draft-ietf-mile-rfc5070-bis-15

Roman Danyliw <rdd@cert.org>

IETF 94

November 2, 2015

What is IODEFv2?

- An XML format to represent data elements commonly exchanged by CSIRTs:
  - Computer security incident reports
  - Cyber security indicators
- Update to the Incident Object Description Exchange Format (IODEF) (RFC5070)
- IODEF is extended by various extensions
  - RFC 5901 (Phishing)
  - RFC 7203 (Structured Cybersecurity Information)
  - RFC 7495 (Reference format)
- IODEFv2 is exchanged with:
  - RID (RFC 6545 and RF C6546)
  - XMPP (draft-appala-mile-grid-00)

Drafts Since IETF 93 (Prague)

- -15 (10-16-2015)
- WGLC started on 10/17/2015

Issues Closed in -15

ID	Issue Summary	Status
#46	Missing cause of an incident	-15
#50	Provide support for "bulk observables"	-15
#38	Improve example in Section 7	2 of 3

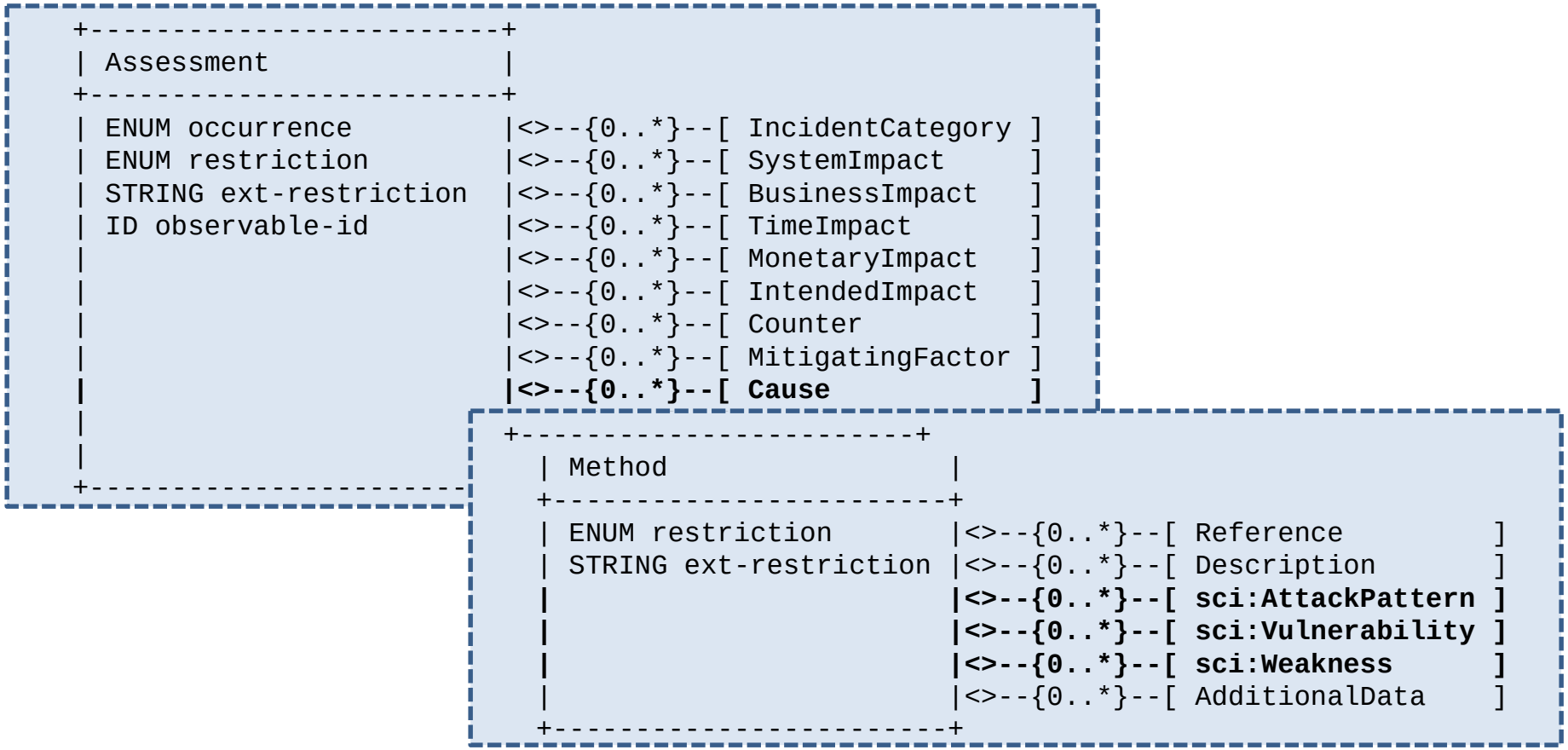
http://trac.tools.ietf.org/wg/mile/trac/report/1?asc=1&sort=ticket

