draft-ietf-mile-rfc5070-bis-11

Roman Danyliw <rdd@cert.org>

IETF 92

March 25, 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)
  - 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 90 (Honolulu)

- -11

Issues Closed in -11

#1	Fix internationalization	-11	2013-06-14
#3	Review implementation of extending enumerated values	Revisited in -11	2013-06-14
#6	Harmonize the specification for Reference with other WG activity	Revisited in -11	2013-06-14
#29	Clarifying the scope of HashInformation@valid	Revisited in -11	2013-08-29
#44	HashData/{ds:Signature,ds:KeyInfo,ds:KeyReference} documentation	Revisited in -11	2014-02-26
#46	Missing data elements from NIST SP800-61 and CERT's Handbook for CSIRTs	6 of 7	2014-02-27

All post-IETF-87 survey items are complete

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

Issue #1: Internationalization

- Redefined iodef:MLStringType
  - @lang -> xml:lang
  - @translation-id

```
<IODEF-Document version="2.00" xml:lang="en" ...
  ...
  <Description translation-id="1"
               xml:lang="en">English</Description>
  <Description translation-id="1"
               xml:lang="de">Englisch</Description>
  <Description translation-id="1"
               xml:lang="fr">Anglais</Description>
  <Description>FooBar</Description>
```

- Redfined as xs:string
  - DomainData/Name
  - File/FileName
  - NameServers/Server
  - DomainContacts/SameDomainContact
- All iodef:MLStringType classes have a 0/1:M with parent

Issue #3: Extending Attributes

- Old Way

```
<NodeRole category="ext-value"
          ext-category="extension value"
```

- New Way
  - IANA Registry "IODEFv2→NodeRole-category"

OR

```
<NodeRole category="ext-value"
          ext-category="extension value"
```

Other Changes

- Added Incident@status

- Added File/FileType

```
<FileData>
  <File>
     ...
     <FileType>application/pdf</FileType>
```

Outstanding Issues

#38	Improve example in Section 7	TODO	2014-01-08
#39	RelatedDNS documentation	4 Options	2014-02-26
#46	Missing data elements from NIST SP800-61 and CERT's Handbook for CSIRTs	1 of 7 left	2014-02-27
#47	Clarify definition of iodef:SoftwareType	4 Options	2014-10-23

+ Various editorial changes to clean up the text and schema

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

Issue #47: `iodef:SoftwareType`

- Problem: iodef:SoftwareType is underspecified
  - http://trac.tools.ietf.org/wg/mile/trac/ticket/47
- Previously Discussed Options:
  1. Use OVAL [3]
  2. Use swid referencing ISO/IEC 19770-2:2009
  3. Don't define it and use AdditionalData
  4. Support multiple techniques to reference software in the same way (like IODEF-SCI and ENUM)

Prior Discussion: http://www.ietf.org/mail-archive/web/mile/current/msg01660.html

Issue #39: `RelatedDNS`

- Problem: RelatedDNS is underspecified
  - http://trac.tools.ietf.org/wg/mile/trac/ticket/39
- Previously Discussed Options:
  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

Prior Discussion: http://www.ietf.org/mail-archive/web/mile/current/msg01637.html

Issue #46: Cause of the incident?

- Problem: 5070bis doesn't specify the cause of the incident
  - http://trac.tools.ietf.org/wg/mile/trac/ticket/46

- Question
  - Is `iodef-sci:Weakness` sufficient?

Discussion