Authentication for IoT

Sean Turner - turners@ieca.com
Outgoing SEC AD
Many slides copied from Russ Housley
Outline

• Why we’re here: Security Services
• What’s the cost: Key Management
• Techniques:
  – Pre-shared keys
  – Public Key Certificates
  – Key Distribution Centers
• Protocols:
  – Enrollment
  – Status Checks
  – Trust Anchor Update
Security Services (1/2)

- **Integrity**
  - Assurance that the content of the message has not been altered

- **Authentication**
  - Assurance that the stated sender of the message is correct

- **Non-repudiation**
  - Assurance that the original sender of the message cannot deny the message content
Security Services (2/2)

• Confidentiality
  – Assurance that the content can only be read by the intended recipients

• Access Control
  – Assurance that a resource can only be used in an authorized manner
    • Identity-based Access Control
    • Rule-based Access Control
    • Role-based Access Control
Key Management

- Nearly all Internet security protocols make use of cryptography for authentication, integrity, and/or confidentiality.
- Cryptography requires key management.
- Key Management tends to be expensive by any measure:
  - Protocol complexity
  - Infrastructure
  - Processing power
Techniques

• Many key management approaches:
  – Pre-shared keys
  – Public key cryptography
  – Key distribution centers (not covered)

• Each has tradeoff
Pre-shared Keys

• Start with a manually installed secret value
• Use an HMAC (keyed-hash message authentication code) algorithm and shared secret to generate signature value
• If more than one entity has the key it is impossible to determine who sent the message.
• Revocation can be challenging.
Public Key Cryptography

• Avoids manual installation in peers
• Mechanism (next slide)
• Need to identify the party that holds the private key that corresponds to the received public key

• Two primary approaches:
  – Leap of faith
  – Certificates
Digital Signatures

• A one-way hash function is used to create a hash of the data to be signed
• A digital signature is cryptographic transformation of the hash value and the signer’s *private* key
Leap of Faith

• No infrastructure
• Server gives client its public key
  – Man-in-the-middle attack is possible
  – May verify the public key out-of-band
• Client remembers the public key for server
  – If public key changes, the man-in-the-middle is detected
  – Or, did the server just changed its public key
Certificates

- Certificates bind an identity to a public key.
- ASN.1 structured encoded with DER.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERIAL NUMBER</td>
<td>12345</td>
</tr>
<tr>
<td>C=US, O=IECA, Inc.</td>
<td>C=US, O=IECA, Inc. CN=Sean Turner</td>
</tr>
<tr>
<td>VERSION</td>
<td>v1 or v2 or v3</td>
</tr>
<tr>
<td>SIGNATURE ALGORITHM</td>
<td>Signing Algorithm</td>
</tr>
<tr>
<td>ISSUER</td>
<td></td>
</tr>
<tr>
<td>VALIDITY</td>
<td>1/1/14 - 1/1/15</td>
</tr>
<tr>
<td>SUBJECT</td>
<td></td>
</tr>
<tr>
<td>SUBJECT PUBLIC KEY INFO</td>
<td>Key</td>
</tr>
<tr>
<td>ISSUER UNIQUE ID</td>
<td>NOT USED</td>
</tr>
<tr>
<td>SUBJECT UNIQUE ID</td>
<td>NOT USED</td>
</tr>
<tr>
<td>EXTENSIONS</td>
<td></td>
</tr>
<tr>
<td>SIGNATURE</td>
<td></td>
</tr>
</tbody>
</table>
X.509 Certificate Extensions

- Authority Key Identifier
- Subject Key Identifier
- Key Usage
- Private Key Usage Period
- Certificate Policies
- Policy Mappings
- Subject Alternative Name
- Issuer Alternative Name
- Freshest CRL

- Basic Constraints
- Name Constraints
- Policy Constraints
- Extended Key Usage
- CRL Distribution Points
- Inhibit Any-Policy
- Authority Information Access
- Subject Information Access
- Subject Directory Attributes
Certification Authority

• Certificate Authority (CA) establishes and maintains an accurate binding between the public key and attributes contained in a certificate

• Manages certificates throughout their lifetime:
  – Enrollment
  – Certifies
  – Revokes
Certification Paths

• Alice can verify Bob’s certificate by verifying a chain of certificates starting at one issued by a Certification Authority (CA) that she trusts.

• Path building is aided by certain certificate extensions.
Establishing the first key is the most expensive part of key management
  - Basis for trust in the keys

Pre-shared keys
  - Manual installation

Public key cryptography
  - Public key certification
  - Often involves some type of identity check
Enrollment (2/2)

• PKCS #10/#7
  – Request: Name, Attributes, and Public Key all signed
  – Response: “certs-only” CMS (i.e., just the cert)
• CMP (Certificate Management Protocol)
• CMC (Certificate Management over CMS)
• EST (Enrollment over Secure Transport)
Status Checks

• Binding between key and name sometimes needs to be broken (i.e., compromised key)

• Mechanisms:
  – CRLs (Certificate Revocation Lists)
  – OCSP (Online Certificate Status Protocol)
  – SCVP (Server-based Certificate Validation Protocol)
C=US, O=IECA,Inc., CN=OCSP1

20140328180000Z

OCSP

v1

20140508194500Z

Good

20140509080000Z

Nonce = 48

Nonce = 48
SCVP Architecture

Client → Certificate

SCVP Responder

Yes / No

OCSP Responder

X.500 Directory

LDAP Directory

Other ...

• Currently TAs (Trust Anchors) are pretty much universally updated through a software patch.
• TAMP (Trust Anchor Management Protocol) is a protocol that allows TAs to be managed.