IODEF Data Model Status

(changes from 02 to 03)

<draft-ietf-inch-iodef-03>

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

Roman Danyliw <rdd@cert.org>

Thursday, November 11. 2004

IETF 61, Washington DC, USA

Outline

Changes from v02 to v03

Editorial Changes

- Compressed the ASCII-art pictures for the classes
- Made UML diagrams, text description, and the DTD consistent
- Re-wrote introduction (Section 1)
- Simplified XML section (Section 2.1)
- Simplified the Processing considerations (Section 5)
- Simplified the Security considerations (Section 9)
- Reference IDMEF specification for <Impact> and <Confidence>
- Dropped all legacy normative references
- More polished text for many of the class descriptions

Simplify the Data Model (#472)

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

- Removed legacy (IDMEF) classes
  - File system classes: <FileList>, <File>, <inode>, etc.
  - Layer 7 classes: <SNMPService>, <HTTPService>
  - User classes: <User>, <UserId>
- Removed unused classes
  - <number>
  - <LifeImpact>
- Removed redundant classes
  - Removed <History> from <EventData> (already in <Incident>)

Simplify the Data Model (#472) [2]

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

- Simplify representations when possible
  - Merged <IncidentData> into <Incident>
  - Simplified <Address> to not use <address> and <netmask>
    - <!ELEMENT Address (address, netmask?)>
    + <!ELEMENT Address (#PCDATA)>

  - Simplified <Service> to no longer redundantly
    - <!ELEMENT Service (((name?, port), portlist, protocol?)>
    + <!ELEMENT Service ((port | portlist), Application?)>
    + <!ATTLIST Service
    + ip_version CDATA "4"
    + ip_protocol CDATA #REQUIRED >

  - Removed NTPSTAMP (ntpstamp attribute) representation from the Time classes
  - Removed @restriction attribute from <Impact>, <TimeImpact>, and <MonetaryImpact>

Clean-up Attributes

- Default value of Address@category="ipv4-addr” not "unknown“
- Dropped Contact@role="actor" enumerated value referenced in the <Expectation> class

Add new data

- Added "asn" to %attvals.addrcat in <Address> (Issue #359)
- Added "investigate" to attvals.expectcat in <Expectation>
- Introduced <Application> (and replace <Process> of <System>, added to <Service>)

Flow Notation and Summarization Support (#360)

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

- Added <Flow> as child of <EventData> to encapsulate <System>s
- Added <Counter> to <Node> and <Service>

Outline

Open Issues

#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:
  - Will fix with Schema trickery? How?

#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
- PROPOSALS
  - Add a way to specify filter patterns and offsets into text and binary log files
- STATUS: further discussion needed

Other Issues

- Rename and redesign Analyzer (drop <pid>, <path>, <Process>); make it more similar to <Application>
- Should <Application> be added to <Method>? (i.e., how to represent attack tools? Is using the System/Service/Application sufficient?)
- Decide whether <Contact>/<name> requires its own class since it is formatted as PERSON, but in other uses of <name> it is STRING.
- Representing OS of <System>

TODO

- To be written
  - IODEF Schema (done for v02, needs update for v03)
  - IANA Considerations
  - Examples and description of XML-Signature and XML-Encryption in Security Considerations
- Define sane default values for all attributes
- Specify format of the TIMEZONE data-type

Moving Forward

- Release an 04 draft using Schema within a month

Comments?