「IETF 106 TEEP Hackathon レポート」

2020年1月9日

塚本　明[1]、須崎　有康[1, 2]

[1] 産業技術総合研究所（AIST）

[2] セキュアオープンアーキテクチャ・エッジ基盤技術研究組合（TRASIO）

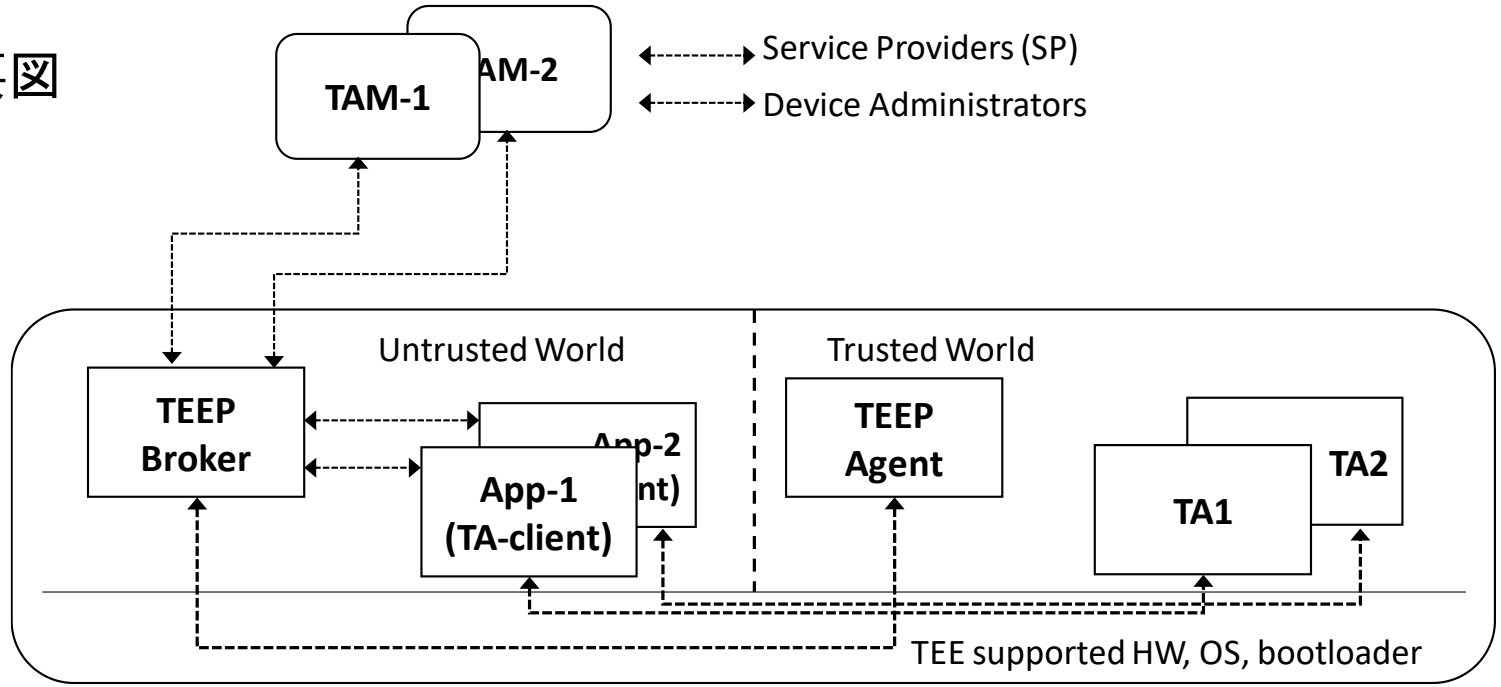
目次

- TEEP とは
- 前回の TETF 105 から 106 までの更新点
- IETF 106 TEEP Hackathon の内容
  - 教訓
  - うまくいったこと
  - 今後の課題
- 次回の IETF 107 に向けて
- まとめ

