TEEP Open Trust Protocol (OTrP) Draft

draft-ietf-teep-opentrustprotocol-02.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
• Hackathon feedback, issues and future work
Status Update

- Updated version v02
  - Alignment with architecture document update in terminology
    - OTrP Agent vs. Broker
    - Trusted Firmware (TFW) etc.
  - Removed “secure boot” reference
  - Focused largely on architecture draft work in the three interim work sessions
## Refresh of 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>
Address Hackathon Observations

1. Adds TA list to be installed in the first device information communication to a TAM GetDeviceStateResponse)
   – TA list to be installed expected from some metadata file

2. Specify the first GET contact call from a Broker to a TAM service

3. A few document clarification
   – Specify OCSP data encoding (BASE64)
   – List signature algorithm names to be choose from "RS256", "ES256"
   – JSON message validation check
Other Change Discussion

1. SD creation call CreateSD become optional?
   – Implicit SD creation per TA or for the first TA of a Service Provider

2. Multiple TEE support
   – TEE identifier needs to be made visible to an OTrP Broker
     – Other options

3. Allow separate TA binary distribution by a Client Application from TA
   device specific configuration data
Q&A

Thank you!