A SOAP Transport for RID

(new draft)

http://www.cert.org/ietf/inch/docs/draft-moriarty-soap-00.txt

Brian Trammell <bht@cert.org>

Wednesday, August 3, 2005

IETF 63 - Paris, France

Why SOAP?

- Need transport semantics for RID messages
- Continue evolution of RID into general-purpose transport and processing framework for IODEF documents
- WG consensus

SOAP Header

- <RID-Policy> child of RID element in <SOAP-ENV:header>.
- Policy information is necessary for processing and routing at SOAP intermediaries.
- Allow XML encryption of IODEF document data to protect incident information from intermediaries.

SOAP Body

- <RID> in <SOAP-ENV:Body> contains all RID children (including duplicate <RID-Policy>).
- <RID> is sibling of <IODEF-Document>.
  - Allows easy separation of RID traceback and handling information from associated IODEF document.

SOAP transport bindings

- HTTP: mandatory
  - Improves implementability [not a word] using off-the-shelf software.
  - Requires all RID systems to listen.
  - May have issues with BCP 56.
    - Requires an IANA-assigned port number specific to RID.
- BEEP: optional
  - Allows bidirectional message initiation without requiring all nodes to listen.
  - Existing implementations are limited.

SOAP transport security

- HTTPS (SSL/TLS) is required
  - Provides privacy and authentication between SOAP intermediaries
- BEEP TLS profile is required

Example: Split RID as IODEF sibling

- ```
  <SOAP-ENV:Envelope>
    <SOAP-ENV:Header>
     <iodef-rid:RID>
       <iodef-rid:RIDPolicy>
        ... [policy information]
       </iodef-rid:RIDPolicy>
     </iodef-rid:RID>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body>
     <iodef-rid:RID>
      ... [all RID (policy and non-policy) information]
     </iodef-rid:RID>
     <iodef:IODEF-Document>
      ... [incident information]
     </iodef:IODEF-Document>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
  ```
- Separates intermediary from final processing.
- However, some information semantically bound to the incident itself doesn't reside in IODEF-Document.
  ```

IPPacket

- <IPPacket> is clearly related to <Incident> and belongs therein (IODEF RecordItem)
- See IODEF open issues
- Future change to RID

Moving Forward

- Completion of -00 draft and release after meeting.

Comments?