draft-ietf-mile-rfc5070-bis-15

Roman Danyliw <rdd@cert.org>

IETF 94

November 2, 2015
What is IODEFv2?

• An XML format to represent data elements commonly exchanged by CSIRTs:
  – Computer security incident reports
  – Cyber security indicators
• Update to the Incident Object Description Exchange Format (IODEF) (RFC5070)
• IODEF is extended by various extensions
  – RFC 5901 (Phishing)
  – RFC 7203 (Structured Cybersecurity Information)
  – RFC 7495 (Reference format)
• IODEFv2 is exchanged with:
  – RID (RFC 6545 and RFC 6546)
  – XMPP (draft-appala-mile-grid-00)
Drafts Since IETF 93 (Prague)

• -15 (10-16-2015)
• WGLC started on 10/17/2015
## Issues Closed in -15

<table>
<thead>
<tr>
<th>ID</th>
<th>Issue Summary</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>#46</td>
<td>Missing cause of an incident</td>
<td>-15</td>
</tr>
<tr>
<td>#50</td>
<td>Provide support for &quot;bulk observables&quot;</td>
<td>-15</td>
</tr>
<tr>
<td>#38</td>
<td>Improve example in Section 7</td>
<td>2 of 3</td>
</tr>
</tbody>
</table>

http://trac.tools.ietf.org/wg/mile/trac/report/1?asc=1&sort=ticket
Incompatibilities with v1

- IODEF-Document@version="1.00" → "2.00"
- Service@ip_protocol → @ip-protocol
- Node/Name → Node/DomainData/Name
- Node/DataTime → Node/DomainData/DateTime
- NodeRole moved to System (from Node)
- Reference class is now defined by draft-ietf-mile-enum-reference-format-11
- Impact v1 class is now SystemImpact and IncidentCategory classes
- Extending ENUM attribute with IANA registries too
- All iodef:MLStringType classes use xml:lang; all @lang attributes now xml:lang
- Counter@type → Counter@unit (there is still a @type)
- IODEF-Document@formatid → @format-id
- ReportTime is not mandatory; GenerationTime is mandatory
Issue #46: Cause of the incident

- Specify the cause of the incident

```
+-------------------------+
| Assessment              |
+-------------------------+
| ENUM occurrence         |<--{0..*}--[ IncidentCategory ] |
| ENUM restriction         |<--{0..*}--[ SystemImpact ]     |
| STRING ext-restriction   |<--{0..*}--[ BusinessImpact ]    |
| ID observable-id         |<--{0..*}--[ TimeImpact ]        |
|                         |<--{0..*}--[ MonetaryImpact ]    |
|                         |<--{0..*}--[ IntendedImpact ]    |
|                         |<--{0..*}--[ Counter ]           |
|                         |<--{0..*}--[ MitigatingFactor ]  |
|                         |<--{0..*}--[ Cause ]             |
+-------------------------+

+------------------------+
| Method                 |
+------------------------+
| ENUM restriction        |<--{0..*}--[ Reference ]        |
| STRING ext-restriction   |<--{0..*}--[ Description ]       |
|                         |<--{0..*}--[ sci:AttackPattern ] |
|                         |<--{0..*}--[ sci:Vulnerability ] |
|                         |<--{0..*}--[ sci:Weakness ]      |
|                         |<--{0..*}--[ AdditionalData ]    |
+------------------------+```
Other Changes

• Corrected text describing the line delimiter for BulkObservable (Issue #50)
• Updated Examples (Issue #38)
  – Minimal IODEF Document
  – Indicator List
• Added Certificate/Description
• Editorial fixes

Full Changelog at https://mailarchive.ietf.org/arch/msg/mile/FkxMLzqKYMofFVC1U6l4qERK5-M
## Outstanding Issues

<table>
<thead>
<tr>
<th>ID</th>
<th>Issue Summary</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>#39</td>
<td>RelatedDNS documentation</td>
<td></td>
</tr>
<tr>
<td>#54</td>
<td>Reorganize IODEF schema</td>
<td>All but reformatting done. Pending any final feedback.</td>
</tr>
<tr>
<td>#38</td>
<td>Improve example in Section 7</td>
<td>2 of 3 example updated.</td>
</tr>
</tbody>
</table>

+ General editorial review  
+ Review completeness of all class write-ups  
+ Consistency in the internal references to classes in declarations  
+ Consistency between text diagrams-and-text  
+ Consistency between all text and schema  
+ Update in-document Changelog in Section 1.1  
+ Review incompatibility with RFC5901

http://trac.tools.ietf.org/wg/mile/trac/report/1?asc=1&sort=ticket
Issue #54: Reformat the Schema

• Reformat the schema:
  ✓ Eliminate nested element declaration
  ✓ Eliminate inline enumerated attribute definitions
  × Fix inconsistent white-spacing
  ? Flexible sequencing of elements?

• Is there interesting in flexible sequencing of elements

Only valid sequence with current Schema

```
01:<IODEF-Document version="2.00" ...>
02:  <Incident purpose="reporting" ...>
03:    <IncidentID name="csirt.example.com">
04:    <GenerationTime>2015-07-18 ...
05:    <Contact type="organization" ...
06:      <Email>...
07:    </Contact>
08:  </Incident>
09:</IODEF-Document>
```

Currently invalid. Should it be?

```
01:<IODEF-Document version="2.00" ...>
02:  <Incident purpose="reporting" ...>
03:    <IncidentID name="csirt.example.com">
04:    <GenerationTime>2015-07-18 ...
05:    <Contact type="organization" ...
06:      <Email>...
07:    </Contact>
08:  </Incident>
09:</IODEF-Document>
```
Issue #38: Improved Examples

• Need to update the existing examples
  – http://trac.tools.ietf.org/wg/mile/trac/ticket/39

• Candidate examples:
  ✓ Minimal IODEF-Document
  ✓ Simple list of indicators
  ✗ Incident Report
Issue #39: RelatedDNS

• Problem: RelatedDNS is underspecified
  – http://trac.tools.ietf.org/wg/mile/trac/ticket/39

• On the Mailing List
  – http://www.ietf.org/mail-archive/web/mile/current/msg01637.html

• Previously Discussed Representation Approaches:
  1. Use draft-hoffman-dns-in-json-02, a JSON representation
  2. A comma separated value list of DNS fields
  3. Defining RelatedDNS as iodef:AdditionalData and requiring an extension
  4. Define an alternative representation for RelatedDNS

• What ahead
  – Specify in 5070bis?
  – Specify in another draft as an extension?
Discussion