IODEF Data Model Status

<draft-ietf-inch-iodef-02>

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

Roman Danyliw <rdd@cert.org>

1200-1530, Sunday, June 13. 2004

Interim Meeting, Budapest, Hungary

Summary of Work

1. Add to Draft
   - XML Schema, XML-Sig
2. Needs Discussion
   - Simplified Representation
   - Flow support
   - Assigning IDs
   - Extension class typing
   - Timestamps
3. Ok to add, but blocking on discussion
   - AS Number support
   - Extension meta data

Summary of Work

1. Add to Draft

3. Needs Discussion

5. Ok to add, but blocking on discussion

#365: XML Schema Migration

https://rt.psg.com/Ticket/Display.html?id=365

http://www.uazone.org/demch/projects/iodef/

- Convert DTD to Schema
- STATUS
  - Release a DTD and Schema in v03 draft
  - v04 with full Schema

#364: XML-Sig and Encryption

https://rt.psg.com/Ticket/Display.html?id=364

- How to apply XML-Signature and XML-Encryption to IODEF documents?
- PROPOSAL
  - Examples of using XML-Signature
  - http://nic.surfnet.nl/scripts/wa.exe?A2=ind04&L=inch&F=&S=&P=2459
- STATUS:
  - Clearly will be used, but solution requires evaluation

Summary of Work

1. Add to Draft

3. Needs Discussion

5. Ok to add, but blocking on discussion

#472: Representation Complex

https://rt.psg.com/Ticket/Display.html?id=472

- System class is too IDS/IDMEF centric and overly complex
- PROPOSAL
  - Create a more flow (i.e., communication between machines) view of the incidents
  - Drop <Process>, <FileList>, and <User> from <System>
  - Simplify <Address> to only IP addresses
  - http://nic.surfnet.nl/scripts/wa.exe?A2=ind04&L=inch&F=&S=&P=1576
- STATUS: needs further discussion

#472: Complexity (2)

- Information lost due to this change:
  - All Layer-2 addresses
  - Non-IP Layer 3 protocols
  - Layer 7 (application) protocols fields
    - SNMP and HTTP
  - Running process at end-points
  - Filesystem information at end-points (e.g., inodes)
  - Explicit netmask of an IP address (deal in CIDR blocks, IPs)

#472: Complexity (3)

- Example snippet -- Current

```
<EventData> ...
   <System category="target">
      <Node>
         <Address category="ipv4-addr">
            <address>10.2.1.1</address>
         </Address>
         <Service>
            <port>1434</port>
            <protocol>udp</protocol>
         </Service>
      </Node
   </System>
   <System category="target">
      <Node>
         <Address category="ipv4-addr">
            <address>10.2.0.0</address>
            <netmask>16</netmask>
         </Address>
            <port>1434</port>
            <protocol>udp</protocol>
         </Service>
      </Node>
   </System>Service>
```

#472: Complexity (4)

- Example snippet -- Proposal

```
<EventData> …
   <Flow>
      <System category="target">
          <Node>
              <IPAddress type="ipv4-addr">127.0.4.1</IPAddress>
          </Node>
          <Service>
              <port>80</port>
          </Service>
      </System>
      <System category="source">
          <Node>
              <IPAddress type="ipv4-addr">10.4.5.1</IPAddress>
          </Node>
          <Service>
              <port>23456</port>
          </Service>
      </System>
      <protocol>16</protocol>
   </Flow>
```

#360: Flow Support

https://rt.psg.com/Ticket/Display.html?id=360

- Want a representation for:
  - flow data
  - statistics on these flows

- PROPOSAL
  - Add a way to represent stats via new <Counter>
  - http://nic.surfnet.nl/scripts/wa.exe?A2=ind04&L=inch&F=&S=&P=1576

- STATUS: needs further discussion

#360: Flow Support (2)

- Aggregation: shows 5683 occurances to 80/tcp and 114 occurances to 137/tcp occured from 10.4.5.1

```
<Flow>
    <System category="target">
      <Service>
                <port>80</port>
                <Counter type="events">5683</Counter>
      </Service>
    </System>
    <System category="target">
      <Service>
                <Counter type="events">114</Counter>
                <port>137</port>
      </Service>
    </System>
    <System category="source">
      <Node>
                <IPAddress type="ipv4-addr">10.4.5.1</IPAddress>
      </Node>
    </System>
    <protocol>16</protocol>
</Flow>
```

#360: Flow Support (3)

- Summary Statistics: a count of the amount of sessions to three netblocks over TCP

```
<Flow>
   <System category="target">
      <ASNumber>42</ASNumber>
      <Node>
          <IPAddress type="ipv4-net">10.4.0.0/16</IPAddress>
          <Counter type="session">12354</Counter>
      </Node>
      <Node>
         <IPAddress type="ipv4-net">10.55.0.0/16</IPAddress>
         <Counter type="session">2345</Counter>
      </Node>
      <Node>
         <IPAddress type="ipv4-net">10.124.0.0/16</IPAddress>
         <Counter type="session">1984</Counter>
      </Node>
    </System>
    <protocol>16</protocol>
</Flow>
```

#357: Assigning IncidentIDs

https://rt.psg.com/Ticket/Display.html?id=357

- How to assign incident identifiers?
  - How to set the CSIRT name in the origin attribute?

- PROPOSALS
  - external registration
  - AS number
  - Domain name
  - Net handles

- STATUS: further discussion needed

#362: Unify type attribute of extensions

https://rt.psg.com/Ticket/Display.html?id=362

- Should the type attribute of the extension classes (i.e., AdditionalData, and Record Item) be identical?
- PROPOSALS
  - Since the enum list for RecordItem is a superset of AdditionalData, use the same for both
  - Since the classes represent different data, keep the attribute definitions different
- STATUS: further discussion needed

#363: Timestamp formats

https://rt.psg.com/Ticket/Display.html?id=363

- Support more commonly used time formats
  - time-zones formats other than GMT+004, including day of the week, etc.

- STATUS: needs further discussion

Summary of Work

1. Add to Draft

3. Needs Discussion

5. Ok to add, but blocking on discussion

#359: Supporting AS Numbers

https://rt.psg.com/Ticket/Display.html?id=359

- Add AS numbers as another address type; needed for RID and providers
- STATUS: accepted, but contingent on any redesign (#360 already includes)

#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: blocking on Schema evaluation

Moving Forward

- Create a v03 draft before IETF 60 with
  - Schema support
  - Resolution to complexity and flow issues

Comments?