IODEF-extension to support structured cybersecurity information

draft-ietf-mile-sci-04.txt

Takeshi Takahashi (NICT), Kent Landfield (McAfee), Thomas Millar (US-CERT), Youki Kadobayashi (WIDE/NAIST)
Agenda

• Brief Overview of the extension

• Remaining issues
  – How to handle identifiers in the SCI draft? (How to cope with a new draft that define the usage of the identifiers?)
  – Which specifications to list as the normative / informative references?
Brief overview of the draft

This draft enables embedding structured cybersecurity information inside IODEF document.
Basic structure of the extension classes

New class name

SpecID
ext-Spec ID
contentID

Actual XML data is embedded here, if no contentID is specified

RawData

Reference (URI)

URI of the specifications (e.g. http://cve.mitre.org/cve/downloads/1.0)

It is optional. Users can this field when they want to use format that is not listed in the IANA table

AttackPattern, Vulnerability, etc.

IDs that identify the contents, e.g. cve-id, capec-id

A link to the xml data is embedded here, if no contentID/RawData is specified
Example description

Case 1: Embedding cve-id

```xml
<iodf-sci:Vulnerability SpecID="http://cve.mitre.org/cve/downloads/1.0"
VulnerabilityID="CVE-2010-3654"/>
```

Case 2: Embedding actual XML

```xml
<iodf-sci:Vulnerability SpecID="http://cve.mitre.org/cve/downloads/1.0">
 <iodf-sci:RawData dtype="xml">
  <cve xmlns="http://cve.mitre.org/cve/downloads/1.0">
   <item seq="1999-0002" name="CVE-1999-0002" type="CVE">
    ... 
   </item>
  </cve>
 </iodf-sci:RawData>
</iodf-sci:Vulnerability>
```
the list of specifications in IANA repository

The draft uses IANA registry to maintain the list of cybersecurity information formats

<table>
<thead>
<tr>
<th>Namespace</th>
<th>Specification Name</th>
<th>Ver.</th>
<th>Reference URI</th>
<th>Applicable classes</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://capec.mitre.org/observables">http://capec.mitre.org/observables</a></td>
<td>Common Attack Pattern Enumeration and Classification</td>
<td>1.6</td>
<td><a href="http://capec.mitre.org/">http://capec.mitre.org/</a></td>
<td>AttackPattern</td>
</tr>
<tr>
<td><a href="http://cce.mitre.org">http://cce.mitre.org</a></td>
<td>Common Configuration Enumeration</td>
<td>5.0</td>
<td><a href="http://cce.mitre.org/">http://cce.mitre.org/</a></td>
<td>Verification</td>
</tr>
<tr>
<td><a href="http://cee.mitre.org">http://cee.mitre.org</a></td>
<td>Common Event Expression</td>
<td>0.6</td>
<td><a href="http://cee.mitre.org/">http://cee.mitre.org/</a></td>
<td>EventReport</td>
</tr>
<tr>
<td><a href="http://cve.mitre.org/cve/downloads/1.0">http://cve.mitre.org/cve/downloads/1.0</a></td>
<td>Common Vulnerability and Exposures</td>
<td>1.0</td>
<td><a href="http://cve.mitre.org/">http://cve.mitre.org/</a></td>
<td>Vulnerability</td>
</tr>
</tbody>
</table>
Agenda

• Brief Overview of the extension

• Remaining issues
  - How to handle identifiers in the SCI draft? (How to cope with a new draft that define the usage of the identifiers?)
  - Which specifications to list as the normative / informative references?
How to handle identifiers inside SCI draft?

Current status
- The SCI draft is already capable of embedding identifiers inside its extension classes
- The detailed usage on the identifiers could be newly defined outside the draft

If the new draft is to be created…
- SCI’s usage of the identifier is supported by the newly defined draft
- The current data structure of the SCI draft will not be affected

If the new draft is not created…
- The SCI draft elaborates the usage of enumeration IDs
- The current data structure of the SCI draft will not be affected, anyway
(Just for confirmation) How to proceed?

We build a new draft on the proper usage of identifiers inside IODEF document

Yes

The new draft redefines IODEF::Reference class

No

The SCI draft describes how to handle identifiers within its scope more clearly

Yes

The structure of the SCI classes need to be reconstructed

No

The SCI classes may maintain their current structure as they are now, though review is needed
Which specifications to list as the normative / informative references?

Problems in the previous versions of the draft

- Previous versions had references that could be inappropriate as normative ones
- Normative references should be a reliable source. Thus RFC or international standards etc. are adequate

- The draft builds blank IANA table, thus specific industry specifications need not be cited as normative references any more
- The potential contents of the IANA table are listed in the draft’s appendix. Related specifications (that are neither RFC nor international standards) are cited as informative reference