Hackathon Report

Team members:
Dave Thaler <dthaler@microsoft.com>
Mingliang Pei <mingliang_pei@symantec.com>

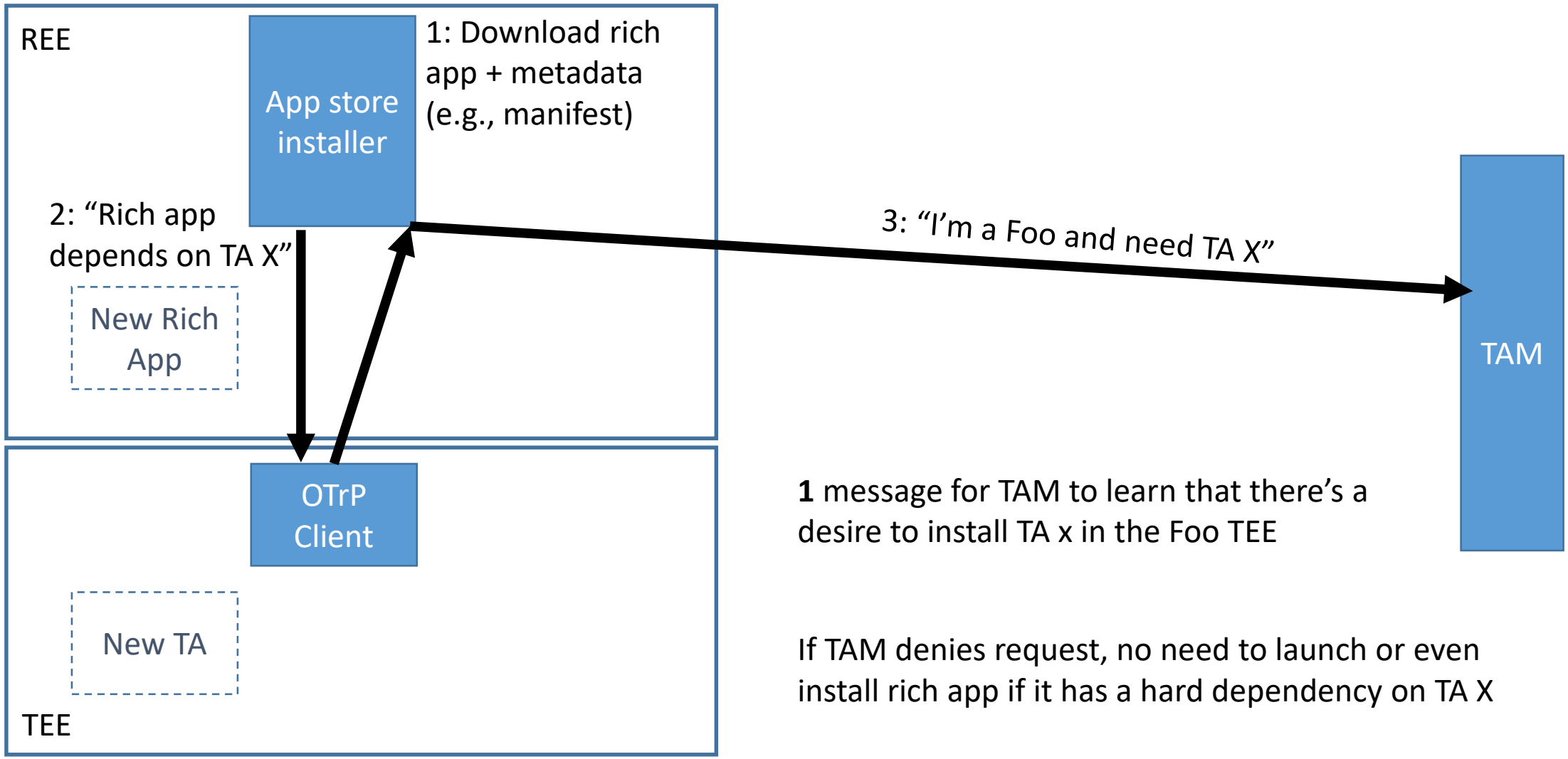
Hackathon Plan

- Goal: Find implementation issues in OTrP spec
    - draft-ietf-teep-opentrustprotocol-02.txt
- Implement OTrP and JOSE dependencies inside trusted execution environments (SGX and TrustZone)
    - RFC 7515: JWS
    - RFC 7516: JWE
    - RFC 7517: JWK

