draft-ietf-mile-rfc5070-bis-14

Roman Danyliw <rdd@cert.org>

IETF 93

July 22, 2015

What is IODEFv2?

- An XML format to represent data elements commonly exchanged by CSIRTs:
  - Computer security incident reports
  - Cyber security indicators
- IODEFv2 is an 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)
  - draft-murillo-mile-cps-00 (Cyber Physical Incidents)
  - draft-schaad-mile-iodef-plasma-00 (Policy Framework)
  - draft-suzuki-mile-darknet-00 (Darknet Monitoring)
- IODEFv2 is exchanged with RID (RFC 6545) and ROILE (draft-field-mile-rolie)

Drafts Since IETF 92 (Dallas)

- -12 (06-18-2015)
- -13 (06-20-2015)
- -14 (07-20-2015)

Issues Closed in -12, -13 and -14

ID	Issue Summary	Status
#47	Clarify definition of iodef:SoftwareType	-13, -14
#48	Disambiguating private enumerated attribute extensions	-12, -14
#49	Clarify the uniqueness of the @translation-id scope	-12
#50	Provide support for "bulk observables"	-12, -14
#51	Distinguish between protocol and port number	-12, -14
#52	Flexibility in the rates expressed in Counter	-12
#53	Add and instance of iodef:SoftwareType to File	-12
#1	Fix internationalization	-12

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

Issue #47: Clarify `iodef:SoftwareType`

- Redefined `iodef:SoftwareType`
- Support external structured (e.g., SWID, CPE) and free-form approaches (e.g., text, URL) to reference software

```
<Application>
  <SoftwareReference spec-name="swid">
      [insert SWID XML here]
  </SoftwareReference>
</Application>
```

```
<Application>
  <SoftwareReference spec-name="cpe">
      [insert CPE XML here]
  </SoftwareReference>
</Application>
```

```
<Application>
  <SoftwareReference spec-name="custom"
                     dtype="string">
      [some text blog]
  </SoftwareReference>
</Application>
```

Issue #48: Identifying Private Extensions

- Added `IODEF-Document@private-enum-name` and `@private-enum-id`
- Uniquely identify source of private extensions

Named enum source

```
<IODEF-Document
      version="2.00"
      private-enum-name="cert.org"
...>
...
  <NodeRole category="ext-value"
            ext-category="my-value1"
...
```

Named enum source + ID

```
<IODEF-Document
      version="2.00"
      private-enum-name="cert.org"
      private-enum-id="3932"
...>
...
  <NodeRole category="ext-value"
            ext-category="my-value1"
...
```

Issue #50: List of Indicators

- Added `Observable/BulkObservable`
- Enumerate a list of commonly shared indicators

```
<BulkObservable type="fqdn">
  <BulkObservableList>
Foo.example.com
Bar.example.com
Moon.example.com
...
</BulkObservableList>
</BulkObservable>
```

Issue #51: Identifying the Service

- Added `Service/ServiceName`
- Distinguish between observed port and the service running on that port
- Identified by IANA, URL, or free-from

By IANA Service Name

```
<Service ip-protocol="6">
  <ServiceName>
    <IANAService>http</IANAService>
  </ServiceName>
  <Port>39182</Port>
   ...
</Service>
```

By Free Form Description

```
<Service ip-protocol="6">
  <ServiceName>
    <Description>
      sneaky custom malware protocol
    </Description>
  </ServiceName>
  <Port>39182</Port>
   ...
</Service>
```

Issue #52: Expressing a Rate in `Counter`

- Updated `Counter@{type, unit}`
- Express peak and average rates

Current Capability
Count of 384923 packets

```
<Counter type="count"
         unit="packet">
384923
</Counter>
```

New Capability
Peak rate of 293 Mbps

```
<Counter type="peak"
         unit="mbit"
         duration="second">
293
</Counter>
```

Other Changes

- Corrected schema to add `xml:lang` into IODEF-Document and MLStringType (per ML, http://mailarchive.ietf.org/arch/msg/mile/KyBng_nav6xMvXtLEBwjt8HP-sE)

Outstanding Issues

ID	Issue Summary	Status
#39	RelatedDNS documentation	
#46	Missing data elements from NIST SP800-61 and CERT's Handbook for CSIRTs	6 of 7 (on list)
#54	Reorganize IODEF schema	-14 (on list)
#38	Improve example in Section 7	

+ 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

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

Issue #54: Reformat the Schema

- Reformat the schema:
  - Fix inconsistent white-spacing
  - Eliminate nested element declaration
  - Eliminate inline enumerated attribute definitions
- On the Mailing List
  - https://mailarchive.ietf.org/arch/msg/mile/oKu0Q7utJKwo84TGVlbBOl8fBHk

New Style

```
<xs:element name="ThreatActor">
 <xs:complexType>
  <xs:sequence>
   <xs:choice>
    <xs:sequence>
     <xs:element ref="iodef:ThreatActorID"/>
...
</xs:element>

<xs:element name="ThreatActorID"
                       type="xs:string"/>
```

```
<xs:element name="RecordPattern">
...
  <xs:attribute name="type"
                type="recordpattern-type-type"
                use="required"/>
...
</xs:element>

<xs:simpleType name="recordpattern-type-type">
  <xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="regex"/>
...
  </xs:restriction>
</xs:simpleType>
```

Issue #46: Cause of the incident

- Need to specify the cause of the incident
  - http://trac.tools.ietf.org/wg/mile/trac/ticket/46
- On the Mailing List
  - https://mailarchive.ietf.org/arch/msg/mile/ZUSlbjlU9fLtkQeIceWpbxkLuBU
- Representation Options
  1. Use Method/AdditionalData/Weakness from the SCI draft
  2. Import the iodef-sci:Weakness class into Method
  3. Add a free-form field
  4. Add an extensible enumerated list
  5. Add a free-form field+enumerated list
  6. ?

Issue #38: Improved Examples

- Need to update the existing examples
  - http://trac.tools.ietf.org/wg/mile/trac/ticket/39
- Candidate examples:
  1. Minimal IODEF-Document
  2. Simple list of indicators
  3. Incident Report
  4. ?

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