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

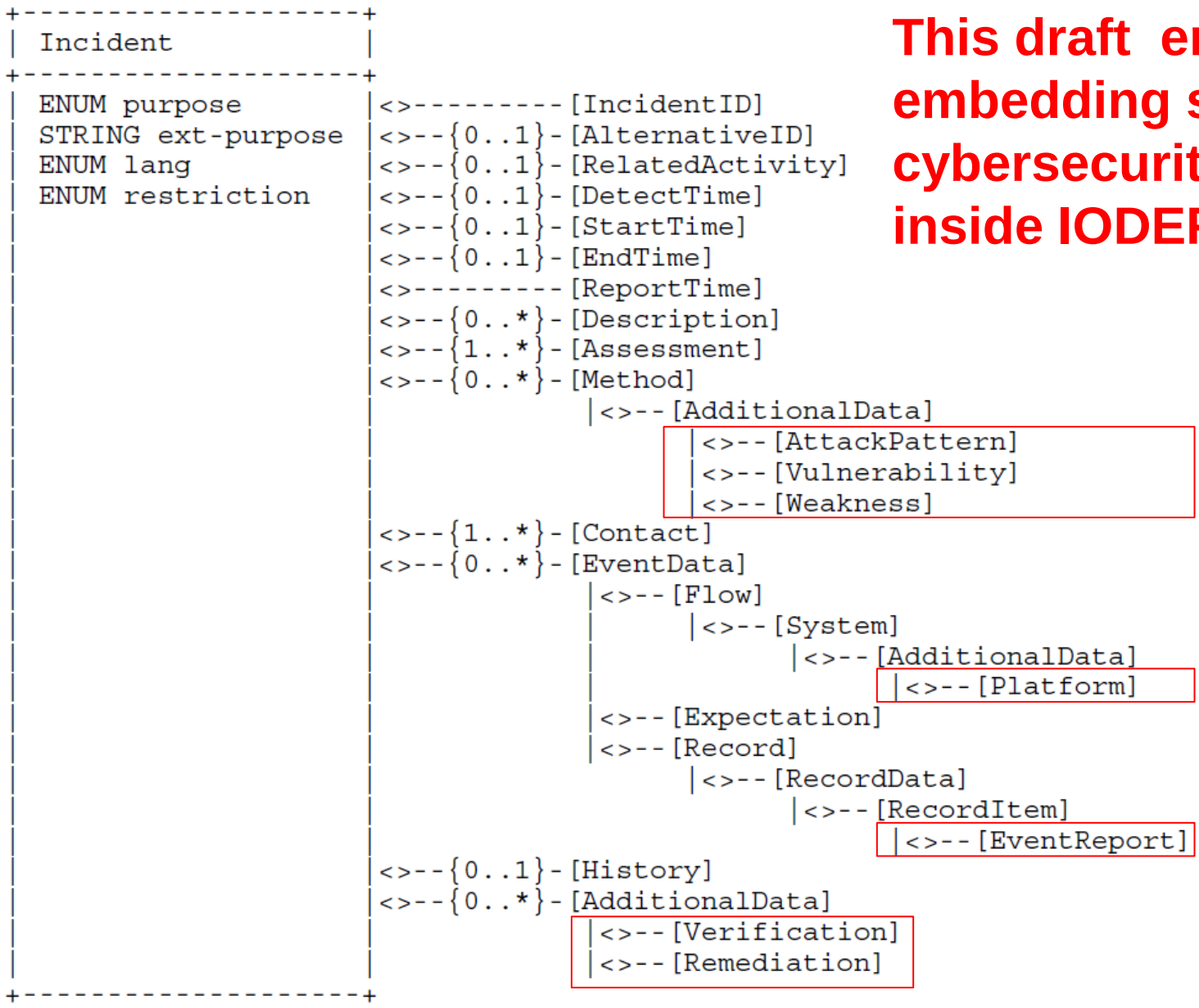
- Brief Overview of the extension

- Remaining issues

  – How to handle identifiers in the SCI draft?
  (How to cope with a new draft that define the usage of the identifiers?)

