IETF 108 TEEP Hackathon Report

Isobe Kohei, TRASIO/SECOM
Akira Tsukamoto, AIST
Agenda

• Hackathons on TEEP
  • SUIT Manifest in TEEP
  • Encrypted TA binaries for TEEP
  • TAM and TEEP Agent using SUIT Manifest
  • Current TEEP implementations list
  • TEEP-Device status on RISC-V
Hackathons

• IETF Hackathon (7.20-7.24)
  • No Hackathons

• SUIT Hackathon (7.13)
  • https://trac.ietf.org/trac/suit/wiki/SuitHackathon
  • 3 projects related with teep
    • Use of SUIT Manifest in TEEP (Dave Thaler)
    • Encrypted TA binaries (Hannes Tschofenig)
    • TAM and TEEP Agent using SUIT Manifest (Yuichi Takita)
TAM and TEEP Agent using SUIT Manifest
(Yuichi Takita)

• What we planned
  • Add SUIT implementation to TEEP implementations
    • Both sides: TEEP Device (libteep) and TAM Server (tamproto)

• What we achieved
  • Implementation of handling TEEP-P messages with static SUIT Manifest
    • Make an example TrustedAppInstall message with SUIT Manifest
    • Success to sign, verify, decode the message

• What we learned
  • Need for more examples of TEEP-P message and SUIT Manifest
    • Especially TA depending on other TA
Current TEEP implementations list

• TEEP Device
  • TEEP-device (C/C++)
  • Dave’s implementation (C/C++)
  • Hannes’s implementation (C)
  • libteep (C)
    • https://github.com/yuichitk/libteep

• TEEP Server (TAM)
  • Dave’s implementation (C/C++)
  • Hannes’s implementation (Java)
  • tamproto (NodeJS)
    • https://github.com/ko-isobe/tamproto
AIST have been working on TEEP-device prototype

- At IETF hackathon and Securing the IoT (SIoT) Hackathon in the past.
- Initial prototype was on ARM dev boards.
- Ported to OP-TEE QEMU.
- Porting to RISC-V QEMU (RV64GC).
- All in C/C++ language
TEEP-device status on RISC-V (2/2)

• Current status

Talk at RISC-V Global Forum
September 3, 2020
## Hackathon Members

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Akira Tsukamoto</td>
<td>AIST</td>
</tr>
<tr>
<td>Kuniyasu Suzaki</td>
<td>TRASIO/AIST</td>
</tr>
<tr>
<td>Kohei Isobe</td>
<td>TRASIO/SECOM</td>
</tr>
<tr>
<td>Dave Thaler</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Hannes Tschofenig</td>
<td>ARM</td>
</tr>
<tr>
<td>Yuichi Takita</td>
<td>SECOM</td>
</tr>
<tr>
<td>Masashi Kikuchi</td>
<td>TRASIO/Lepidum</td>
</tr>
<tr>
<td>Takahito Nagata</td>
<td>TRASIO/Lepidum</td>
</tr>
<tr>
<td>Tsukasa OI</td>
<td>TRASIO</td>
</tr>
<tr>
<td>Brendan Moran</td>
<td>ARM</td>
</tr>
<tr>
<td>Koen Zandberg</td>
<td>RIOT</td>
</tr>
<tr>
<td>Michael Richardson</td>
<td></td>
</tr>
</tbody>
</table>

This presentation of hackathon is based on results obtained from a project commissioned by the New Energy and Industrial Technology Development Organization (NEDO).