

IODEF extensions for structured cybersecurity information

draft-ietf-mile-sci-06.txt

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

Issues to be done before the WGLC

- MTI issue: choose a specification for MTI

Discussion until now

- Some footsteps
 - Individual draft proposal at the IETF 81 meeting in Quebec (Jul, 2011)
 - Accepted as a working group draft at the IETF 82 meeting in Taipei
 - Copyright /IPR issues cleared at the IETF 85 meeting in Atlanta
- Content of the draft had been discussed and revised until now
 - IANA table structure
 - New class names (verification, detection, remediation etc.)
 - Normative/informative references
- MTI issue to be agreed in this meeting?

MTI specification

- **MMDEF is our choice**, according to the discussion over the mailing list
- Specifications described below, for instance, will be added to the IANA table once the draft becomes RFC
 - “Vulnerability Data Model” (draft-booth-sacm-vuln-model-01)
 - “Asset Identification” (draft-montville-sacm-asset-identification-00)

A brief overview of MMDEF

- IEEE’s specification that is available for anybody
- It describes the metadata of malware files in XML
- <http://standards.ieee.org/develop/indcon/icsg/mmdef.html>
- A tool that generate MMDEF-based XML (genMMDEF) is available online

MTI specification – example usage

- Example XML is [available here](#)
- This example XML is created following the steps as below
 - Prepare a sample zip file (“sample.zip”)
 - Generate an MMDEF XML file (“MMDEFsample.xml”) by using genMMDEF
 - Embed the XML file inside the IODEF-SCI sample file
 - Checked its validity by using MSV validator

Non-MTI spec example

```
<Method>
  <Description>An identifier of the exploited vulnerability is embedded</Description>
  <AdditionalData dtype="xml">
    <iodef-sci:Vulnerability SpecID="http://cve.mitre.org/cve/downloads/1.0" VulnerabilityID="CVE-2010-0483"/>
  </AdditionalData>
</Method>

<EventData><Record><RecordData>
  <Description>a Web-server event record</Description>
  <RecordItem dtype="xml">
    <iodef-sci:EventReport SpecID="http://cee.mitre.org">
      <iodef-sci:RawData dtype="xml">
        <cee:cee xmlns="http://cee.mitre.org/1.0/profile/" xmlns:cee="http://cee.mitre.org/1.0/"> ... </cee:cee>
      </iodef-sci:RawData>
    </iodef-sci:EventReport>
  </RecordItem>
</RecordData></Record></EventData>
```

Next steps

- What else do we need for the draft before the WGLC?

Thank you