Survivable IoT Edge: Lightweight Attestation and Recovery for Tiny / COTS IoT

Steffen Schulz, André Schaller, Florian Kohnhäuser

- Novel “Boot Attestation” technology for tiny/low-cost IoT
- E2E secure Device Management with Remote Attestation & Sealing
- Zero-touch Provisioning and Exploit Recovery

New Attestation Scheme for Tiny/Edge IoT
- Automotive ECU, smart factory, home automation
- USB sticks, SD card, keyboard, BLE gadgets

Basic Idea: Commit Measurements as we Boot

Owner / CA

Intel – SAP Predictive Maintenance Scenario
- Monitoring of city-wide gas distribution network
- Optimize spending on maintenance, replacements
- Critical infrastructure, privacy-sensitive data

Prototype Implementation & Results
- Intel Curie (Quark C1000) + TI Stellaris (Cortex-M4F)
- Real Root of Trust & Key Protection
- Very efficient, supports many MCUs

Minimal Hardware Requirements
- Lock-able Boot ROM (e.g. OTP Flash)
- Lock-able Key Storage (e.g. EEPROM, lock bits)

Lightweight Provisioning and Recovery
- Fresh storage/auth. keys for each firmware update

Extension for Attesting to Third Parties
- Turn Platform Owner into Attestation CA
- Distribute Akpub for valid hash/device combinations

Related Work
- Boot Attestation: Secure Remote Reporting with COTS IoT Sensors (in submission)
- BadUSB – On Accessories that turn evil, Nohl et.al. BlackHat USA’14
- SMART Attestation, Eldefrawy et al. (NDSS 2012)
- TrustLite Security Architecture, Koeberl et al. (EuroSys12)

<table>
<thead>
<tr>
<th>Implementation Overhead</th>
<th>Intel Quark</th>
<th>ARM Cortex-M4</th>
</tr>
</thead>
<tbody>
<tr>
<td>ROM RoT</td>
<td>2.6 kB</td>
<td>3.1 kB</td>
</tr>
<tr>
<td>(HMAC-SHA256 &amp; Key Protection)</td>
<td>1.5 ms</td>
<td>3 ms</td>
</tr>
<tr>
<td>LoRa Trusted Channel</td>
<td>4.5 kB</td>
<td>-</td>
</tr>
<tr>
<td>(ECDH &amp; ECDSA)</td>
<td>2.1s</td>
<td>-</td>
</tr>
</tbody>
</table>

Supported devices:
- Intel Quark D2000
- Intel Quark C1000
- Stellaris Launchpad
- Atmega328p
- PIC16F1825
- MSP430G5338

Intel CRI for Secure Computing

Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
*Other names and brands may be claimed as the property of others.