IODEF Interoperability Report

Brian Trammell <bht@cert.org>

Wednesday, July 12, 2006

IETF 66 - Montréal, QC, Canada
Introduction

• IODEF interoperability testing held through June and July 2006.

• Three steps:
  – Test facilitator generated tests.
  – Participants submitted results.
  – Test facilitator evaluated and compiled results.

• Not a standard interop
  – IODEF is as its core a document format.
  – Semantics are important.
  – Offline testing and evaluation are possible.
The Tests

- **Three IODEF documents**
  - Designed to test features of the schema, especially corner cases.
  - Results are some representation of the internal data model of the implementation after parsing.
  - Variety of implementation makes evaluation an ad-hoc process.

- **Four textual incident reports**
  - Designed to verify IODEF semantics across implementations.
  - Derived from real incidents.
  - Results are IODEF documents.

- **User-contributed IODEF documents**
# Results Summary

<table>
<thead>
<tr>
<th>Test</th>
<th>n</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parsing</td>
<td>3</td>
<td>Succeeded</td>
</tr>
<tr>
<td>Loopback</td>
<td>2</td>
<td>Succeeded*</td>
</tr>
<tr>
<td>Validation</td>
<td>3</td>
<td>Failed (minor nits)</td>
</tr>
<tr>
<td>Generation</td>
<td>3</td>
<td>Succeeded*</td>
</tr>
</tbody>
</table>
IODEF Document Input Results

• All participants that attempted to do so were able to parse the supplied IODEF documents.

• Two participants submitted “loopback” results
  – parse IODEF to internal data model, then regenerate IODEF from internal data model.

• One participant reported successful parse
IODEF Document Loopback Results

- Some of the more esoteric features of the schema do not appear to be universally supported
  - Dual-stack iodef:Node instances
  - Rate counters
- Extension data inconsistently handled
  - Entity-encoding of XML AdditionalData
- Limitations of internal data model
  - One implementation discarded most Contact information and other incident context.
Document Generation Results

• Three participants submitted IODEF documents
  – Two used the incident reports supplied with the interoperability test package

• None of these documents passed xmllint validation against -070
  – Missing IODEF-Document version
  – Element content ordering
  – Timezone class representation
  – ISO8601 date formatting
Document Generation Results (2)

• Contact information represented inconsistently
  – No generation of RFC 2252 compliant postal addresses
  – Private storage of semantically richer geographic information

• Use of Description for private data
  – Should there be support for AdditionalData on other first-class objects such as Contact and System?
Document Generation Results (3)

• In general, good use of recursion where available and applicable.

• Confusion about representing many-source, many-target attacks with iodef:Flow
  - Use cross-product? Use one large Flow instance?
Recommendations

• Will continue maintenance of interoperability test document repository.
  – Simply submit your IODEF output to interop-ietf66@iodef.org to place it in the repository.

• Implementers should use XML Schema validators to test their own output.
  – Test coordinator used xmllint.
Next Steps

• Implementer comments and discussion: now
• Final interoperability report: end of July
  – Additional results accepted after meeting
  – Comments from Montréal