IODEF Data Model Status
(progression from -04)
<draft-ietf-inch-iodef-05>

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

Roman Danyliw <rdd@cert.org>
Wednesday, November 9, 2005
IETF 64, Vancouver, Canada
Status of Issues

- -05 resolved 5 open issues
- 4 remaining issues
  - Require Discussion (w/ Proposal) = 1
  - Require Discussion (w/o Proposal) = 1
  - Editorial = 2
Closed Issues

• #885: Add Structure to <Location>
  – (per IETF 63) no WG support

• #857: Handling binary files
  – No response from proponent in 11-months
Substantial Editorial Review

- Fixed (45+) inconsistencies between Schema and UML
  - Different `<xs:sequence />`
  - Different enumerated values
  - Different attribute names
    - e.g., `@type` and `@type = df, df`
  - Assigned Schema data-types per DM types
  - Dropped global attributes in the Schema but not in the UML
Enforce Consistent Design

• Recurring attributes appear in the same sequence
  – e.g., @restriction is always the last attribute
Apply Good Design

• Only define shared attributes globally
• Defined complex types in Schema
  – ExtensionType (e.g., AdditionalData, RecordItem)
  – MLStringType (all things defined ML_STRING)
• Identical enumerated lists should be merged
  – Expectation@priority renamed to Expectation@severity
Old issues resolved in -05

• #698: Representing a Name in <Contact>
  – Replaced “name” with “ContactName”

• #551: Formalizing <RecordData>
  – Added <RecordPattern>
  – Specify a search pattern (e.g., regex, binary, xpath) starting at an offset (e.g., bytes or lines) and match the pattern n-number of times

• Standardized IncidentID@name scheme to CSIRT domain name
Other issues resolved in -05

• Derived SoftwareType for <Application> and <OperatingSystem>
  – Added fields to describe versions @{vendor, family, name, version, patch}

• Removed inconsistent approaches to dealing with internationalization
  – All multilingual capable classes (ML_STRING) have “lang” attribute (xs:language)
  – Dropped Multilingualtexttype
Other issues resolved in -05 (cont ..)

• #1144: Align <Expectation> with RID
  –@category={block,rate-limit} -{host, network, port}
  –Moved <Expectation> to <EventData> so that different expectations could be set
  –UNRESOLVED: documenting this activity in HistoryItem
#1143: Support for ICMP traffic


- Represent ICMP information in <Service> since malicious activity might use it (e.g., scanning, DoS)

**PROPOSAL:**

```
Service
+---------------------+
| STRING ip_version   |<>--{0..1}--[ port ] |
| STRING ip_protocol  |<>--{0..1}--[ portlist ] |
|                     |<>--{0..1}--[ Application ] |
|                     |<>--{0..1}--[ Type ] |
|                     |<>--{0..1}--[ Code ] |
+---------------------+
```

**STATUS:**

- Discussion required; problem is valid
#700: IANA considerations

Per RFC3733 and IANA discussions:
- Request to register “iodef” namespace
- Request to register IODEF XML Schema
- Text should reference the section number of the XML Schema

STATUS
- Must write this text
#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:
  - Existing volunteer making progress
  - Any more volunteers?
Moving Forward

• Release an -06 draft within a month
  – Ensure logical constraints in text enforced in Schema
  – Resolve the two remaining modeling issues

• Publish new diagrams

Comments?