About the Bootstrapping of Security in IoT

Oliver Pfaff
The Challenge

- Lifecycle of a thing (WoT/IoT/OT):
  - Manufacturing phase
    - Manufactured
  - Bootstrapping phase
    - Installed
    - Commissioned
  - Operational phase
    - (Devices) started
    - Application running
  - Maintenance phase
    - Updated
    - Application reconfigured
  - Off-boarding phase
    - Decommissioned
    - Removed and replaced
    - Re-owned

...and may be here too

...so something has to happen here
There is no *out-of-the-nothing* security

We want the thing to interact securely here
Thing-to-thing, thing-to-service, service-to-thing...
Common Practices

• What solution properties do we find today - with respect to the bootstrapping of security?
  • Easy-to-use but not (really) secure: naïve security (e.g. shared credentials) or no security at all
  OR
  • Secure but not easy-to-use: tedious handling, manual processing steps…

• What do we not yet find?
  • Easy-to-use AND secure
Not Yet Championed Task

- The overall **security challenge**: IoT component and site shall establish mutual trust
- Is comprised of following tasks:
  a) Site authenticates and authorizes the IoT component: *What is this component? Do I want it?*
  b) IoT component authenticates and authorizes the site: *What is this site? Should I join it?*
- Their hardness differs:
  a) is moderate; can be solved by using known recipes
  b) is hard and is **not yet solved** esp. when this task shall be done without manual intervention at the thing
Relevant Initiatives

- Anima (IETF WG, BSRKI/EST)
- 6tisch Zero Touch (IETF WG Draft)
- 6tisch Minimal Security (IETF WG Draft)
- Netconf SZTP (IETF WG Draft)
- …(not meant to be an exhaustive list)

Their trick: *let somebody else* (manufacturer service) do the hard task
Takeaways

- Bootstrapping security is a **key concern** in WoT/IoT/OT. It is not yet championed to a full extent.
- Important **innovations** and **adoptions** are happening right **now**, on international level e.g. the [IETF Anima](https://www.ietf.org/search?query=Anima) working group, the [Fairhair Alliance](https://fairhairalliance.org) or the [Thread Group](https://www.threadgroup.org/)
- The emerging IETF Anima solution is in a leading position. It allows to **do more** than just security bootstrapping.
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anima</td>
<td>Autonomic Networking Integrated Model and Approach</td>
</tr>
<tr>
<td>Authn</td>
<td>Authentication</td>
</tr>
<tr>
<td>Authz</td>
<td>Authorization</td>
</tr>
<tr>
<td>BRSKI</td>
<td>Bootstrapping Remote Secure Key Infrastructures</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CoAP</td>
<td>Constrained Application Protocol</td>
</tr>
<tr>
<td>coaps</td>
<td>Access scheme for CoAP-over-DTLS</td>
</tr>
<tr>
<td>(D)TLS</td>
<td>TLS or DTLS</td>
</tr>
<tr>
<td>DTLS</td>
<td>Datagram Transport Layer Security</td>
</tr>
<tr>
<td>EE</td>
<td>End Entity</td>
</tr>
<tr>
<td>EST</td>
<td>Enrollment over Secure Transport</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>https</td>
<td>Access scheme for HTTP-over-TLS</td>
</tr>
<tr>
<td>IDevID</td>
<td>Initial Device IDentifier</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>LDevID</td>
<td>Locally significant Device IDentifier</td>
</tr>
<tr>
<td>MASA</td>
<td>Manufacturer Authorized Signing Authority</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Technology</td>
</tr>
<tr>
<td>SZTB</td>
<td>Secure and Zero-Touch Bootstrapping</td>
</tr>
<tr>
<td>SZTP</td>
<td>Secure and Zero-Touch Provisioning</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
</tbody>
</table>
References

Oliver Pfaff
Siemens AG
CT RDA ITS
oliver.pfaff@siemens.com

siemens.com
Architectural Patterns

- **Site-facing** manufacturer services:
  - The manufacturer does authenticate and authorize (3rd party) sites i.e. the users of its IoT components through this service
  - This requires interoperability, local-area network connectivity is sufficient for IoT components
  - It allows to support site/user-aware use cases e.g. SZTB and CRM

- **IoT component-facing** manufacturer services:
  - The manufacturer does authenticate (own) IoT components through this service
  - This requires wide-area connectivity, DIY services sufficient
  - It allows to support site/user-unaware use cases e.g. component maintenance
Doing the SZTB Trick with **IETF Anima**

- **Moderate task a)** is addressed by a **site service**. It authenticates and authorizes the IoT component using (D)TLS with manufacturer credentials (called IDevID) plus information about acceptance.

- **Hard task b)** is solved by an indirection: a **manufacturer service** is introduced that authenticates and authorizes the site and reports about this to the IoT component, see [5].
Anima System Architecture
Anima Swim-Lane

[discover]
- <RFC4862 IPv6 addr
- <RFC3927 IPv4 addr
- optional: mDNS query
- GRASP M_FLOOD
  periodic broadcast

[identity]
- TLS via the Join Proxy
- <Register TLS server authentication
- [PROVISIONAL accept of server cert]
- P --- X.509 client authentication

[request join]
- P --- Voucher Request(w/nonce for voucher) -> P
  [accept device?]
  [contact Vendor]
  -- Pledge ID -------->
  -- Domain ID -------->
  -- optional nonce -->
  [extract DomainID]
  [update audit log]
  optional: can occur in advance
  if nonces less
  P
  \------------------------------------>
  <- voucher ----------------
    w/nonce if provided

[imprint]
--- voucher status telemetry ---
 <- device audit log--
  [verify audit log and voucher]

[enroll]
Continue with RFC7030 enrollment
using now bidirectionally authenticated
TLS session.
[enrolled]
Current Blind Spots of Anima

- Blueprints for site-facing manufacturer services emerge right now ➔ do expect to get a core; not yet expect fully-blown specifications covering all possible aspects
- The current IETF Anima specifications come with white-spots and limitations including:
  - **Site-facing services**: assuming manufacturers to provide site-facing services
  - **Brown-field friendliness**: the current addressing scheme is not adequate for manufacturers with many, small pools of unique product serial numbers
  - **Sustainability**: service API versioning is not yet covered, message objects are self-contained but do not embody information about their structure
  - **Scalability**: bulk operation modes are not yet supported
  - **Unified credentialing**: supplying multiple, site-specific credentials that are bound to dedicated application domains to one IoT component can be accommodated but this is not yet profiled or detailed