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 (2018) size of Symantec CRL: 1,211,730 bytes (34,610 entries)
  - Newer technology: OCSP (Online Certificate Status Protocol)

---

Example: Amazon Certificate

(Extension fields removed)

- **Data:**
  - Version: 3 (0x2)
  - Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec
  - Class 3 Secure Server CA – G4
  - Validity
    - Not Before: Oct 6 00:00:00 2017 GMT
    - Not After: Sep 21 23:59:59 2018 GMT
  - Signature Algorithm: sha256WithRSAEncryption

- **Subject Public Key Info:**
  - Public Key Algorithm: rsaEncryption
  - Modulus:
    - 00:de:59:92:15:5c:f4:ae:8e:c4:ee:8e:ff:b3:97:
    - [Deleted] ...
  - Exponent: 65537 (0x10001)

- **Signature Algorithm:** sha256WithRSAEncryption

Example: Amazon Certificate, Part 2

**Extension fields**

- **X509v3 extensions:**
  - Subject Alternative Name:
    - DNS:amazon.com, DNS:amzn.com, DNS:buybox.amazon.com, ...
  - Basic Constraints:
    - CA:FALSE
  - Key Usage:
    - critical
  - Digital Signature, Key Encipherment
  - TLS Web Server Authentication, TLS Web Client Authentication
  - Certificate Policies:
    - Policy: 2.23.140.1.2.2
    - CPS: https://d.symcd.com/cps
  - User Notice:
    - Explicit Text: https://d.symcd.com/rpa
  - Authority Key Identifier:
  - CRL Distribution Points:
    - Full Name: Full Name
    - URI: http://ss.symcd.com/ss.crl
  - Authority Information Access:
    - OCSP - URI:http://ss.symcd.com
    - CA Issuers - URI:http://ss.symcd.com/ss.crt
Certificate Chains
(Hypothetical)

"Trust Anchor" or "Root CA"

Subject: UNCG CA
UNCG Public Key
Issuer: Verisign

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

Subject: UNCG CA
UNCG Public Key
Issuer: Verisign

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

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

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”) is 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