PUBLIC-KEY CERTIFICATES

◆ reliable distribution of public-keys
◆ public-key encryption
  ● sender needs public key of receiver
◆ public-key digital signatures
  ● receiver needs public key of sender
◆ public-key key agreement
  ● both need each other’s public keys
THE CERTIFICATE TRIANGLE

user

X.509 attribute certificate

attribute

SPKI certificate

public-key

X.509 identity certificate

X.509 CERTIFICATE

VERSION
SERIAL NUMBER
SIGNATURE ALGORITHM
ISSUER
VALIDITY
SUBJECT
SUBJECT PUBLIC KEY INFO

SIGNATURE
**X.509 CERTIFICATE**

<table>
<thead>
<tr>
<th>0</th>
<th>1234567891011121314</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RSA+MD5, 512</td>
</tr>
<tr>
<td></td>
<td>C=US, S=VA, O=GMU, OU=ISSE</td>
</tr>
<tr>
<td></td>
<td>5/1/97-5/1/98</td>
</tr>
<tr>
<td></td>
<td>C=US, S=VA, O=GMU, OU=ISSE, CN=Ravi Sandhu</td>
</tr>
<tr>
<td></td>
<td>RSA, 1024, xxxxxxxxxx xxxxxxxxxx xxxxxxxxxx</td>
</tr>
</tbody>
</table>

**CERTIFICATE TRUST**

- how to acquire public key of the issuer to verify signature
- whether or not to trust certificates signed by the issuer for this subject
Lecture 7: Digital Certificates

PEM CERTIFICATION GRAPH

- Internet Policy Registration Authority (IPRA)
  - Policy Certification Authorities (PCAs)
    - HIGH ASSURANCE
      - MITRE
        - Abrams
    - MID-LEVEL ASSURANCE
      - Certification Authorities (CAs)
      - GMU
        - Virginia
    - RESIDENTIAL
      - Anonymous
    - PERSONA
      - LEO

Subjects:
- Sandhu

CRL FORMAT

- SIGNATURE ALGORITHM
- ISSUER
- LAST UPDATE
- NEXT UPDATE
- REVOKEDE CERTIFICATES
- SIGNATURE
- SERIAL NUMBER
- REVOCATION DATE
PGP BOTTOM UP
TRUST MODEL

◆ How does Alice get Bob’s public key
  ● directly from Bob through some secure channel (e.g., post, phone, floppy)
  ● from Chuck, who is known to both Alice and Bob and introduces Bob to Alice
  ● from a trusted certifying authority
◆ PGP has mechanisms to support these, and related, alternatives

X.509 CERTIFICATES

◆ X.509v1
  ● very basic
◆ X.509v2
  ● adds unique identifiers to prevent against reuse of X.500 names
◆ X.509v3
  ● adds many extensions
  ● can be further extended
SEPARATE KEYS FOR SEPARATE PURPOSES

- RSA is the only known public-key cryptosystem in which the same public-private key pair can be used for
  - digital signatures
  - encryption
- perceived as a major advantage

SIGNATURE KEYS

- private key: must be private for entire life, may never leave smart card
  - needs to be securely destroyed after lifetime
  - no need for backup or archiving (would conflict with above)
  - no need to weaken or escrow due to law
- public key: must be archive possibly for a long time

© Ravi Sandhu 2000
**ENCRYPTION KEY**

- **private key:** backup or archive required for recovery
  - should not be destroyed after lifetime
  - may be weakened/escrowed due to law
- **public key:**
  - no need to backup RSA or other encryption keys
  - need to backup Diffie-Hellman key agreement keys

---

**X.509 INNOVATIONS**

- distinguish various certificates
  - signature, encryption, key-agreement
- identification info in addition to X.500 name
- name other than X.500 name
  - email address
- issuer can state policy and usage
  - good enough for casual email but not good enough for signing checks
- limits on use of signature keys for further certification
X.509v3 EXTENSIONS

◆ X.509v3 same as X.509v2 but adds extensions  
◆ provides a general extension mechanism  
  ● extension type: registered just like an algorithm is registered  
  ● standard extension types: needed for interoperability

X.509v3 EXTENSIONS
CRITICALITY

◆ non-critical: extension can be ignored by certificate user  
  ● alternate name can be non-critical  
◆ critical: extension should not be ignored by certificate user  
  ● limit on use of signatures for further certification
X.509v3 EXTENSIONS
CRITICALITY

- criticality is flagged by certificate issuer
  - certificate user may consider non-critical extensions more important than critical ones
  - certificate user may refuse to use certificate if some extensions are missing
- critical extensions should be few and should be standard