Trusted Execution Environment Provisioning(TEEP) とは

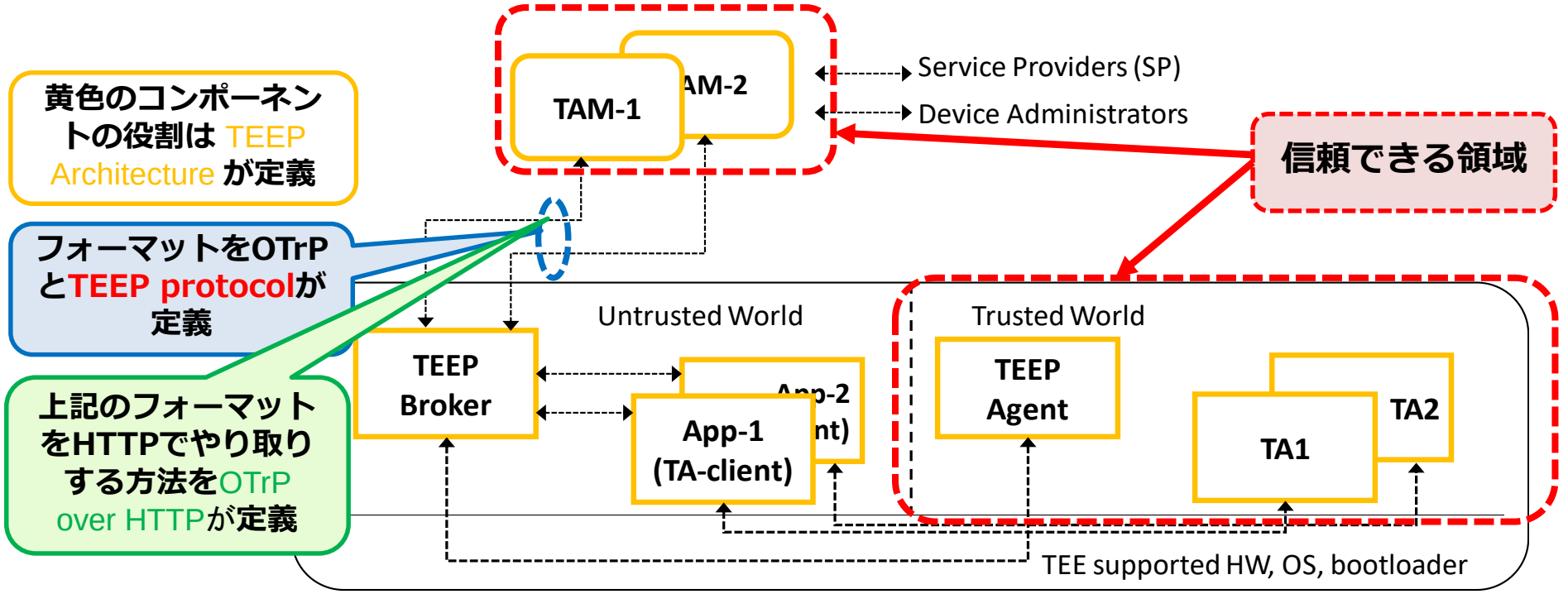
- 信用できないかもしれないデバイスで、Service Provider が開発したTrusted Application (TA)をインストール・ 実行・削除（TAのライフサイクル管理）のセキュリティーを担保する方式の定義と標準化を目的としている。
- 本目的のためにハード的に TA を隔離実行できるTrusted Execution Environment (TEE) 機能を活用する。

概要図



TEEP の各ドラフトの関係

- TEEP Architecture, OTrP, TEEP protocol, OTrP over HTTPの守備範囲 (赤字は新規のドラフト)
  - TEEP Architecture ドラフトで策定するのは、TAM(Trusted Application Manager), TEE broker, TEE Agent, App, TA などの役割。下図のボックス部分
  - OTrPとTEEP protocol ドラフトで策定するのは上記のTAMとTEEP Broker間がやり取りするフォーマット。
  - OTrP over HTTP ドラフトはTAMとTEEP Broker 間のメッセージを HTTP に乗せる方法を策定。



