CS 465

Certificates

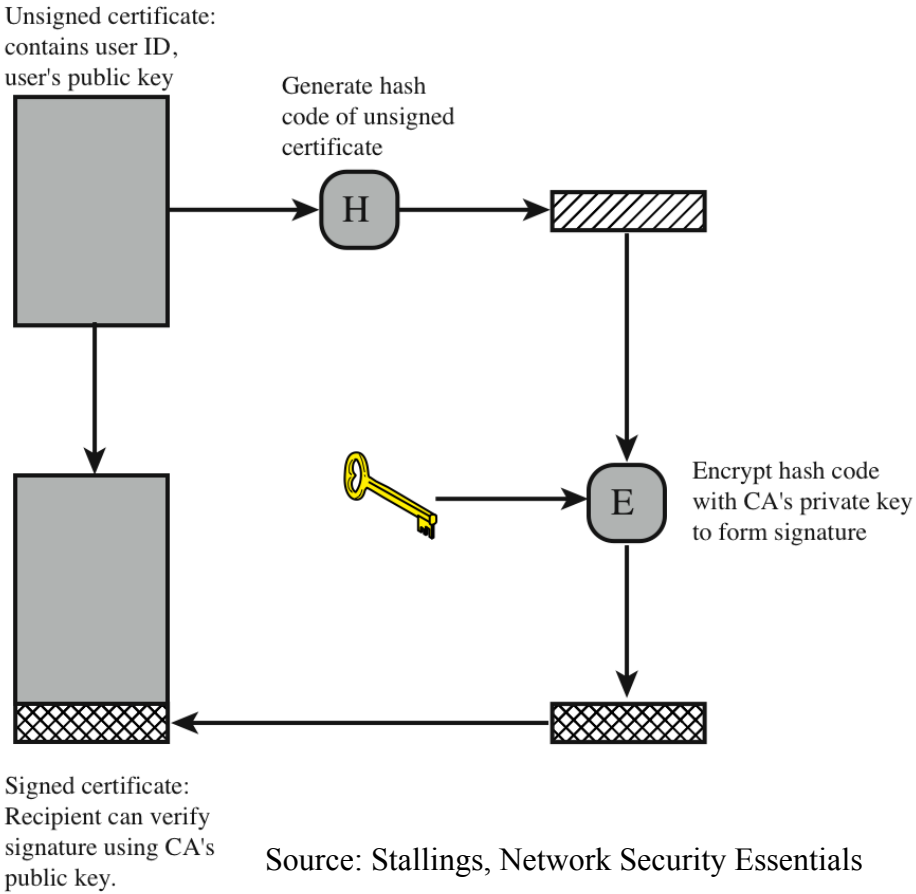
Last Updated: Oct 14, 2017

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?
  - Usually the subject generates the key pair and the CA only sees the public key. The CA challenges for ownership of the private 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 – encryption or signing
  - Ownership
    - Does the entity presenting the certificate have access to the associated private key?
    - Challenge for ownership of the key at the time of the transaction

Compromised CAs

There are risks when we trust a third party

The system is only as strong as the weakest link

Attack examples (links on the lectures page)

- 2001: Verisign issued two fraudulent Microsoft certificates
  - No revocation infrastructure, so Microsoft patch had to explicitly blacklist these two certificates in the verification code
- 2011: Dutch CA DigiNotor was compromised
  - Led to man-in-the-middle attack on 300,000 Iranian citizens

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
  - Certificate Revocation List (hard to keep updated, lists grow large)
  - Fast expiration through short-lived keys
  - Online certificate verification (OCSP)

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?
  - BYU CA issues certificates to College CAs
  - College CAs issue certificates to Department Cas
  - Departments issue certificates to students

- How to create a hierarchy?
- How to verify a certificate chain?
  - The relying party could only have the BYU public key
  - The client or server has to discover the certificate chain – one method is for the client to deliver the chain to the server

Certificate Hierarchies

- How to recover from a lost/stolen private key?
- What if the college has a private key compromised?
  - College has to generate a new key pair and get BYU to sign a certificate with the new public key
  - College has to sign department public keys again with the new key private key Re-issue department certificates
  - Student certificates are ok
- What if department has it's key compromised?
- Only have to re-sign certificates one level below in the hierarchy. Don't need to re-create the entire hierarchy