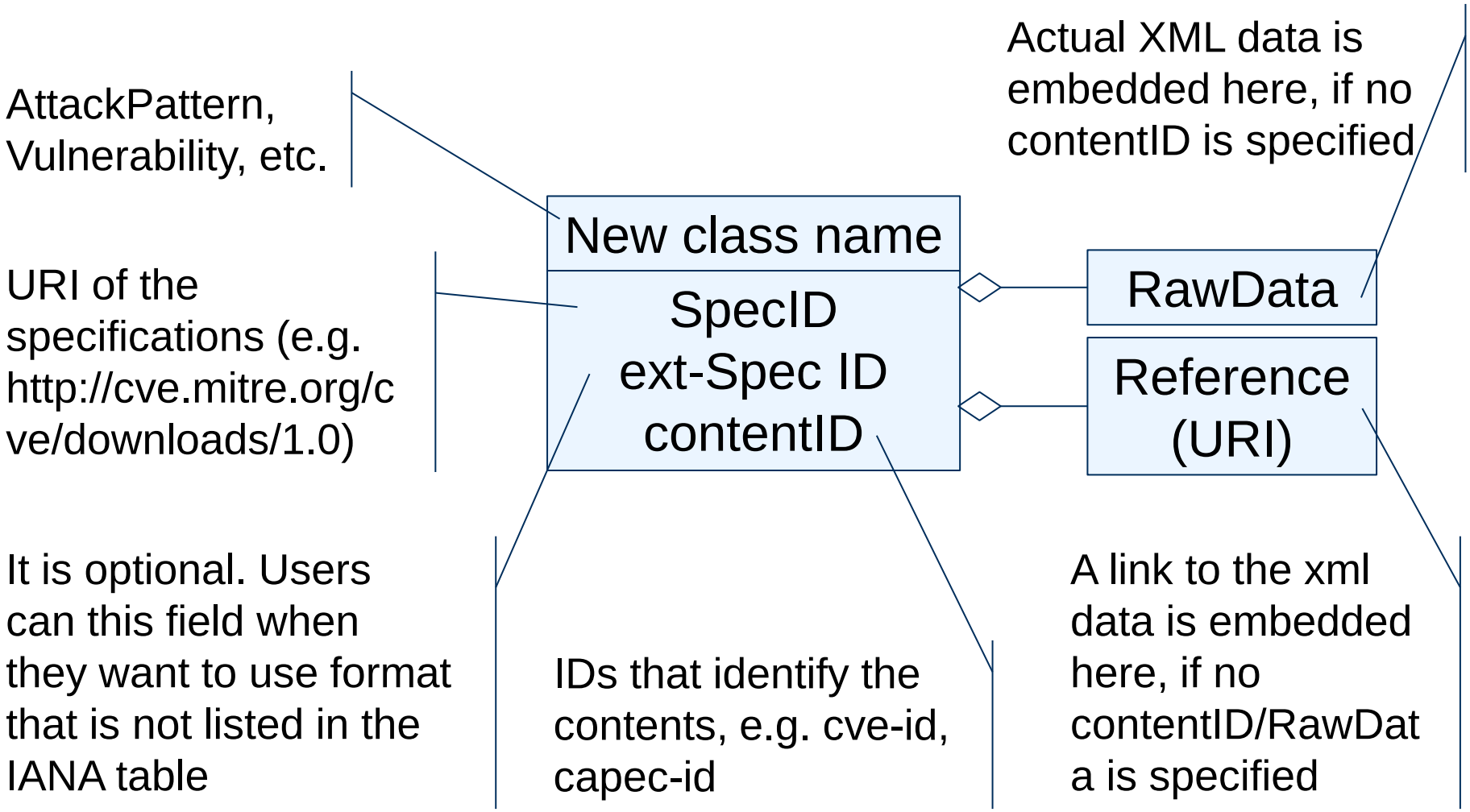
  – Which specifications to list as the normative / informative references?

Brief overview of the draft



This draft enables embedding structured cybersecurity information inside IODEF document

Basic structure of the extension classes



Example description

Case 1: Embedding cve-id

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

Case 2: Embedding actual XML

```
<iodef-sci:Vulnerability SpecID="http://cve.mitre.org/cve/downloads/1.0">
    <iodef-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>
    </iodef-sci:RawData>
</iodef-sci:Vulnerability>
```

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

Namespace	Specification Name	Ver.	Reference URI	Applicable classes
http://capec.mitre.org/observables	Common Attack Pattern Enumeration and Classification	1.6	http://capec.mitre.org/	AttackPattern
http://cce.mitre.org	Common Configuration Enumeration	5.0	http://cce.mitre.org/	Verification
http://cee.mitre.org	Common Event Expression	0.6	http://cee.mitre.org/	EventReport
http://cpe.mitre.org/dictionary/2.0	Common Platform Enumeration	2.3	http://scap.nist.gov/specifications/cpe/, http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7695	Platform
http://cve.mitre.org/cve/downloads/1.0	Common Vulnerability and Exposures	1.0	http://cve.mitre.org/	Vulnerability