前回の IETF 105 から

- Dave Thaler が TEEP WG の Chair から降りて RFC ドラフトの Author に専念することに
- RFC の議論は主に github で行われるようになった。
  - 議論がすべて可視化されることで議論が活発化、RFC のドラフトの更新効率がよくなった。
- ドラフト OTrPv2 が大幅更新
  - 名前が OTrPv2 から TEEP Protocol に変更。OTrP とメッセージフォーマットの互換性が無くなったため。
  - https://github.com/ietf-teep/teep-protocol
- ドラフト TEEP architecture の更新
  - 一つのデバイスにTEEが複数ある場合、TAMが複数ある場合、TEEP Brokerの役割明確化など、実適応をより考慮した内容に。ほぼ書き直しに近い状況。
  - Trust Anchor は SGX と ARM TrustZone をそのまま利用する前提に。
  - https://github.com/ietf-teep/architecture
- ドラフト OTrP は微調整
  - https://github.com/ietf-teep/OTrP

IETF 106 TEEP Hackathon メンバー

- Dave Thaler (Microsoft)
  - SUIT WG の Chair、Open Enclave 開発リーダー、OTrP over HTTP の Author
  - TAM サーバーを持ち込む
- Hannes Tschofenig (ARM)
  - TEEP protocol の Author
- 磯部さん（セコム）
  - TAM サーバーを試作し持ち込む
- 須崎、塚本（産総研）
  - TEEP device を試作し持ち込む
- Nancy Cam-Winget（Cisco）
  - TEEP WG の Chair

What we planned

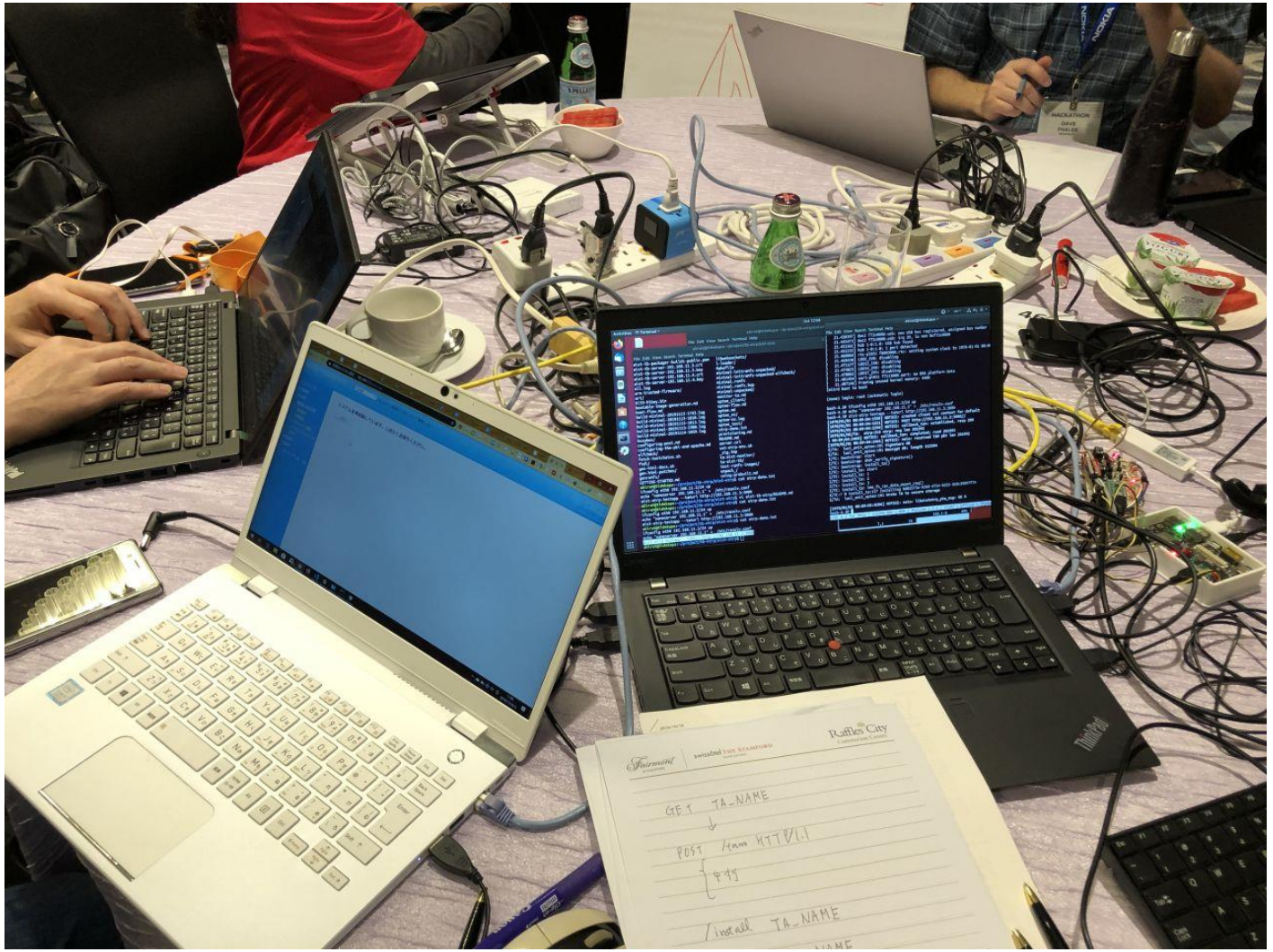
- Open Trust Protocol:
  - Evaluate OTrPv1 vs TEEP (aka OTrPv2) proposal
  - Test implementations of OTrP-over-HTTP
    - draft-ietf-teep-otrp-over-http-02

