Open Trust Protocol (OTrP)
draft-pei-opentrustprotocol-06.txt

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

IETF 101th, London
OTrP Proposed Design Choices

• Use asymmetric keys and certificates for device and TAM attestation
  – Manufacturer-provided keys and trust anchors
  – Enable attestation and establish mutual trust between a TAM and a TEE-device

• An OTrP Agent in REE relays message exchanges between a TAM and TEE

• JSON-based messaging between TAM and TEE
  – Other message format: CBOR?

• Capable to support different transport
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>
OTrP Message Exchange via an OTrP Agent

- An OTrP Agent handles how to interact with a TEE from a REE
- Most commonly developed and distributed by TEE vendor
OTrP Agent Message Relay between TEE and TAM

1. **ProcessOTrPMessage**
   A TEE specific OTrP Agent function that passes OTrP messages between TEE and TAM

   **Input:**
   An OTrP message from TAM

   **Output:**
   An OTrP message returned by TEE

2. **GetTAINformation**
   Local query for a TA's information in the device. The response can be verified by a locally stored TEE SP specific anonymous public key.

   **Input:**
   A JSON message with TA identifier, SP Identifier, and a nonce value

   **Output:**
   An OTrP message received from TEE that describes a TA
Sample Protocol Usage Flow

- Security of the Operation Protocol is enhanced by applying the following three measures:
  - Verifies validity of a message sender's Certificate
  - Verifies signature of a message sender to check immutability
  - Encrypted to guard against exposure of sensitive data

- Request to TAM for TA installation
  - Send \textbf{[GetDeviceState]} to TEE
  - Return DSI as a response to \textbf{[GetDeviceState]}

- Send \textbf{[CreateSD]} to create a SD where the TA will be installed
  - Send other prerequisite commands (if necessary)

- Send \textbf{[installTA]} with encrypted TA binary and its personalization data

- **Phase#1**
  - "Device Attestation" Operation request triggered and verify Device state information
    - Request to TAM for TA installation

- **Phase#2**
  - Prerequisite operation (if Security domain doesn't exist where the TA should be installed)
    - Send \textbf{[CreateSD]} to create a SD where the TA will be installed

- **Phase#3**
  - Perform Operation requested by SP or Client Application
    - Send \textbf{[installTA]} with encrypted TA binary and its personalization data

- TAM
- Client App / OTrP Agent
- TEE

- **Get Device State**
  - Check TAM trustworthiness

- **Create new SD**

- **Install TA**
  - Check TAM trust and device state
  - Decrypt and install the TA binary and personalization data
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

• Added transport mandatory support
  – HTTPs as default for now

• Schema small changes to support multiple values
  – GetDeviceStateRequest:
    • Use an array to represent a list of OCSP stapling data ("ocspdat")
    • Use an array to represent a list of support of signing algorithms for algorithm agility instead of comma separate strings ("supportedsigalgs")
  – Use JSON Boolean true | false instead of string “true” and “false”
  – Use “TAM” consistently across the entire document in place of “TSM” (e.g. tsmid to tamid)
  – Communicated with GP editors (also preferred during discussion with the editors)
Changes from the prior version cont.

• OTrP Agent API changed to be abstract ones
  – Independent of programming languages
• Separated trusted error codes (TEE responded) from the non-trusted error codes (TEE not reachable etc.)
  – E.g. ERR_AGENT_TEE_BUSYERR_AGENT_TEE_FAILERR_AGENT_TEE_UNKNOWN
• Many small editorial updates
Transport Support Consideration

• TEE generally doesn’t have networking capability
• A Rich Application, or Client Application in REE will be doing all networking with TAM
• A Rich App in a device with TEE, which already does PKI cryptography, is most probably capable to do HTTPs, at least on devices with a TEE such as one over TrustZone or SGX today
• Question:
  – Can we start with the protocol with just HTTPs or CoAP must be an mandate for TAM to start with?
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