What got done

- Ported open source latchset/jose to run in SGX
- Designed and implemented OTrP transport details (not in I-D)
    - (see next slides)
- Designed and implemented initial OTrP message exchange (I-D is incomplete)
- Designed (not implemented) periodic checks for policy changes
    - OTrP agent triggers session when new TA is needed, e.g., by app installer
    - OTrP agent also triggers session either:
        - A) at interval configured by TAM, OR
        - B) lazily when existing TA is started and it’s been longer than that interval

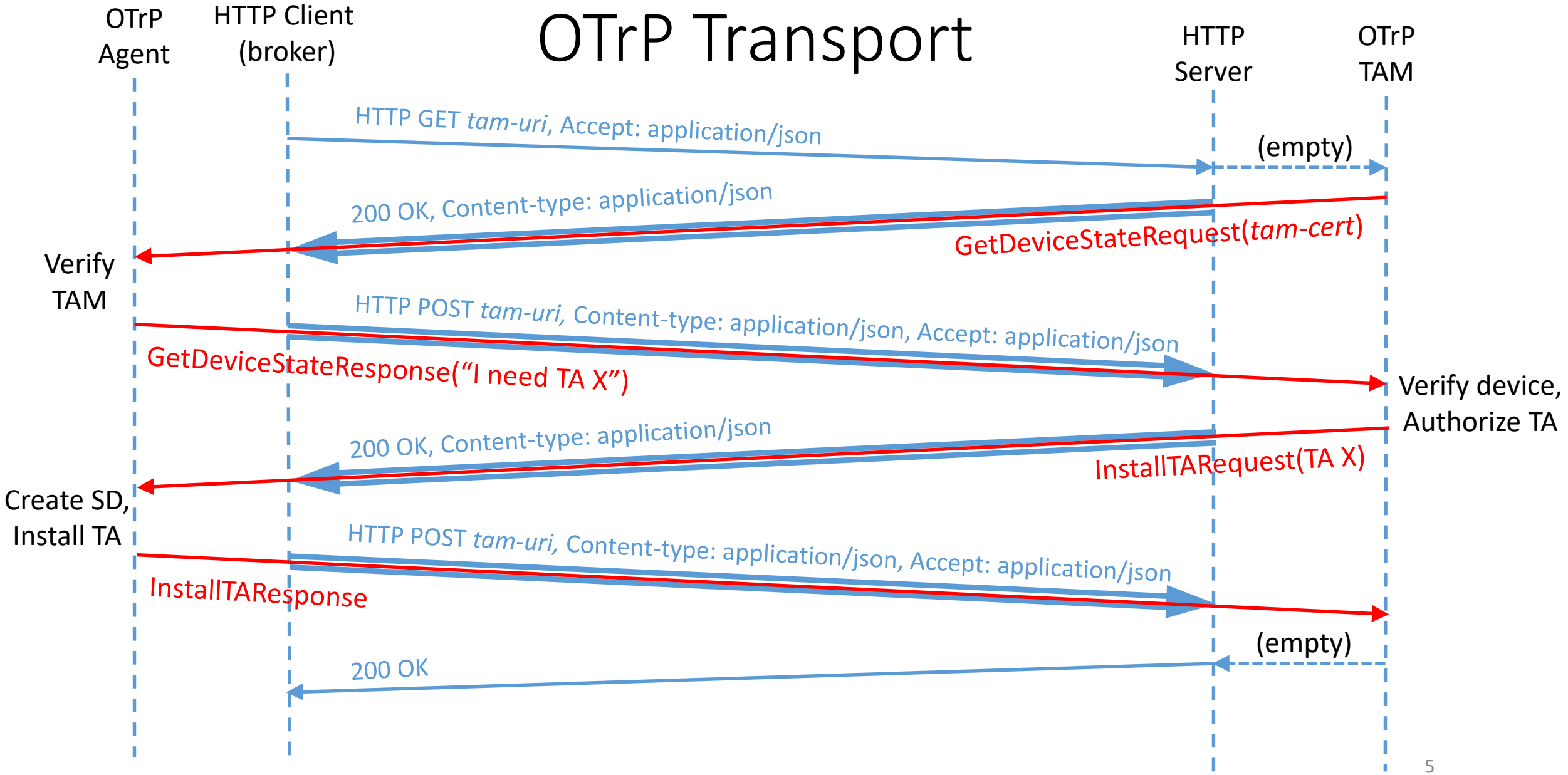
Connection model discussed at IETF 102



1 message for TAM to learn that there's a desire to install TA x in the Foo TEE

If TAM denies request, no need to launch or even install rich app if it has a hard dependency on TA X

OTrP Transport



Questions?