- 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

What got done

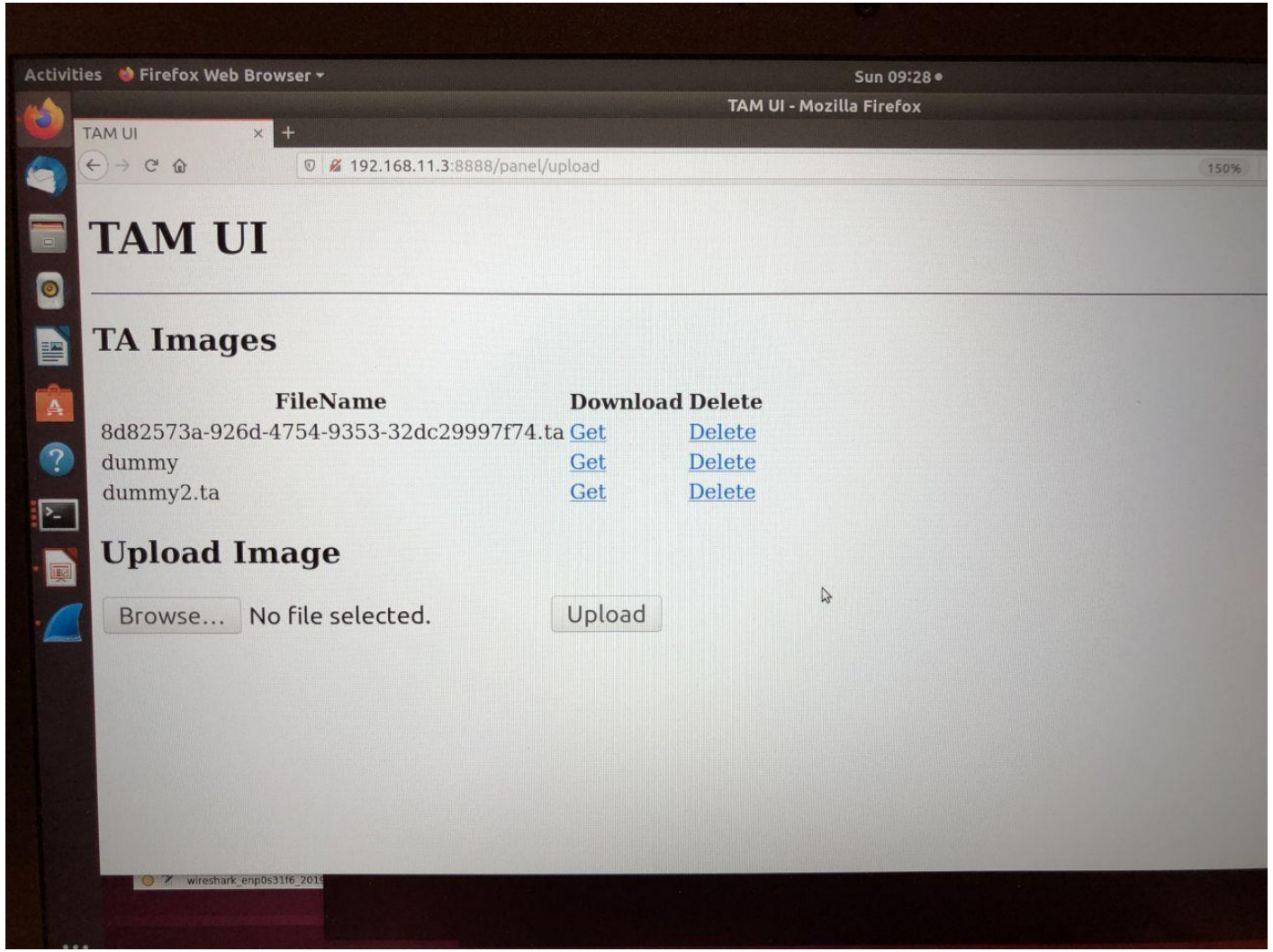
- First time to interop OTrP/TEEP protocol implementations built from specs.
  - See pictures on following pages.

