

MILE Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 30, 2012

T. Takahashi
NICT
K. Landfield
McAfee
T. Millar
USCERT
Y. Kadobayashi
NAIST
Dec 28, 2011

IODEF-extension to support structured cybersecurity information
draft-ietf-mile-sci-01.txt

Abstract

This document extends the Incident Object Description Exchange Format (IODEF) defined in RFC 5070 [RFC5070] to facilitate enriched cybersecurity information exchange among cybersecurity entities by embedding structured information formatted by specifications, including CAPEC[TM] [CAPEC], CEE[TM] [CEE], CPE[TM] [CPE], CVE(R) [CVE], CVRF [CVRF], CVSS [CVSS], CWE[TM] [CWE], CWSS[TM] [CWSS], OCIL [OCIL], OVAL(R) [OVAL], and XCCDF [XCCDF].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 30, 2012.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	4
2.	Terminology	4
3.	Applicability	4
4.	Extension Definition	5
4.1.	IDs for Structured Cybersecurity Information Specifications	5
4.1.1.	CAPEC_1.6	6
4.1.2.	CCE_5.0	6
4.1.3.	CCSS_1.0	7
4.1.4.	CEE_0.6	7
4.1.5.	CPE_Ref_2.3	7
4.1.6.	CPE_Dic_2.3	8
4.1.7.	CVE_1.0	8
4.1.8.	CVRF_1.0	8
4.1.9.	CVSS_2.0	9
4.1.10.	CWE_5.0	9
4.1.11.	CWSS_0.8	9
4.1.12.	OCIL_2.0	9
4.1.13.	OVAL_Def_5.10.1	10
4.1.14.	OVAL_Res_5.10.1	10
4.1.15.	OVAL_Com_5.10.1	10
4.1.16.	XCCDF_1.2	11
4.2.	Extended Classes	11
4.2.1.	AttackPattern	12
4.2.2.	PlatformID	14
4.2.3.	Vulnerability	15
4.2.4.	Scoring	16
4.2.5.	Weakness	17
4.2.6.	EventReport	19
4.2.7.	Verification	20
4.2.8.	Remediation	21
5.	Examples	22
5.1.	Reporting an attack	22
6.	Security Considerations	25
6.1.	Transport-Specific Concerns	25
6.2.	Using the iodef:restriction Attribute	25
7.	IANA Considerations	26
8.	Acknowledgment	27
9.	Appendix I: XML Schema Definition for Extension	28
10.	References	32
10.1.	Normative References	32
10.2.	Informative References	33
	Authors' Addresses	34

1. Introduction

Cyber attacks are getting more sophisticated, and their numbers are increasing day by day. To cope with such situation, incident information needs to be reported, exchanged, and shared among organizations. IODEF is one of the tools enabling such exchange, and is already in use.

To efficiently run cybersecurity operations, these exchanged information needs to be machine-readable. IODEF provides a structured means to describe the information, but it needs to embed various non-structured such information in order to convey detailed information. Further structure within IODEF increases IODEF documents' machine-readability and thus facilitates streamlining cybersecurity operations.

On the other hand, there exist various other activities facilitating detailed and structured description of cybersecurity information, major of which includes CAPEC [CAPEC], CEE [CEE], CPE [CPE], CVE [CVE], CVRF [CVRF], CVSS [CVSS], CWE [CWE], CWSS [CWSS], OCIL [OCIL], OVAL [OVAL], and XCCDF [XCCDF]. Since such structured description facilitates cybersecurity operations, it would be beneficial to embed and convey these information inside IODEF document.

To enable that, this document extends the IODEF to embed and convey various structured cybersecurity information, with which cybersecurity operations can be facilitated. Since IODEF defines a flexible and extensible format and supports a granular level of specificity, this document defines an extension to IODEF instead of defining a new report format. For clarity, and to eliminate duplication, only the additional structures necessary for describing the exchange of such structured information are provided.

2. Terminology

The terminology used in this document follows the one defined in RFC 5070 [RFC5070].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Applicability

To maintain cybersecurity, organization needs to exchange cybersecurity information, which includes the following information:

attack pattern, platform information, vulnerability and weakness, countermeasure instruction, computer event log, and the severity.

