IODEF-extension to support structured cybersecurity information

draft-takahashi-mile-sci-02.txt

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

Agenda

- Brief Overview of the extension

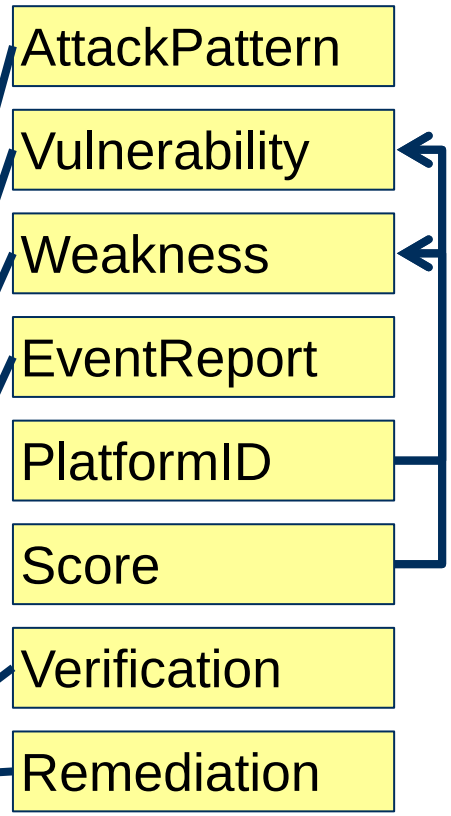
- Discussion issues

The extension enables embedding structured cybersecurity information inside IODEF document

Original IODEF

```
+---------------------+
| Incident            |
+---------------------+
| ENUM purpose        |<>----------[ IncidentID      ]
| STRING ext-purpose  |<>--{0..1}--[ AlternativeID   ]
| ENUM lang           |<>--{0..1}--[ RelatedActivity ]
| ENUM restriction    |<>--{0..1}--[ DetectTime      ]
|                     |<>--{0..1}--[ StartTime       ]
|                     |<>--{0..1}--[ EndTime         ]
|                     |<>----------[ ReportTime      ]
|                     |<>--{0..*}--[ Description     ]
|                     |<>--{1..*}--[ Assessment      ]
|                     |<>--{0..*}--[ Method          ]
|                     |<>--{1..*}--[ Contact         ]
|                     |<>--{0..*}--[ EventData       ]
|                     |<>--{0..1}--[ History         ]
|                     |<>--{0..*}--[ AdditionalData  ]
+---------------------+
```

Extensions



Source: http://tools.ietf.org/html/draft-takahashi-mile-sci-02

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

ID	Specification Name	Ver.	Namespace
CAPEC_1.6	Common Attack Pattern Enumeration and Classification	1.6	http://capec.mitre.org/observables
CEE_0.6	Common Event Expression	0.6	http://cee.mitre.org
CPE_2.3	Common Platform Enumeration	2.3	http://cpe.mitre.org/dictionary/2.0
CVE_1.0	Common Vulnerability and Exposures	1.0	http://cve.mitre.org/cve/downloads/1.0
CVRF_1.0	Common Vulnerability Reporting Format	1.0	http://www.icasi.org/CVRF/schema/cvrf/1.0
CVSS_2.0	Common Vulnerability Scoring System	2	http://scap.nist.gov/schema/cvss-v2/1.0
CWE_5.0	Common Weakness Enumeration	5.1	N/A
CWSS_0.8	Common Weakness Scoring System	0.8	N/A
OCIL_2.0	Open Checklist Interactive Language	2.0	http://scap.nist.gov/schema/ocil/2.0
OVAL_5.10	Open Vulnerability and Assessment Language	5.10	http://oval.mitre.org/XMLSchema/oval-definitions-5
XCCDF_1.2	Extensible Configuration Checklist Description Format	1.2	http://checklists.nist.gov/xccdf/1.2

Agenda

- Brief Overview of the extension

- Discussion issues

Discussion Issues

- Applicable specifications for each class **1**
- Guideline for the IANA expert review **2**
- Verification/Remediation class **3**

Applicable specifications for each class

New Addition

ID	Specification Name	Ver.	Namespace	Applicable Class
CAPEC_1.6	Common Attack Pattern Enumeration and Classification	1.6	http://capec.mitre.org/observables	AttackPattern
CEE_0.6	Common Event Expression	0.6	http://cee.mitre.org	EventReport
CPE_2.3	Common Platform Enumeration	2.3	http://cpe.mitre.org/dictionary/2.0	PlatformID
CVE_1.0	Common Vulnerability and Exposures	1.0	http://cve.mitre.org/cve/downloads/1.0	Vulnerability
CVRF_1.0	Common Vulnerability Reporting Format	1.0	http://www.icasi.org/CVRF/schema/cvrf/1.0	Vulnerability
CVSS_2.0	Common Vulnerability Scoring System	2	http://scap.nist.gov/schema/cvss-v2/1.0	Scoring
CWE_5.0	Common Weakness Enumeration	5.1	N/A	Weakness
CWSS_0.8	Common Weakness Scoring System	0.8	N/A	Scoring
OCIL_2.0	Open Checklist Interactive Language	2.0	http://scap.nist.gov/schema/ocil/2.0	Verification
OVAL_5.10	Open Vulnerability and Assessment Language	5.10	http://oval.mitre.org/XMLSchema/oval-definitions-5	Verification
XCCDF_1.2	Extensible Configuration Checklist Description Format	1.2	http://checklists.nist.gov/xccdf/1.2	Verification

Guideline for the IANA expert review

Discussion issues	Direction
• What would be the criteria for accepting new specification registration?	• "Specification Required" : any registration is accompanied by a public specification for the standard that has been registered • Confirm three independent and interoperable implementations
• What would be the criteria for a new version registration?	• The same as above

Verification/Remediation class

Discussion issues

- Version 2 of the draft has the class, called “Remediation”, which seems to be inappropriate name

Direction

- I would suggest to have both “Verification” and “Remediation” classes
  - Verification class could be represented by OVAL and XCCDF
  - Remediation class could be represented by CRE

Thank you