Securing IoT Devices on our networks

Eliot Lear
IETF 103
Why is IoT different?
Questions that need answering

- What is this thing?
- Who is responsible for it?
- What access does it need?
- Is it doing what it should be doing?

- What is the device’s identity? Does this particular thing belong on the network?
- What type of thing is it?
- If something breaks, who should be called?
- With which devices should it communicate?
- With which devices is it actually communicating?
- Is it behaving as designed?
Steps needed to get a device to join a network

- Out of the box
- Device learns which network to join
- Provision device to trust network
- Provision network to trust device
- Operational State
Design goal choices

- Correct network selection
- Proof of ownership
- Supply chain security
Basic concept: a voucher (RFC 8366)

module: ietf-voucher

yang-data voucher-artifact:
  +---- voucher
    +---- created-on       yang:date-and-time
    +---- expires-on?      yang:date-and-time
    +---- assertion        enumeration
    +---- serial-number    string
    +---- idevid-issuer?   binary
    +---- pinned-domain-cert binary
    +---- domain-cert-revocation-checks? boolean
    +---- nonce?           binary
    +---- last-renewal-date? yang:date-and-time
Bootstrapping with wired (ANIMA BRSKI)

- Pledge=Device
- Registrar=Store of known devices (tied to AAA infrastructure)
- MASA="Manufacturer Authorized Signing Authority"
- EST – enrollment over secure transport
Client gets a certificate via EST (RFC 7030)
Getting there with wireless

- Use existing management path in the network: EAP
- Keep onboarding capabilities in interface “bring up”
- Reuse as much as possible
draft-lear-eap-teap-brski

Can do EAP-Success here if we recognize local cert
Can skip BRSKI and go right to enroll if we need to re-enroll
Does MASA know lightbulb was sold to Company B?
What if the Internet isn’t there?

SSID="Company A"

SSID="Company B"

MASA
MASA tests proof of ownership

1. Label scanned in

2. Normal voucher request

3. Proof of ownership included
Thing tests proof of ownership

1. Label scanned in

2. Normal voucher request

3. Proof of ownership included

4. Proof of ownership included in response.

Thing

Registrar

MASA
No MASA

1. Label scanned in
2. Voucher request
3. Proof of ownership included
# Approaches to onboarding

<table>
<thead>
<tr>
<th></th>
<th>WPS</th>
<th>Simple Serial #</th>
<th>DPP</th>
<th>BRSKI w/ sales integration</th>
<th>BRSKI no sales integration</th>
<th>BRSKI with POP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct Network Selection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Onboard without Internet access</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Proof of ownership</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes**</td>
<td>Yes***</td>
</tr>
<tr>
<td>Supply chain security</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes***</td>
<td>Partial</td>
</tr>
<tr>
<td>Hands free*</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Well secured</td>
<td>No</td>
<td>Maybe</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Status</td>
<td>Here</td>
<td>Not planned</td>
<td>Std</td>
<td>Partially standardized</td>
<td>Partially standardized</td>
<td>Beginning</td>
</tr>
<tr>
<td>Key type</td>
<td>None</td>
<td>Ser #</td>
<td>Asym.</td>
<td>X.509</td>
<td>X.509</td>
<td>X.509 + private</td>
</tr>
<tr>
<td>Manufacturing complexity</td>
<td>Nvram</td>
<td>Serial#</td>
<td>Public Key + label/BOM</td>
<td>Cert+Back End Integration</td>
<td>Cert</td>
<td>Cert+label/BOM</td>
</tr>
</tbody>
</table>

*Hands free = no label or BOM integration  
**Assumes protection of proof of ownership  
***Assumes Internet access to enterprise AAA at some point
Lines of complexity

Device:
- WPA-2/EAP
- Asymmetric Keys
- Certs

Manufacturing:
- Labels
- Back end sales integration

Deployment Complexity
Key Observation

• All of this revolves around a formal assertion handed to the device—a voucher

• Making the voucher extensible for different forms of authentication/pop seems ideal
Questions

• Which methods should we standardize?
  • Thing tests proof of ownership
  • MASA test proof of ownership
  • No MASA involved

• Can manufacturers reasonably use...
  • 802.1X?
  • EAP-TLS/EAP-TEAP?
  • X.509 Certificates?
  • COSE/JOSE objects?

• Can we merge some of these capabilities with EAP-NOOB?
Drafts

- draft-ietf-anima-bootstrapping-keyinfra-16 (core draft)
- draft-friel-anima-brski-over-802dot11-01 (some options)
- draft-lear-eap-teap-brski-01 (BRSKI over EAP)
- draft-lear-brski-pop-00 (proof of possession)