TEEP over HTTP

draft-ietf-teep-otrp-over-http-03

Dave Thaler <dthaler@microsoft.com>
Issues discussed at IETF 105:
1. Terminology alignment on transport layer implementation
2. HTTP Bindings
3. Move media type to OTrP spec (closed)

Issues raised since IETF 105:
4. Relationship to OTrPv2 TEEP protocol
5. Demuxing to OTrP vs TEEP protocol (new from Hackathon!)
Issue #4: Relationship to TEEP protocol

• Issue:
  • Old title was “HTTP Transport for the Open Trust Protocol (OTrP)” but WG decided to rename OTrPv2 to TEEP protocol
  • Examples used otrp media type but TEEP uses teep media type

• Changes in -03 (ready to close)
  • Updated title, discussion, and examples to use TEEP instead of OTrP
  • Did not remove support for OTrP in addition (but see Issue #5)
    • OTrP and TEEP have different media types, so references both as supportable over the same transport
Issue #5: Demuxing to OTrP vs TEEP protocol

• Discovered by Hackathon 106 implementation experience

• Issue:
  • Draft did not adequately explain how to demux if both are supported
  • Example: 0-byte POST arrives at TAM, which protocol should respond?

• Possible resolutions:
  1. Remove all support for OTrP
  2. Demux behavior based on media type
     • On receipt of an HTTP message, the choice is made based on the Content-Type header if present, else the Accept header if it is present.
     • For other events on the Agent side (request to install a TA, etc), the choice is learned together with learning the TAM URI, i.e., the TAM URI and protocol to use go together.
  3. Demux based on TAM URI
     • Unlike option 2, this requires separate URIs (e.g., separate paths) for TEEP vs OTrP
     • On the Agent side (request to install a TA, etc), still requires learning the TAM URI and protocol together, since Agent cannot infer anything from the URI itself
Issue #1: Terminology alignment (1/2)

• Implementations of TEEP-over-HTTP spec are now called:
  • TEEP/HTTP Client
  • TEEP/HTTP Server

• Independent of whether TAM has a TEE or not
Issue #1: Terminology alignment (2/2)

TEE

TEE Agent

Broker

TEE/HTTP Client

HTTP Client

TCP or QUIC Client

TEE

TEE Agent

TEEP/HTTP Client

HTTP Client

TCP or QUIC Client

TEE

TEE Agent

HTTP Client

TCP or QUIC Client

... (etc.)

TEEP Broker can be at different layers in different implementations
Issue #2: HTTP Bindings (1/3)

Current model:

Anders asked about:

IETF 106 - TEEP WG
Issue #2: HTTP Bindings (2/3)

• Might also apply to Red Hat’s Enarx scenario, if standard protocol is desired

• Options:
  A. Do nothing
  B. **Punt to future work, but update title of this doc (IETF 105 consensus)**
  C. Start on separate doc, and update title of this doc
  D. Work on now, in same doc
Issue #2: HTTP Bindings (3/3)

• Changes in draft-03:
  • Updated title
    HTTP Transport for Trusted Execution Environment Provisioning: Agent-to-TAM Communication
  • Updated introduction with a discussion of the two topological scenarios
    • States that remainder of doc is scoped to the Agent-to-TAM scenario, with other scenario left to future work, except...
    • HTTP headers section and security considerations apply to both scenarios
  • Ready to close (any subsequent feedback can be a new issue)?
Next Steps

• Address issue #5
• Any other issues?
• Then WGLC?