Digital Certificates, Certification Authorities, and Public Key Infrastructure

Sections 14.3-14.5

Basic Problem

• What does a public-key signature verification tell you?
  Verification parameters include public key, and successful verification says “Only someone holding the corresponding private key could have made this signature.”

• What do you want a signature verification to tell you?
  Probably something like “Joe Smith signed this.”

• Problem: What assurance do you have that the public key really belongs to Joe Smith?

What is a Digital Certificate?

• Associates an identity/properties with a public key
  – Identity can be person’s name, website, e-mail, ...
  – Properties can be valid key uses, age of individual, access rights granted, ...

• Signed by someone you trust
  – Signature is trusted party vouching for ID/key pair
  – Role is similar to a notary public

• Some typical properties of certificates:
  – Good for a set time (validity period)
    • Must get a new certificate after expiration
  – Certificates may be revoked
More on Certificates

• Common types of certificates:
  – X.509 standard (version 3)
  – PGP certificates

• Who signs certificates? Several possibilities:
  – Independent “Certification Authority” organization
  • Disinterested third party – company or government
  • Examples: Verisign, Deutsche Telekom, Entrust, AOL, …
  – Internal (organizational) certification authority
  • Organization controls certificates for employees or clients
  – Could be just an individual you trust
  • This is how PGP certificates are typically certified

X.509 Certificates

• Most prevalent type of digital certificate
• Related to X.500 directory services
• An integral part of the Web
  – All major web browsers and servers support X.509
  – CA “industry” (Verisign, etc.) built around X.509
• Also part of secure e-mail specifications
  – S/MIME
• Currently “version 3” of X.509
  – Includes a flexible “extension field” capability

X.500 Names
(Also called “Distinguished Names”)

• Hierarchical naming
• Parts of names are attribute/value pairs
• Example attributes:
  – C=country
  – ST=state
  – L=locality
  – O=organization
  – OU=organizational unit
  – CN=common name
Important “Additional Information”

- How does a CA state how they do business?
  - A Certification Practices Statement (CPS) is a human-readable statement of practices used by CA
    - Based on this, a person/vendor may decide whether to trust or not trust the CA
    - Problem: What if CPS becomes a dead link? Trust the CA?
- Where to obtain the Certification Revocation List (CRL)
  - Called a CRL Distribution Point (CDP)
  - Certificates may be revoked due to
    - Private key compromised
    - Incorrectly issued certificate
    - CA compromised
    - Properties change
  - CRL contains unexpired revoked certificates
    - Current size of Symantec CRL: 1,266,051 bytes (36,162 entries)

Example: Amazon Certificate
(Extension fields removed)

<table>
<thead>
<tr>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version: 3 (0x2)</td>
</tr>
<tr>
<td>Serial Number:</td>
</tr>
<tr>
<td>Signature Algorithm: sha1WithRSAEncryption</td>
</tr>
<tr>
<td>Issuer: C=US, O=RSA Data Security, Inc., OU=Secure Server Certification Authority</td>
</tr>
<tr>
<td>Validity: Not Before: Jan 06 00:00:00 2005 GMT Not After: Jan 06 23:59:59 2006 GMT</td>
</tr>
<tr>
<td>Subject: C=US, ST=Washington, L=Seattle, O=Amazon.com Inc., CN=www.amazon.com</td>
</tr>
<tr>
<td>Subject Public Key Info:</td>
</tr>
<tr>
<td>Public Key Algorithm: rsaEncryption</td>
</tr>
<tr>
<td>RSA Public Key: (1024 bit)</td>
</tr>
<tr>
<td>Modulus (1024 bits):</td>
</tr>
<tr>
<td>Exponent: 65537 (0x10001)</td>
</tr>
<tr>
<td>Signature Algorithm: sha1WithRSAEncryption</td>
</tr>
</tbody>
</table>

Example: Amazon Certificate, Part 2
Extension fields

- X509v3 extensions:
  - X509v3 Basic Constraints: CA:FALSE
  - X509v3 Key Usage: Digital Signature, Key Encipherment
  - X509v3 CRL Distribution Points: URL:http://crl.verisign.com/RSASecureServer.crl
  - 1.3.6.1.5.5.7.1.2:
    - 8...:CMVMAU...image/gif/8R.B... disposed...K...J/N,8...
    - 8...:http://logo.verisign.com/vlslogo.gif
Certificate Chains
(Hypothetical)

"Trust Anchor" or "Root CA"

Subject: UNCG CS CA
UNCG CS Public Key
Issuer: UNCG CA

Subject: Steve Tate
Steve's Public Key
Issuer: UNCG CS CA

Subject: UNCG CA
UNCG Public Key
Issuer: Verisign

Subject: Verisign
Verisign Public Key
Issuer: Verisign (trusted)

Public Key Infrastructure (PKI)

- A PKI is "a collection of technologies and policies for creating and using digital certificates." [Garfinkel and Spafford]
- Many people originally envisioned an official digital ID system
  - In reality: Very little personal ID done with certificates – mostly used for server identification
  - Could change if security tokens or smart cards become more prevalent! Maybe smartphones?

Another Trust Model: PGP "Web of Trust"

- PGP is "Pretty Good Privacy"
  - Originally for e-mail encryption/signing
  - Now regularly used for software verification
  - Originally written by Phil Zimmerman
  - Now several free and commercial versions
  - GPG ("Gnu Privacy Guard") if a Free-Software alternative (they use only free algorithms)
- Trust model is less hierarchical than X.509
- I can sign keys and distribute them
  - Anyone who trusts me can use me as a CA!
  - Difference between "trusted" and "valid" keys
PGP/GPG Keyservers

- Problem: How do you get public keys?
  - Note: In PGP public keys are always certificates

- Solution: Keyservers – databases of keys
  - You can submit your own keys
  - You can look up keys by name or e-mail address
  - Support integrated into many e-mail programs

- Keyservers can be accessed in many ways
  - LDAP
  - HTTP
  - E-mail

Keyserver example – WWW interface
Sending an encrypted email – Step 1: Look up the key

Keyserver example – WWW interface
Sending an encrypted email – Step 2: Find the right one - who vouches for it?
Keyserver example – WWW interface
Sending an encrypted email – Step 3: Download key (to import into PGP)

Some problems with certificates

- Private keys are not people
- Distinguished names are not people
- There are too many Robert Smiths
- X.509 v3 doesn’t allow selective disclosure
- Ubiquitous certificates could lead to privacy issues
- How do you loan a key?
- Signatures are “brittle”

- But overall: Not perfect, but solves some important problems