On the Table

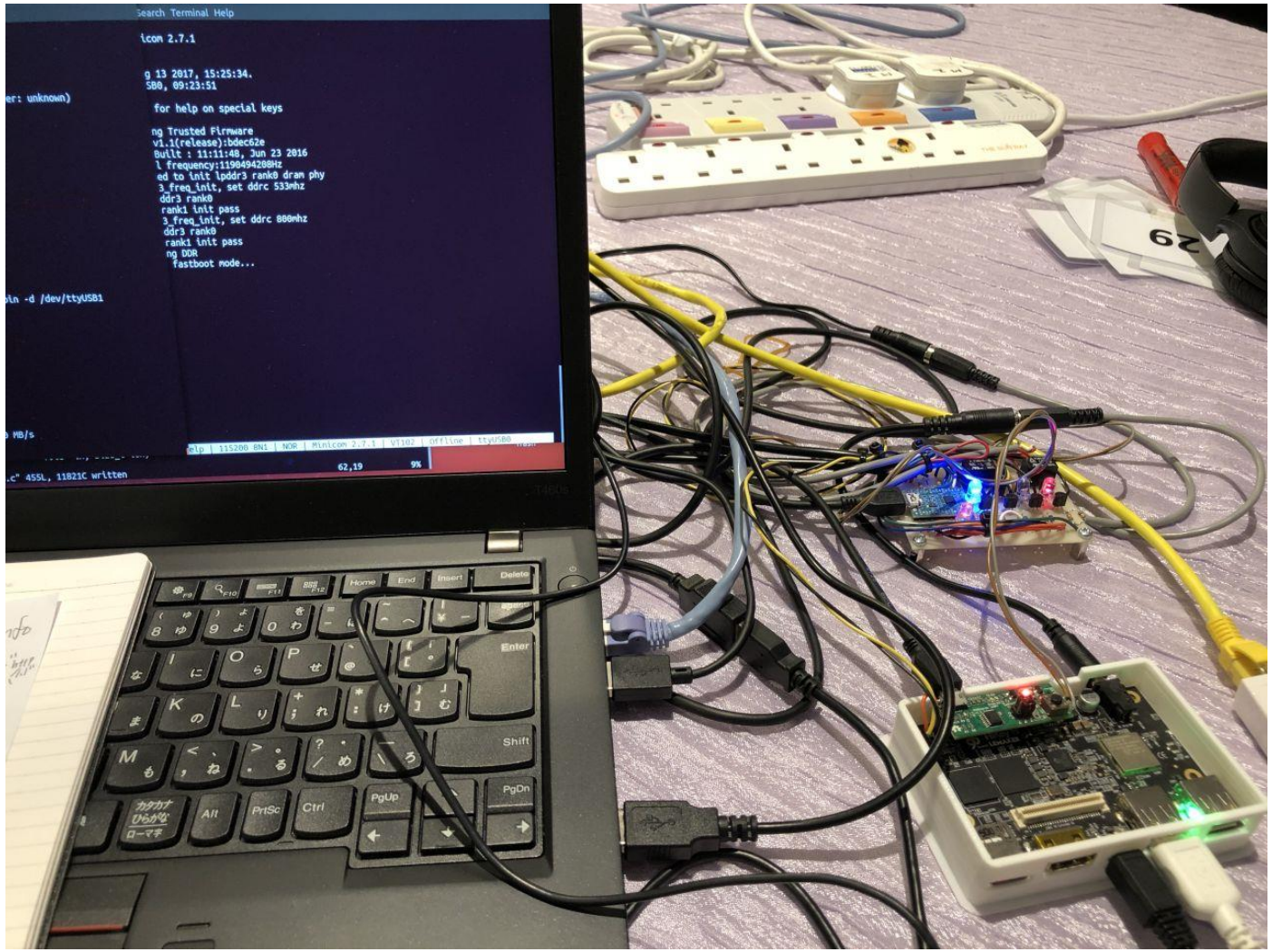


TAM`s UI for uploading TA

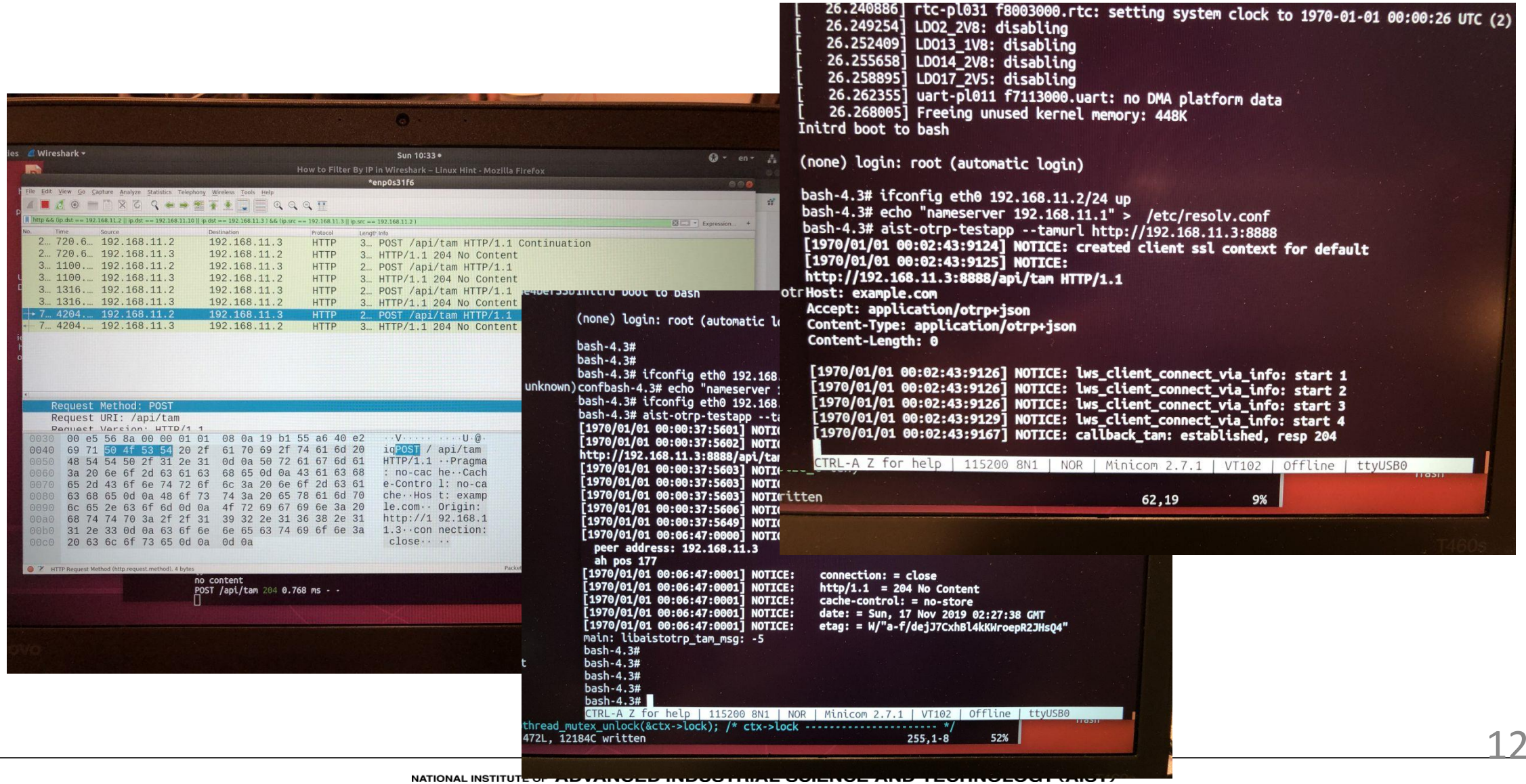
磯部さん（セコム）
試作 TAM



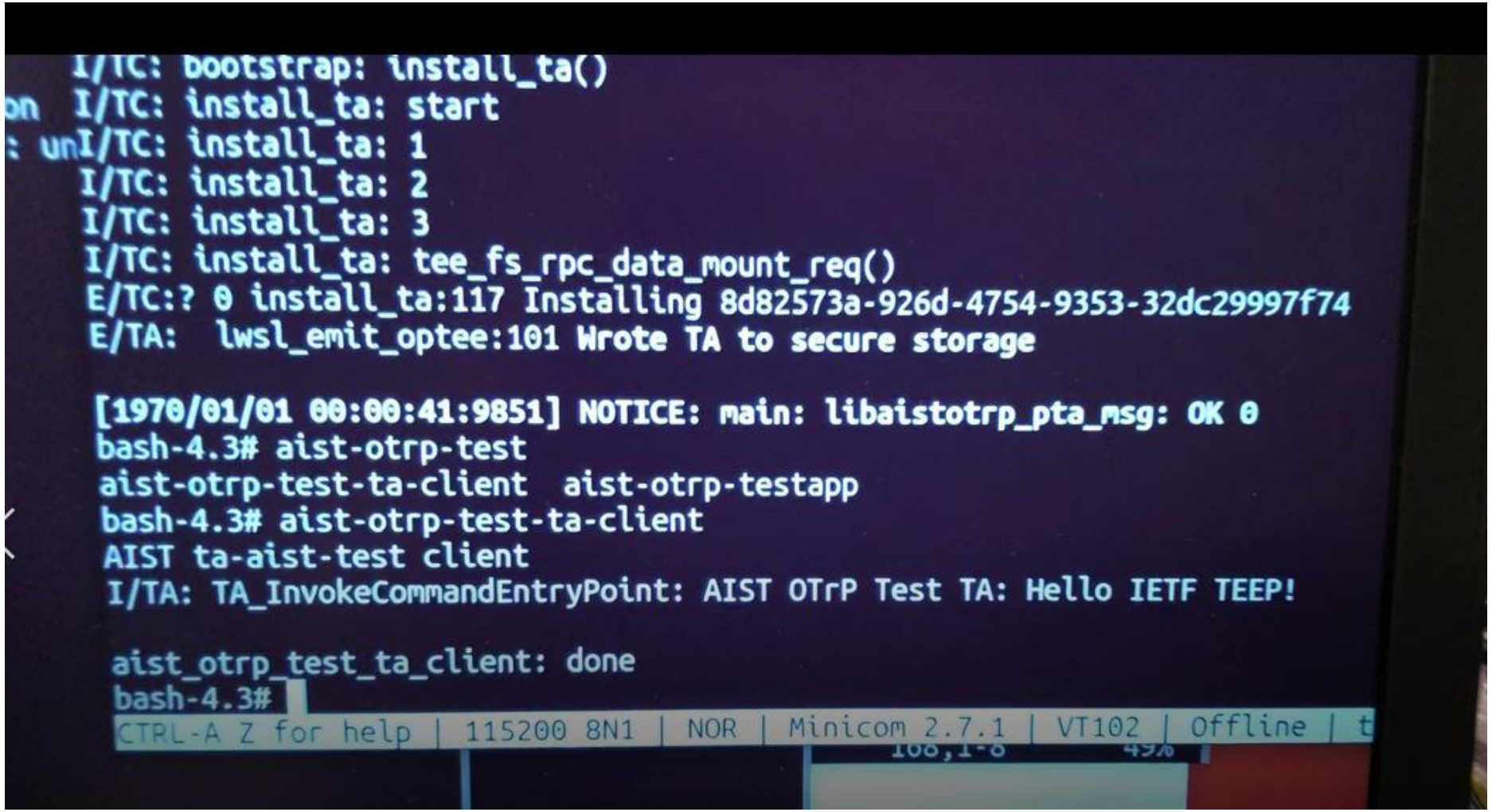
TEEP device


Search Terminal Help
icom 2.7.1
for help on special keys
ng Trusted Firmware
v1.1(release):bdec62e
Built : 11:11:48, Jun 23 2016
l frequency:1190494208Hz
ed to init lpddr3 rank0 dram phy
3_freq_init, set ddrc 533mhz
ddr3 rank0
rank1 init pass
3_freq_init, set ddrc 800mhz
ddr3 rank0
rank1 init pass
ng DDR
fastboot mode...
in -d /dev/ttyUSB1
62,19
9%
Home
End
Insert
Delete
Enter
Shift
PgUp
PgDn
Ctrl
Alt
PrtSc

Hacking, Debugging!



TEEP Device installing TA



What we learned (1/2)

- Hackathon 当日に見つかったドラフトの課題点
  - draft-ietf-teep-otrp-over-http-03
