TEEP Open Trust Protocol (OTrP) Draft

draft-ietf-teep-opentrustprotocol-01.txt

Mingliang Pei (mingliang_pei@symantec.com)
Andrew Atyeo (andrew.atyeo@intercede.com)
Nick Cook (nicholas.cook@arm.com)
Minho Yoo (paromix@sola-cia.com)
Hannes Tschofenig (hannes.tschofenig@arm.com)

IETF 102th, Montreal
Agenda

• Draft status update
• Main changes in the last version
• TEEP architecture and protocol implementation mapping
• Gap discussion and future work
Status Update

• WG draft approved 4/26/2018
  – Draft name change to draft-ietf-teep-opentrustprotocol v00
  – Minor changes from the previously draft discussed in IETF 101 WG

• Updated version v01
  – Split the draft into a architecture draft and the updated protocol draft
  – Architecture draft v00 was made more general, incorporating discussions in IETF 101 and mailing list
OTrP Design Quick Refresh

• Original TEEP architecture and protocol foundation before split
• Covers protocol part that implements TEEP architecture
• A message protocol
  – JSON-based messaging between TAM and TEE
• Use asymmetric keys and certificates for device and TAM attestation
• An OTrP Agent in REE is used to facilitate communication between a device TEE and a TAM
• Support a transport binding
## OTrP Operations and Messages

### Remote Device Attestation

<table>
<thead>
<tr>
<th>Command</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetDeviceState</td>
<td>• Retrieve information of TEE device state including SD and TA associated to a TAM</td>
</tr>
</tbody>
</table>

### Security Domain Management

<table>
<thead>
<tr>
<th>Command</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateSD</td>
<td>• Create a SD in the TEE associated with a TAM</td>
</tr>
<tr>
<td>UpdateSD</td>
<td>• Update a SD or associated SP information</td>
</tr>
<tr>
<td>DeleteSD</td>
<td>• Delete a SD or SD related information in the TEE associated with a TAM</td>
</tr>
</tbody>
</table>

### Trusted Application Management

<table>
<thead>
<tr>
<th>Command</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallTA</td>
<td>• Install a TA in a SD associated with a TAM</td>
</tr>
<tr>
<td>UpdateTA</td>
<td>• Update a TA in a SD associated with a TAM</td>
</tr>
<tr>
<td>DeleteTA</td>
<td>• Delete a TA in a SD associated with a TAM</td>
</tr>
</tbody>
</table>
An OTrP Agent handles how to interact with a TEE from a REE

Most commonly developed and distributed by TEE vendor
OTrP JSON Message Format and Convention

{
   "<name>[Request | Response]": {
      "payload": "<payload contents of <name>TBS[Request | Response]>",
      "protected": "<integrity-protected header contents>",
      "header": <non-integrity-protected header contents>,
      "signature": "<signature contents>"
   }
}

For example:

- CreateSDRequest
- CreateSDResponse
Changes from the prior version

• Moved general architecture specification into the architecture draft
  – Adjusted introduction part to link with the architecture draft
  – Referred to Architecture draft to definitions and terminologies
  – Referred to Architecture doc for general architecture requirements
  – Retained the most part of entity relationship, certificate types, and OTrP Agent as part of Architecture to OTrP mapping reference

• No changes in API and messages

• Changed to make Trusted Firmware (TFW) check optional
  – TAM will decide whether a TEE acceptable in the absence of TFW signature

• Terminology update
  – Use TFW in all occurrences of Secure Boot Module (SBM)
TEEP Architecture to Implementation Mapping

• Mostly mapped implementation except a few new architecture expansion requests from mailing list

• Multiple TEE support
  – TEEP architecture proposes to expand single active TEE in a device to allow multiple full TEEs

• TA binary distribution by a Client Application
  – OTrP currently requires TA binary be distributed by a TAM and sent in an encrypted form
  – Issue in authorizing a Client Application and TA personalization data

• Use of an Agent for communication between a TEE and a TAM
  – Discussion around making it optional
Gap Discussion and Future Work

- Multiple TEE support
  - TEE identifier needs to be made visible to an OTrP Agent
  - OTrP Agent isn’t just relaying anymore; add routing capability to a target TEE
  - Other options

- TA binary distribution by a Client Application
  - Installation can be addressed
    - The signer of TA is trusted by a TEE
  - Issues with SD update and TA update in future
  - Issues to send device specific data that a TA needs to use

- Communication between a TEE and TAM might be facilitated by OS
  - A Rich App may not need to call OTrP Agent itself
Q&A

Thank you!
Message Format Negotiation

• A Client Application may query a device for its preferred message format
• A Client Application triggers TAM to send messages in a preferred format
• Use a default message format