IODEF-extension to support structured cybersecurity information

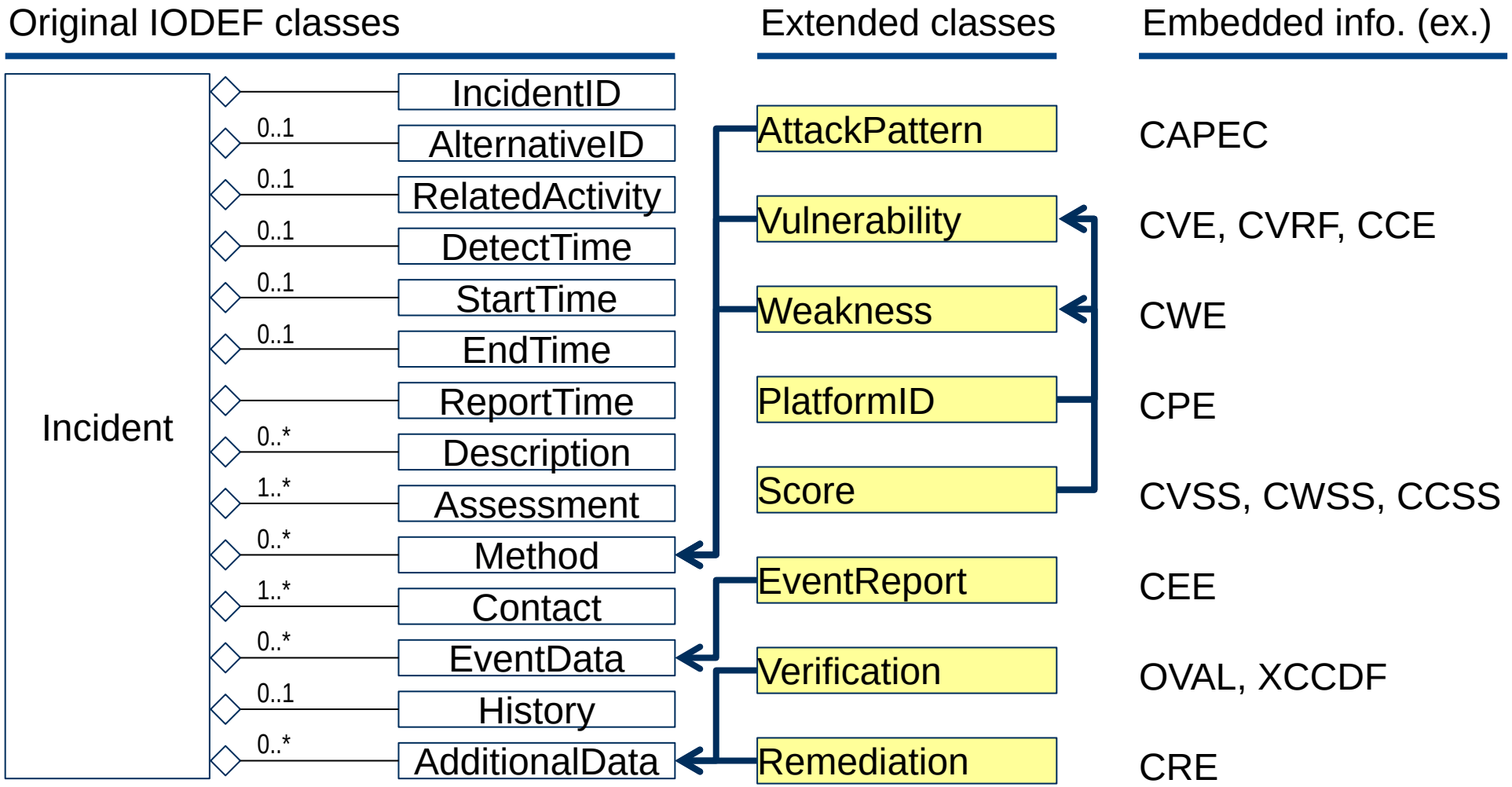
draft-ietf-mile-sci-05.txt

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

Remaining issues

- Specifications in the IANA table
- IPR statement (mainly trademark)
- Test/example code

This draft provides a means to embed structured cybersecurity information inside IODEF document

