Public-Key Certificates

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 4

ravi.utsa@gmail.com
www.profsandhu.com
• authenticated 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
<table>
<thead>
<tr>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION</td>
</tr>
<tr>
<td>SERIAL NUMBER</td>
</tr>
<tr>
<td>SIGNATURE ALGORITHM</td>
</tr>
<tr>
<td>ISSUER (Certificate Authority)</td>
</tr>
<tr>
<td>VALIDITY</td>
</tr>
<tr>
<td>SUBJECT</td>
</tr>
<tr>
<td>SUBJECT PUBLIC KEY INFO</td>
</tr>
<tr>
<td>SIGNATURE</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>12345678910111121314</td>
</tr>
<tr>
<td>RSA+SHA-3, 2048</td>
</tr>
<tr>
<td>C=US, S=TX, O=UTSA, OU=CS</td>
</tr>
<tr>
<td>1/1/17-12/31/18</td>
</tr>
<tr>
<td>C=US, S=TX, O=UTSA, OU=CS, CN=Ravi Sandhu</td>
</tr>
<tr>
<td>RSA, 2048, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx</td>
</tr>
<tr>
<td>SIGNATURE</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
  - prefix rule is not universally applicable
<table>
<thead>
<tr>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234567891011121314</td>
</tr>
<tr>
<td>RSA+SHA-3, 2048</td>
</tr>
<tr>
<td>C=US, S=VA, O=GMU, OU=ISE</td>
</tr>
<tr>
<td>1/1/17-12/31/18</td>
</tr>
<tr>
<td>C=US, S=TX, O=UTSA, OU=CS, CN=Ravi Sandhu</td>
</tr>
<tr>
<td>RSA, 2048, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx</td>
</tr>
<tr>
<td>SIGNATURE</td>
</tr>
</tbody>
</table>
SET CA Hierarchy

Root
- Brand
- Brand
- Brand

Geo-Political
- Bank
- Acquirer

Customer
Merchant
Certificate Revocation Lists (CRLs)

- Signature Algorithm
- Issuer
- Last Update
- Next Update
- Revoked Certificates
  - Signature
  - Serial Number
  - Revocation Date
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
X.509v3 Innovations

- distinguish various certificates
  - signature, encryption, key-agreement
- identification info in addition to X.500 name
  - internet names: email addresses, host names, URLs
- issuer can state policy and usage
  - ok for casual email but not for signing checks
- extensible
  - proprietary extensions can be defined and registered
- attribute certificates
  - to enable attribute-based authorization
• CRL distribution points
• indirect CRLs
• delta CRLs
• revocation reason
• push CRLs
Multiple Root CA’s Plus Intermediate CA’s

Model on the web today
Certificate Triangle

User (Identity)

Attributes

Public-keys + Secured secrets