IODEF Data Model Status

<draft-ietf-inch-iodef-02>

Roman Danyliw <rdd@cert.org>

1300-1500, Thursday, March 4. 2004

IETF 59, Seoul, Korea

XML Schema Migration

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

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

Supporting AS Numbers

(http://nic.surfnet.nl/scripts/wa.exe?A2=ind03&L=inch&O=D&P=1814)

- Add AS numbers as another address type; needed for RID and providers

- STATUS: accepted, but todo

Indexing IODEF Documents

(http://nic.surfnet.nl/scripts/wa.exe?A2=ind03&L=inch&O=D&P=19014)

- What is the equivalent to the current "subject" line of an email message?
- STATUS: resolved; use /IODEF-Document/Incident/Description

XML-Signature and XML-Encryption

(http://nic.surfnet.nl/scripts/wa.exe?A2=ind03&L=inch&O=D&P=19142)

- 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: needs more discussion and volunteers

Assigning IncidentIDs

(http://nic.surfnet.nl/scripts/wa.exe?A2=ind03&L=inch&O=D&P=18902)

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

- PROPOSALS
  - external registration
  - AS number
  - Domain name

- STATUS: consensus on the list is domain name

Type attribute of the extension classes

(http://nic.surfnet.nl/scripts/wa.exe?A2=ind03&L=inch&O=D&P=21811)

- 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
  - todo: fix typo between data model and DTD
  - requires further discussion

Timezone element of Contact

(http://nic.surfnet.nl/scripts/wa.exe?A2=ind03&L=inch&O=D&P=21811)

- What should be the cardinality between Contact and Timezone?

- STATUS: todo: fix typo between data model and DTD; timezone is 0..1

- What is the name of the class: “Timezone” or “TimeZone”

- STATUS: consensus on the list is with "Timezone"

Supporting IR Process

(http://nic.surfnet.nl/scripts/wa.exe?A2=ind03&L=inch&O=A&P=22621)

- Want a representation for:
  - flow data
  - statistics on these flows
- System class is too IDS/IDMEF centric and overly complex
- PROPOSAL
  - Drop <Process>, <FileList>, and <User> from <System>
  - Simplify <Address> to only IP addresses
  - Add a way to represent stats
  - http://nic.surfnet.nl/scripts/wa.exe?A2=ind04&L=inch&F=&S=&P=1576
- STATUS: needs further discussion

Standardize extension classes

(http://nic.surfnet.nl/scripts/wa.exe?A2=ind04&L=inch&F=&S=&P=748)

- 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: needs further discussion
  - Need to consider implications of Schema

Timestamp formats

(http://nic.surfnet.nl/scripts/wa.exe?A2=ind03&L=inch&O=D&P=19259, http://nic.surfnet.nl/scripts/wa.exe?A2=ind04&L=inch&O=D&P=866)

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

Comments?