Capabilities and Expectations Working Group

NTIA Multistakeholder Process on IoT Upgradability and Patching
July 18, 2017 Meeting
Capabilities WG Overview

• Desired Outcomes:
  – A shared understanding of the component steps in an update, including a baseline for security purposes

• Draft Document Status
  – Basic Steps in an Illustrative Over-the-Air Update Process
  – Security features for each step, including basic steps and layers of enhancement

• Goals and audience
  – Voluntary, nonregulatory guidance
  – Update mechanisms should not introduce new security risks
  – Aimed at IoT manufacturers, solution implementers, system integrators, and those who deploy and maintain systems
WG2 Summary of Activity

• Initially pursued two tracks: device categories and the steps of an update
  – Goal: mapping between update steps and necessary tech/capabilities of that device and its supporting systems
  – Reviewed a wide range of device categories, capabilities, and use cases
  – Considered a metric for update security
  – Decided for the moment that a better operative goal was to understand the nature of an update (software or firmware), and the security features of those updates.

• Steps in an update that might apply to a very wide range of devices
• Security features to secure this update process
• Scoping:
  – Connected, remotely addressable devices (as opposed to non-connected devices)
  – The development of the update by manufacturer is out of scope.
Basic Steps
An Illustrative OTA Update Process

0. **Create** – Update image created.
   Important, but out of scope for guidelines.

1. **Sign** – Ensure update integrity.
   Update is signed.

2. **Protect** – Prevent update exposure.
   Update is encrypted/obfuscated.

3. **Send** – Data is in motion.
   Update is communicated to target.

4. **Receive** – Update is received.
   Target receives update deliverable.

5. **Check** – Update is processed.
   Target validates, decrypts, and processes update deliverable as needed.

6. **Announce** – User made aware.
   End user notified about/approves of update installation.

7. **Distribute** – Image distributed.
   Update parsed/distributed to hardware targets (e.g. CPU, FPGA).

8. **Process** – Image is processed.
   Target hardware receives, validates, and decrypts update.

9. **Stage** – System in pre-update state.
   System-specific pre-update activities.

10. **Apply** – Update process triggered.
    Actual image install process is run.

11. **Re-verify** – Post-update verification.
    Target validates integrity of install and communicates results (if needed).

12. **Activate** – Updated code enabled.
    New code begins execution if verified.

13. **Clean-up** – Post-update activities.
    System –specific verification, messaging, and clean-up. (Could be negative.)
Security Features Mapping

Basic

1. **Sign** – Ensure update integrity.
   128-bit hash.

2. **Protect** – Prevent update exposure.
   Ephemeral, unique AES-128 keys in device.

3. **Send** – Data is in motion.
   No special assumptions.

4. **Receive** – Update is received.
   No special assumptions.

5. **Check** – Update is processed.
   Hash validation, decryption w/ per-device keys.

6. **Announce** – User made aware.
   Optional end-user approval.

7. **Distribute** – Image distributed.
   No special assumptions.

8. **Process** – Image is processed.
   Target hardware validates, decrypts image.

9. **Stage** – System in pre-update state.
   Manufacturer defined.

10. **Apply** – Update process triggered.
    Actual image install process is run.

11. **Re-verify** – Post-update verification.
    Target hardware validates installed material.

12. **Activate** – Updated code enabled.
    No special assumptions.

13. **Clean-up** – Post-update activities.
    No special assumptions.
Security Features Mapping
Upgraded (+1)

1. **Sign** – Ensure update integrity.
   NIST key management for hashing.

2. **Protect** – Prevent update exposure.
   NIST key management for decryption.

3. **Send** – Data is in motion.
   Cryptographic endpoint verification (e.g. challenge/response) before update.

4. **Receive** – Update is received.
   Best practices (e.g. TLSv1.2, certificate pinning)

5. **Check** – Update is processed.
   See Basic.

6. **Announce** – User made aware.
   See Basic.

7. **Distribute** – Image distributed.
   Encrypted in motion; can target multiple layers.

8. **Process** – Image is processed.
   Target validation, decryption with AES-256.

9. **Stage** – System in pre-update state.
   See Basic.

