IETF 106
TEEP Hackathon Report

Akira Tsukamoto, Nov. 19, 2019
What we planned

• Open Trust Protocol:
  • Evaluate OTrPv1 vs TEEP (aka OTrPv2) proposal
  • Test implementations of OTrP-over-HTTP
    • draft-ietf-teep-otrpv-over-http-02

• Brought prototypes of TAM and TEEP device
  • TAM with node-js by Isobe-san
  • TAM with SGX by Dave Thaler
  • TEEP device on OP-TEE by Akira Tsukamoto
  • TEEP device on SGX by Dave Thaler
Great TEEEm ^
What got done

• First time to interop OTrP/TEEP protocol implementations built from specs.
  • See pictures on following pages.
On the Table
TAM`s UI for uploading TA
TEEP device
Hacking, Debugging!
TEEP Device installing TA
What we learned

• Filed issues
  • draft-ietf-teep-otrp-over-http-03
    • #5: demuxing TEEP vs OTrP
  • draft-tschofenig-teep-protocol-00.txt
    • Would like to have JSON example

• A lot of implementation action items
  • Prerequisite required for OTrP/TEEP
    • HTTP, JSON, CBOR stack must be completely working
  • Understand TEE concepts, such as SGX, Arm TrustZone, knowledge of implementation details (e.g. OP-TEE)
What went well

• Constructing stand alone wired network on Hackathon table for TAMs and TEEP devices but having uplink
  • This will prevent harming IETF network when sending broken packets.
  • My TEEP device needs to talk to ntp, since does not have RTC.
• Cross checking different TAMs and different TEEP device OTrP messages.
  • Dave`s TAM even sends back what was wrong in the message in the http response. e.g. Content-length missing etc.
• Able to come up for the future plan.
Future consideration

• How to make it easier to implementation TEEP system?
• What to do for reference implementation?
  • At the hackathon, I started of OTrP debugging and end up debugging http header and json parser.
• IDE Development environment for TA on TEE?

• Many selections for hardware and software stack for TEEP
  • Which hardware?
  • Which software stack to use on TEEP device?
    • JSON stack
    • HTTP stack
    • Crypto stack for TLS and JWE, JWS
    • CBOR parser
Hardware recommendation

• Reference TAM machine
  • Recommending IBM PC compatible machine?
  • Any other hardware requirement?

• Reference TEEP device (IoT device, Edge device and etc)
  • Recommended device for each Intel, ARM, RISC-V.
    • ARM, OP-TEE usable device
      • Raspberry Pi 3B (Cortex A53) or later?
    • Intel, SGX usable device
      • Laptop PC? (not all SGX usable)
    • RISC-V, PMP extension usable device
      • HiFive Unleashed? (the device only exist at the moment)
Software stack recommendation

• TAM
  • HTTP stack: Apache
  • JSON stack: Node.js
  • Crypto: openssl
  • CBOR: ?

• TEEP device (limited hardware performance)
  • rootfs: buildroot, Yocto/OE, openwrt?
  • HTTP stack: libwebsocket?
  • JSON stack: libwebsocket?
  • Crypto(TLS,JWE,JWS): openssl, LibreSSL, mbedTLS, wolfSSL, s2n?
  • CBOR: ?
Nice to have? Or out of scope?

• TEEP: Testbed on Internet
  • TAM: Everybody connecting from their own TEEP devices
• IDE Development environment for TA on TEE
  • OpenEnclave

• Hosting github for TEEP reference implementation?

• TAM: security hardware
  • SGX: Any other? OpenTitan?
• TEEP: security hardware
  • Any other? Azure Sphere IoT?
My notes from hackathon

- Fix header for HTTP compliant
  - I broke the HTTP header when revising OTrP messages.
- Add JSON parsing for every packet received
- Cleanup and dependency fix of Makefile
  - It does not detect some dependency when I change some of the code.
- microUSB cable for flashing bootloader
  - Suffered a lot of having bad connection, have to change both the 3D printed case and cable.
- Add dumping the all content of http packet every time
  - To reduce the time using wireshark.
- Buy reliable self-powered USB-hub.
  - One of the hub did not recognize the gpio board.
Wrap Up

Team members:

Akira Tsukamoto
Kuniyasu Suzuki
Kohei Isobe
Dave Thaler
Hannes Tschofenig
Nancy Cam-Winget

https://trac.tools.ietf.org/wg/teep/

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