - Advantages of PKI server to key server
  - Recommend key server for small systems, PKI for larger systems

Source: Cryptography Engineering, Ferguson et al., Chapter 19

PKI Examples

- What are some examples of how a PKI could be implemented and used?
  - Universal PKI
  - Corporate VPN
  - On-line banking
  - University

Certificate Hierarchies

- Complex organization may distribute the certificate issuing process
  - Example: How might BYU issue student certificates using the University, College, Department organizational structure?

- How to create a hierarchy?
- How to verify a certificate chain?
- How to recover from a lost/stolen private key?

Compromised CAs

- There are risks when we trust a third party
  - Some examples are posted on the lectures page
    - Verisign issued two fraudulant Microsoft certificates in 2001
    - Dutch CA DigiNotor was compromised in 2011