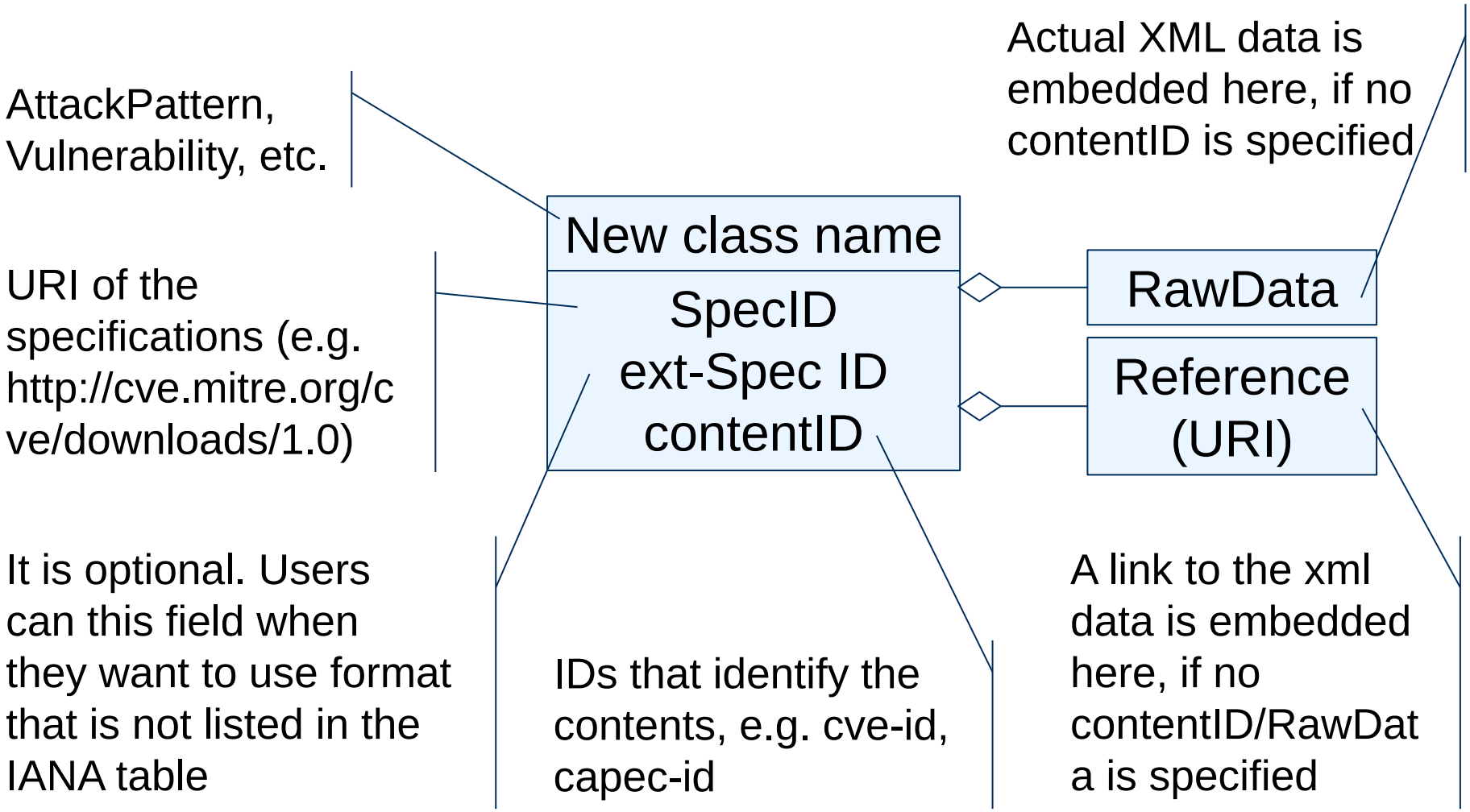


Example: a sensor sends incident info with logs

```
<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>
```

Basic structure of the extension classes



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				
http				
http dict				
http cve				

Currently, the IANA table is empty, as we agreed in the previous meeting.
There is no normative reference of these specifications.

Trademark issue

- All the specifications are removed from the normative references and the IANA table
- The appendices describes these specifications with informative references to them
- Trademark declaration attached there

10. Appendix II: Candidate Specifications for the IANA Table

This draft defined the structure of the IANA table in Section 4.1. Though the management of the table is up to IANA, this appendix provides candidate entries. Note that OVAL and CVE are registered trademarks, and CAPEC, CCE, CEE, CPE, CWE, CWSS, MAEC, and OCIL are trademarks, of The MITRE Corporation.

Next steps

- Describe several use cases inside the draft
- Join discussion in SACM so that description techniques become RFCs

Thank you