X.509v3 NAMES

- internet email address
- internet domain name
- web uri (url's are subset of uri)
- IP address
- X.400 email address
- X.500 directory name
- registered identifier
- other name
X.509v3 STANDARD EXTENSIONS

- Key and policy information
- Subject and issuer attributes
- Certification path constraints
- Extensions related to CRLs
  - will be discussed with CRLs

KEY AND POLICY INFORMATION

- key usage
  - critical: intended only for that purpose, limits liability of CA
  - non-critical: advisory to help find the correct key, no liability implication
- private-key usage period
  - certificate valid for 2 years for verifying signature
  - key valid only for one year for signing
- certificate policies
  - for CAs
SUBJECT AND ISSUER ATTRIBUTES

- Subject alternative names
- Issuer alternative names
- Subject directory attributes
  - whatever you like
  - position, phone, address etc.

CERTIFICATION PATH CONSTRAINTS

- Basic Constraints
  - can or cannot act as CA
  - if can act as CA limit on certification path
    - limit=1 means cannot certify other CAs
- Name Constraints
  - limits names of subjects that this CA can issue certificates for
- Policy Constraints
  - concerned with CA policies
CERTIFICATION PATH CONSTRAINTS

- **Basic Constraints**
  - can or cannot act as CA
  - if can act as CA limit on certification path extending from here
  - limit=1 means cannot certify other CAs

- **Name Constraints**
  - limits names of subjects that this CA can issue certificates for
  - to be discussed

- **Policy Constraints:**
  - concerned with CA policies
  - to be discussed

CERTIFICATE REVOCATION LISTS

- **CRLs issued periodically as per CA policy**
  - off-cycle CRLs may also be needed
  - blank CRLs can be issued
CERTIFICATE REVOCATION LISTS

- CRL distribution
  - pull method
  - push method
- DMS example
  - pull method with push for compromised key list (CKL) which is broadcast via secure email, single CKL for entire system

immediate or real-time revocation
- needs query to CA on every certificate use
- maybe ok for small closed communities
**REVOCATION TIME-LINE**

Issue Of CRL 1 → Revocation Request → Issue Of CRL 2

↑ Compromise Event

↑ Revocation Time

---

**OCSP**

ON-LINE CERTIFICATE STATUS PROTOCOL

- consult authoritative server
- the server in turn can look up CRLs
SHORT-LIVED CERTIFICATES

- Authorization certificates can be short lived
  - minutes, hours, days instead of
  - months, years

X.509 CRL EXTENSIONS

- General Extensions
- CRL distribution points
- Delta-CRLs
- Indirect-CRLs
- Certificate Suspension
GENERAL EXTENSIONS

◆ Reason Code
  ● Key Compromise
  ● CA Compromise
  ● Affiliation changed
  ● Superseded
  ● Cessation of operation
  ● Remove from CRL: defer till Delta-CRL
  ● Certificate hold: defer
◆ Invalidity Date

CRL DISTRIBUTION POINTS

◆ CRLs can get very big
  ● version 1 CRL (1988, 1993)
    ■ each CA has two CRLs: one for end users, one for CAs
    ■ end user CRL can still be very big
  ● version 2 CRL
    ■ can partition certificates, each partition associated with one CRL
    ■ distribution point
    ■ also can have different distribution points for different revocation reasons
CRL DISTRIBUTION POINTS

- certificate extension field, says where to look
- CRL extension field
  - distribution point for this CRL and limits on scope and reason of revocation
  - protects against substitution of a CRL from one distribution point to another

DELTA-CRLs

- Delta CRL indicator
  - only carries changes from previous CRL
- Remove from CRL reason code causes purge from base CRL (stored at certificate user)
- removal due to expiry of validity period or restoration of suspension
INDIRECT-CRL

- CRL can be issued by different CA than issuer of certificate
  - allows all compromise revocations to be one list
  - allows all CA revocations to be on one list (simplify certificate chasing)

CERTIFICATE SUSPENSION

- Certificate hold reason code in CRL
- Supporting CRL entry extension
  - Instruction code: instructions on what to do with held certificate
    - call CA, repossess token
Lecture 7: Digital Certificates

TOP-DOWN HIERARCHICAL STRUCTURE

PEM CERTIFICATION GRAPH

© Ravi Sandhu 2000

© Ravi Sandhu 2000

INFS 766/INFT 865
Prof. Ravi Sandhu

Network and Distributed Systems
Security

Spring
SET CA HIERARCHY

FOREST OF HIERARCHIES