    - 初代 OTrP と TEEP protocol の両対応を考慮すべき
    - https://github.com/ietf-teep/otrp-over-http/issues/5
  - draft-tschofenig-teep-protocol-00.txt
    - JSON 記述のexampleが必要
    - CBOR 方式のみがドラフトに記述。binary表現のCBORより文字列表現のJSONの方がHackathon のように現場でデバッグするには効率がよい。

What we learned (2/2)

- 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)

- IETF 106 Hackathon での最大の教訓
  - TEEP 実現には TEE 自体の概要とコンセプトの理解、Intel SGX と ARM TustZone の知識、HTTPや JSONのプログラミング技術並びにインターネットでのデバイス管理の知識、実装力など複数の素養を必要であることが判明。ドキュメントだけで活用できる人は非常に限られることから、参考となる実装の重要性が上がる。

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, Apache?
  - 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 there 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?

次回の IETF107 に向けて

- ３月のIETF 107 前に hackathon 実施
  - 2020年2月 Hanness 主催のSecuring the IoT Hackathon 2020
  - TEEP protocol で使う CBOR のフォーマットをほぼ確定したいのが背景。
  - Hackathon 参加には、事前にCBORパーサーの実装が要求される。
  - IETF 107 でも hackathon 実施。
- IETF 107 以降ドラフトの議論が大幅に活発化
  - github 上で、ほぼ数日ごとに課題点の議論や更新。

- ドラフトと実装の両方の完成度を上げるスピードが加速している。
- 課題
  - 実利用を想定すればするほど、ドラフトの不明瞭点更新や、実装工数の肥大化に直面し始めている印象。

まとめ

- TEEP のコンセプトの紹介
- IETF 106 での Hackathon 活動を主体に、TEEP working group の活動の紹介
  - ドラフト内容の詳細化と実装の両方ともに活発化。実社会でのTEEP 活用を念頭に置いた時に検討課題が多く発見される。
- 参考実装の重要性が上がり、Hackathon を繰り返す方向性
  - 3月末のIETF107 の前の２月に再度 Hackathon 開催
- IETF 107 に向けての今後の課題点と活動

- この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（ＮＥＤＯ）の委託業務「高効率・高速処理を可能とするAIチップ・次世代コンピューティングの技術開発/革新的AIエッジコンピューティング技術の開発/セキュアオープンアーキテクチャ基盤技術とそのAIエッジ応用研究開発」の結果得られたものです。

用語集

- IETF - Internet Engineering Task Force
- TEEP - Trusted Execution Environment Provisioning
  - https://datatracker.ietf.org/doc/draft-ietf-teep-architecture/
- OTrP - Open Trust Protocol
  - https://tools.ietf.org/html/draft-tschofenig-teep-otrp-v2-00
- TEE - Trusted Execution Environment
- リモートアテステーション – Remote Attestation
- CA - Certificate Authority
- RATS - Remote ATtestation ProcedureS
  - https://datatracker.ietf.org/wg/rats/documents/
- SUIT - Software Updates for Internet of Things
  - https://datatracker.ietf.org/wg/suit/about/
- JSON - JavaScript Object Notation
- CBOR - Concise Binary Object Representation
  - https://datatracker.ietf.org/doc/rfc7049/
- Intel SGX (Software Guard Extensions)
- ARM TrustZone
- Global Platform

付録

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.