Incompatibilities with v1

- IODEF-Document@version="1.00" → "2.00"
- Service@ip_protocol → @ip-protocol
- Node/Name → Node/DomainData/Name
- Node/DataTime → Node/DomainData/DateTime
- NodeRole moved to System (from Node)
- Reference class is now defined by draft-ietf-mile-enum-reference-format-11
- Impact v1 class is now SystemImpact and IncidentCategory classes
- Extending ENUM attribute with IANA registries too
- All iodef:MLStringType classes use xml:lang; all @lang attributes now xml:lang
- Counter@type → Counter@unit (there is still a @type)
- IODEF-Document@formatid → @format-id
- ReportTime is not mandatory; GenerationTime is mandatory

Issue #46: Cause of the incident

- Specify the cause of the incident



Other Changes

- Corrected text describing the line delimiter for BulkObservable (Issue #50)
- Updated Examples (Issue #38)
  - Minimal IODEF Document
  - Indicator List
- Added Certificate/Description
- Editorial fixes

Full Changelog at https://mailarchive.ietf.org/arch/msg/mile/FkxMLzqKYMofFVC1U6l4qERK5-M

Outstanding Issues

ID	Issue Summary	Status
#39	RelatedDNS documentation	
#54	Reorganize IODEF schema	All but reformatting done. Pending any final feedback.
#38	Improve example in Section 7	2 of 3 example updated.

+ General editorial review
+ Review completeness of all class write-ups
+ Consistency in the internal references to classes in declarations
+ Consistency between text diagrams-and-text
+ Consistency between all text and schema
+ Update in-document Changelog in Section 1.1
+ Review incompatibility with RFC5901

http://trac.tools.ietf.org/wg/mile/trac/report/1?asc=1&sort=ticket

Issue #54: Reformat the Schema

- Reformat the schema:
  - ✓Eliminate nested element declaration
  - ✓ Eliminate inline enumerated attribute definitions
  - ✗ Fix inconsistent white-spacing
  - ? Flexible sequencing of elements?
- Is there interesting in flexible sequencing of elements

Only valid sequence with current Schema

```
01:<IODEF-Document version="2.00" ...>
02:  <Incident purpose="reporting" ...>
03:    <IncidentID name="csirt.example.com">...
04:    <GenerationTime>2015-07-18 ...
05:    <Contact type="organization" ...>...
06:      <Email>...
07:    </Contact>
08:  </Incident>
09:</IODEF-Document>
```

Currently invalid. Should it be?

```
01:<IODEF-Document version="2.00" ...>
02:  <Incident purpose="reporting" ...>
03:    <IncidentID name="csirt.example.com">...
05:    <Contact type="organization" ...>...
06:      <Email>...
07:    </Contact>
04:    <GenerationTime>2015-07-18 ...
08:  </Incident>
09:</IODEF-Document>
```

Issue #38: Improved Examples

- Need to update the existing examples
  - http://trac.tools.ietf.org/wg/mile/trac/ticket/39
- Candidate examples:
  - ✓ Minimal IODEF-Document
  - ✓ Simple list of indicators
  - ✗ Incident Report

Issue #39: RelatedDNS

- Problem: RelatedDNS is underspecified
  - http://trac.tools.ietf.org/wg/mile/trac/ticket/39
- On the Mailing List
  - http://www.ietf.org/mail-archive/web/mile/current/msg01637.html
- Previously Discussed Representation Approaches:
  1. Use draft-hoffman-dns-in-json-02, a JSON representation
  2. A comma separated value list of DNS fields
  3. Defining RelatedDNS as iodef:AdditionalData and requiring an extension
  4. Define an alternative representation for RelatedDNS
- What ahead
  - Specify in 5070bis?
  - **Specify in another draft as an extension?**

Discussion