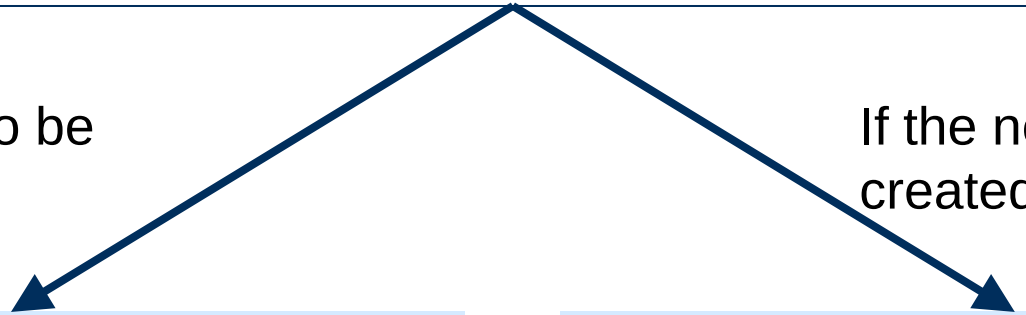
Agenda

- 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



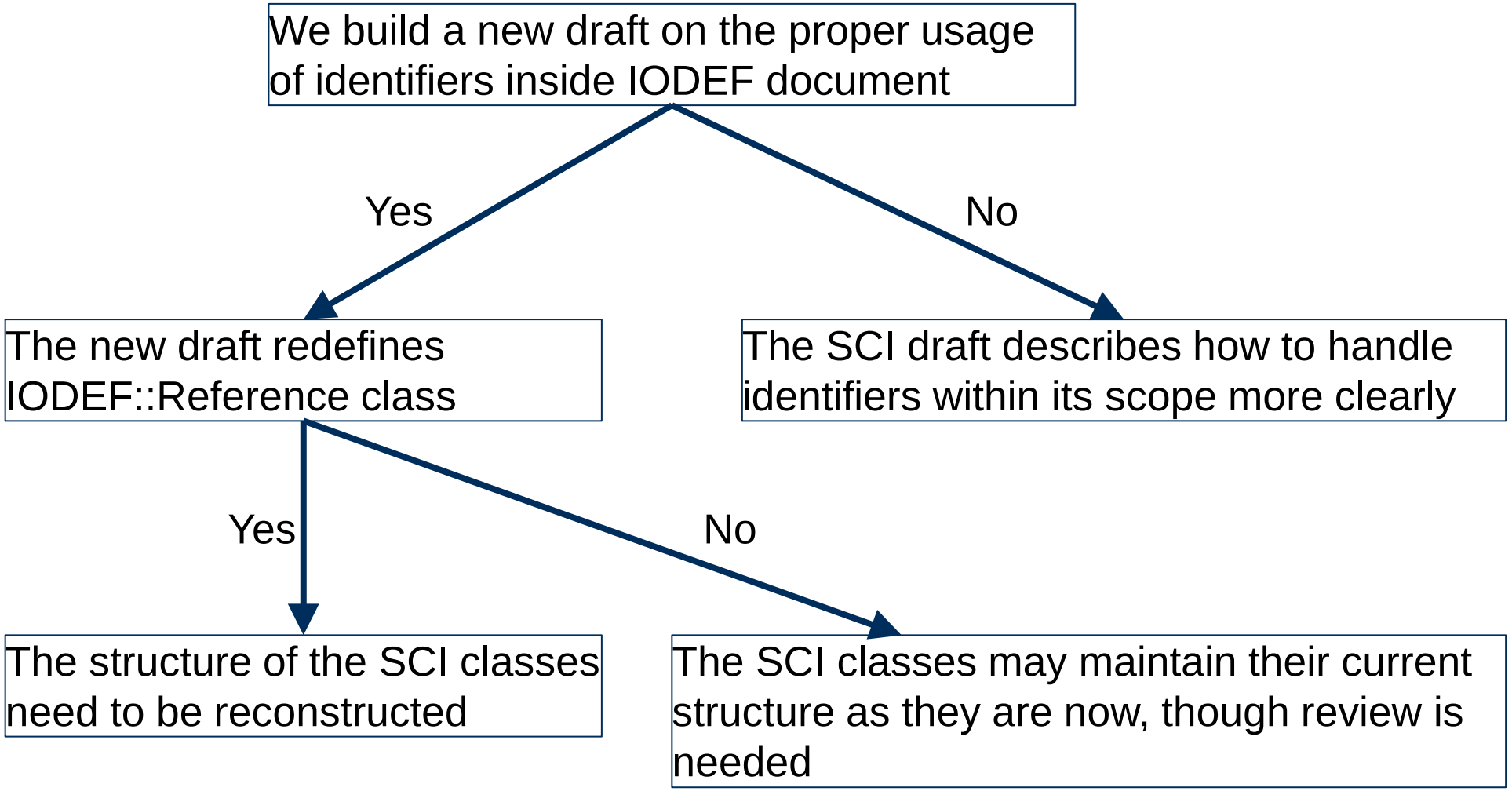
If the new draft is to be created…

- 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

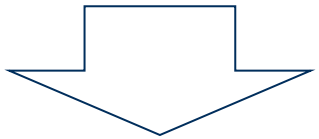
(Just for confirmation) How to proceed ?



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