IODEF Data Model Status

(progress from 03)

<draft-ietf-inch-iodef-03>

tracked @ https://rt.psg.com : inch-dm queue

Roman Danyliw <rdd@cert.org>

Wednesday, March 9. 2005

IETF 62, Minneapolis, USA

Progress on issues from v03

- Status of Open Issues
  - 4 Resolved, but TODO
  - 6 Require Discussion with Proposal
  - 3 Require Discussion (no Proposal)

XML Schema v04 (#365)

- Schema that tracks existing data model can be found at:
  - http://www.uazone.org/demch/projects/iodef/
- Schema v04.01 will form basis of -04 draft

#699: Format TIMEZONE data-type

https://rt.psg.com/Ticket/Display.html?id=699

- Provide an explicit format (not STRING) for the TIMEZONE data
- PROPOSAL

```
<xs:element name="TimeZone" type="iodef:TimeZoneType">
  <xs:simpleType name="TimeZoneType">
    <xs:restriction base="xs:string">
        <xs:pattern value="[+-][0-9][0-9][0-9][0-9]" />
    </xs:restriction>
  </xs:simpleType>
```

- STATUS: Accepted

#856: Implementation-Friendly Time

https://rt.psg.com/Ticket/Display.html?id=856

- Use Schema-provided simple data-type (xs:dateTime) instead of xs:string to represent timestamp information

- PROPOSAL

```
<xs:element name="DateTime" type="xs:dateTime"/>
<xs:element name="ReportTime" type="xs:dateTime"/>
<xs:element name="DetectTime" type="xs:dateTime"/>
<xs:element name="StartTime" type="xs:dateTime"/>
<xs:element name="EndTime" type="xs:dateTime"/>
```

- STATUS: Accepted; xs:dateTime = ISO 8601 = IODEF DATETIME data-type

#356: Standardize extensions

https://rt.psg.com/Ticket/Display.html?id=356

- Add a mandatory top-level container class to all extensions to allow an easy determination of which one is used
- PROPOSAL

```
 <!ELEMENT IODEF-Extention (ANY)>
<!ATTLIST IODEF-Extention
          name     CDATA    #REQUIRED
          source   CDATA    #REQUIRED
          version  CDATA    #IMPLIED >
```

- STATUS: Unnecessary with XML Schema

#703: Redesign <Analyzer>

https://rt.psg.com/Ticket/Display.html?id=703

- Simplify the <Analyzer> class dropping unnecessary information inherited from IDMEF

- PROPOSAL
  - Rename <Analyzer> to <Sensor>
  - Drop child classes: <pid>, <path>, and <Process>
  - Add versioning attributes similar to <Application>

- STATUS: further discussion necessary

#858: Redefine Incident@purpose

https://rt.psg.com/Ticket/Display.html?id=858

- Capture all the general use-cases of the IODEF
- PROPOSAL

```
<xs:attribute name="purpose">
<xs:simpleType>
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="traceback"/>
    <xs:enumeration value="mitigation"/>
    <xs:enumeration value="reporting"/>
    <xs:enumeration value="other"/>
  </xs:restriction>
</xs:simpleType>
</xs:attribute>
```

- STATUS: discussion required to assess completeness

#702: Representing OS information

https://rt.psg.com/Ticket/Display.html?id=702

- Represent the operating system of a network node (in <System>)
- PROPOSAL

```
<xs:element name="OperatingSystem">
<xs:complexType>
        <xs:attribute name="vendor" type="xs:string"/>
        <xs:attribute name="name" type="xs:string"/>
        <xs:attribute name="version" type="xs:string"/>
        <xs:attribute name="patch" type="xs:string"/>
</xs:complexType>
</xs:element>

<OperatingSystem vendor="Microsoft" name="Windows" version="XP" patch="SP2" />
<OperatingSystem name="FreeBSD" version="5.3" patch="RC2" />
<OperatingSystem vendor="Apple" name="OS X Server" version="10.3.7" />
<OperatingSystem vendor="FireFly" name="BSD" version="1.0" />
```

- STATUS: further discussion needed

#698: Representing a Name in <Contact>

https://rt.psg.com/Ticket/Display.html?id=698

- Define a new class with a structured data-type to replace <Contact>/<name> to represents an individual contact
- PROPOSAL

```
<xs:element name="NameIdentifier" type="iodef:NameIdentifierType"/>
…
<xs:extension base="iodef:MultilingTextType">
…
<xs:attribute name="format">
<xs:simpleType>
   <xs:restriction base="xs:NMTOKEN">
     <xs:enumeration value="emailAddress"/>
     <xs:enumeration value="x509NameQualifier"/>
     <xs:enumeration value="urn"/>
     <xs:enumeration value="local"/>
     <xs:enumeration value="other"/>
   </xs:restriction>
</xs:simpleType>
</xs:attribute>
```

- STATUS: agreement on necessity, no consensus on proposal
  - Proposal currently conflicts with existing definition of <Contact>

#855: Formalize <Location>

https://rt.psg.com/Ticket/Display.html?id=698

- Apply structure to the currently free-form <Location>
- PROPOSALS
  - Use X.509 DN-like syntax

```
<Location CN=Yuri Demchenko, OU=AIRG, O=UvA,
          S=NH,  L=Holland, C=NL>
    <Timezone>+0600</Timezone>
</Location>
```

- STATUS: further discussion required
  - Concerns that the proposal redefines the intent of the class (i.e., it provides a way to bind a <Node> to an organization).
  - Relationship between <Contact> and <Location>

#701: Review of Default Values

https://rt.psg.com/Ticket/Display.html?id=701

- Review all default attribute values and report back to the WG
- STATUS: Any volunteers?

#551: Formalizing <RecordData>

https://rt.psg.com/Ticket/Display.html?id=551

- Add meta-information so that in-lined logs snippets and those reference externally can be processed
  - Support a way to specify a filter pattern and offsets into text and binary log files
- STATUS: Concrete proposal needed

#857: Handling Binary Files

https://rt.psg.com/Ticket/Display.html?id=857

- Handing binary files and impact of XOP (XML-binary Optimization Packaging) on transport

- STATUS: Awaiting proposal

To be written

- IANA Considerations (Issue #700)
- Examples and description of XML-Signature and XML-Encryption in Security Considerations

Moving Forward

- Release an -04 draft using Schema within a month

Comments?