Microcontroller-based IoT systems (IoT-μCs)
A significant portion of the IoT.
- Examples:
  - WiFi SoC.
  - Amazon Dash Button.
- Traditionally an isolated system with no network connectivity.
- Suffers from poor security practices.
- Increasingly under attack with the rise of IoT.

Benchmarking Challenges
- External events are hard to reproduce.
- Peripherals excluded for portability.
- No Connectivity

Evaluation Challenges
- IoT-μCs are constrained systems with limited Flash, RAM, and Energy.
- Evaluation is limited, manual, and tedious.
- Evaluation often depend on additional hardware.
- Security evaluation became ad-hoc as a result.

Evaluation metrics
- Security
  - Total Privileged cycles
  - Privileged Thread cycles
  - SVC cycles
  - Max. code region ration
  - Max. data region ration
  - DEP
  - # of ROP gadgets
  - # of indirect calls
- Performance & Energy
  - Total runtime cycles
  - CPU sleep cycles
  - Total Energy
- Memory
  - Slack+Heap usage
  - Total RAM usage
  - Total Flash usage
- Our Solution: IoT2
  - External events are triggered in software and are reproducible.
  - Benchmarks are portable and Peripherals are utilized.
  - Realistic IoT applications
  - Automated Evaluation

Benchmarks
<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Task Type</th>
<th>Peripheral</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Light</td>
<td>✓</td>
<td>Low-power Timer, GPIO, Real-time clock</td>
</tr>
<tr>
<td>Smart Thermostat</td>
<td>✓ ✓</td>
<td>ADC, Display, GPIO, uSD Card</td>
</tr>
<tr>
<td>Smart-locker</td>
<td>✓ ✓</td>
<td>Serial (UART), Display, uSD Card, Real-time clock</td>
</tr>
<tr>
<td>Firmware Updater</td>
<td>✓ ✓</td>
<td>Flash in-application programming</td>
</tr>
<tr>
<td>Connected Display</td>
<td>✓ ✓</td>
<td>Display, uSD Card</td>
</tr>
</tbody>
</table>

Security Evaluation
<table>
<thead>
<tr>
<th>Defense</th>
<th>Memory Isolation and Code injection Metrics</th>
<th>Max code Reg. ratio</th>
<th>Max data Reg. ratio</th>
<th>DEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mbed-uvisor</td>
<td>1.0 1.0 &lt;x&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Attestation (OS)</td>
<td>0.99 1.0 ✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Integrity (OS)</td>
<td>1.0 0.99 &lt;x&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Integrity (bare-metal)</td>
<td>1.0 0.99 &lt;x&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Code Reuse Protection

Privileged Execution Minimization

Performance

Energy

Memory

Our Team