10. **Apply** – Update process triggered.
    Optional synchronous updating, end-user coordination, and data persistence.

11. **Re-verify** – Post-update verification.
    Install validated w/hash (AES-256), checksum (CRC-16).

12. **Activate** – Updated code enabled.
    See Basic.

13. **Clean-up** – Post-update activities.
    Local success notification; external logging of successful updates (including ID, versioning).
Security Features Mapping
Enhanced (+2)

1. **Sign** – Ensure update integrity.
   *Upgraded (+1)*, plus secure memory and PKI.

2. **Protect** – Prevent update exposure.
   *Upgraded (+1)*, plus secure memory and PKI.

3. **Send** – Data is in motion.
   *Upgraded (+1)*, plus PKI.

4. **Receive** – Update is received.
   Best practices (e.g. TLSv1.3, certificate pinning)

5. **Check** – Update is processed.
   See Basic.

6. **Announce** – User made aware.
   See Basic.

7. **Distribute** – Image distributed.
   See Upgraded (+1).

8. **Process** – Image is processed.
   See Upgraded (+1).

9. **Stage** – System in pre-update state.
   See Basic.

10. **Apply** – Update process triggered.
    See Upgraded (+1).

11. **Re-verify** – Post-update verification.
    See Upgraded (+1).

12. **Activate** – Updated code enabled.
    See Basic.

13. **Clean-up** – Post-update activities.
    See Upgraded (+1).
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Basic</th>
<th>+1 (&quot;Upgraded&quot;)</th>
<th>+2 (&quot;Enhanced&quot;)</th>
<th>+3 (&quot;Quantum&quot;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Create</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Sign</td>
<td>Update signed.</td>
<td>128-bit hash.</td>
<td>NIST key management for hashing.</td>
<td>Secure memory, PKI.</td>
</tr>
<tr>
<td>2</td>
<td>Protect</td>
<td>Encryption and/or obfuscation</td>
<td>Ephemeral, unique AES-128 keys in device.</td>
<td>NIST key management for decryption.</td>
<td>Secure memory, PKI.</td>
</tr>
<tr>
<td>3</td>
<td>Send</td>
<td>Communicated to target device.</td>
<td>No special assumption.</td>
<td>Endpoint verification</td>
<td>PKI.</td>
</tr>
<tr>
<td>4</td>
<td>Receive</td>
<td>Target device receives update.</td>
<td>No special assumption.</td>
<td>Best practices (e.g. TLSv1.2, cert. pinning)</td>
<td>TLSv1.3.</td>
</tr>
<tr>
<td>5</td>
<td>Check</td>
<td>Target validates, decrypts, and processes as needed.</td>
<td>Validation, decryption w/per-device keys.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Announce</td>
<td>End-user notified about / approves update install.</td>
<td>Optional end-user approval</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Distribute</td>
<td>Image parsed, distributed to HW targets (e.g. CPU, FPGA).</td>
<td>No special assumption.</td>
<td>Encrypted in motion; can target multiple layers.</td>
<td>SHS-256 or Lamport.</td>
</tr>
<tr>
<td>8</td>
<td>Process</td>
<td>Hardware target receives, validates, and decrypts image.</td>
<td>Target hardware validates, decrypts.</td>
<td>Target validation, decryption w/ AES-256.</td>
<td>Target and image validation w/ AES-256.</td>
</tr>
<tr>
<td>9</td>
<td>Stage</td>
<td>System-specific pre update tasks.</td>
<td>Manufacturer defined.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Apply</td>
<td>Image install process runs.</td>
<td>No special assumption.</td>
<td>Opt. update and end-user coordination, data persistence.</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Re-verify</td>
<td>Install integrity check; optional communication of results.</td>
<td>Install results validated.</td>
<td>Validated with hash, checksum.</td>
<td>Minimum CRC-16 checksum and AES-256 hash.</td>
</tr>
<tr>
<td>12</td>
<td>Activate</td>
<td>New code executes if verified.</td>
<td>No special assumption.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Clean-up</td>
<td>System-specific: verification, messaging, and cleanup.</td>
<td>No special assumption.</td>
<td>Local notification and external logging of update.</td>
<td></td>
</tr>
</tbody>
</table>