IODEF provides a scheme to exchange such information among interested parties. However, the detailed common format to describe such information is not defined in the IODEF base document.

On the other hand, to describe those information and to facilitate exchange, a structured format for that is already available. Major of them are CAPEC, CEE, CPE, CVE, CVRF, CVSS, CWE, CWSS, OCIL, OVAL, and XCCDF. By embedding them into the IODEF document, the document can convey more detailed contents to the receivers, and the document can be easily reused. Note that interactive communication is needed in some cases, and some of these structured information such as OCIL solicits reply from recipients. These reply could be also embedded inside the IODEF document.

These structured cybersecurity information facilitates cybersecurity operation at the receiver side. Since the information is machine-readable, the data can be processed by computers. That expedites the automation of cybersecurity operations

For instance, an organization wishing to report a security incident wants to describe what vulnerability was exploited. Then the sender can simply use IODEF, where an CAPEC record is embedded instead of describing everything in free format text. Receiver can also identify the needed details of the attack pattern by looking up some of the xml [XML1.0] tags defined by CAPEC. Receiver can accumulate the attack pattern information (CAPEC record) in its database and could distribute it to the interested parties if needed, without needing human interventions.

4. Extension Definition

This draft extends IODEF to embed structured cybersecurity information by introducing new classes, with which these information can be embedded inside IODEF document as element contents of AdditionalData and RecordItem classes.

4.1. IDs for Structured Cybersecurity Information Specifications

This extension embeds structured cybersecurity information from external specifications. The initial list of supported specifications is in Figure 1 below, followed by a subsection for each specification that lists the ID, specification name, version, namespace [XMLNames], specification URI and applicable classes for each specification. Future assignments are to be managed by IANA

using the Expert Review [RFC5226] and Specification Required [RFC5226] allocation policies as further specified in Section 7.

ID	Specification Name
CAPEC_1.6	Common Attack Pattern Enumeration and Classification
CCE_5.0	Common Configuration Enumeration
CCSS_1.0	Common Configuration Scoring System
CEE_0.6	Common Event Expression
CPE_Ref_2.3	Common Platform Enumeration Reference
CPE_Dic_2.3	Common Platform Enumeration Dictionary
CVE_1.0	Common Vulnerability and Exposures
CVRF_1.0	Common Vulnerability Reporting Format
CVSS_2.0	Common Vulnerability Scoring System
CWE_5.0	Common Weakness Enumeration
CWSS_0.8	Common Weakness Scoring System
OCIL_2.0	Open Checklist Interactive Language
OVAL_Def_5.10.1	Open Vulnerability and Assessment Language Definitions
OVAL_Res_5.10.1	Open Vulnerability and Assessment Language Results
OVAL_Com_5.10.1	Open Vulnerability and Assessment Language Common
XCCDF_1.2	Extensible Configuration Checklist Description Format

Figure 1: List of specification IDs

4.1.1. CAPEC_1.6

ID: CAPEC_1.6

Specification Name: Common Attack Pattern Enumeration and Classification

Version: 1.6

Namespace: <http://capec.mitre.org/observables>

Specification URI: <http://capec.mitre.org/>

Applicable Classes: AttackPattern

4.1.2. CCE_5.0

ID: CCE_5.0

Specification Name: Common Configuration Enumeration

Version: 5.0

Namespace: <http://cce.mitre.org>

Specification URI: TBD

Applicable Classes: Remediation

4.1.3. CCSS_1.0

ID: CCSS_1.0

Specification Name: Common Configuration Scoring System

Version: 1.0

Namespace: N/A

Specification URI: TBD

Applicable Classes: Scoring

4.1.4. CEE_0.6

ID: CEE_0.6

Specification Name: Common Event Expression

Version: 0.6

Namespace: <http://cee.mitre.org>

Specification URI: <http://cee.mitre.org/>

Applicable Classes: EventReport

4.1.5. CPE_Ref_2.3

ID: CPE_Ref_2.3

Specification Name: Common Platform Enumeration Reference

Version: 2.3

Namespace: <http://cpe.mitre.org/language/2.0>

Specification URI: <http://cpe.mitre.org/>

Applicable Classes: PlatformID

4.1.6. CPE_Dic_2.3

ID: CPE_Dic_2.3

Specification Name: Common Platform Enumeration Dictionary

Version: 2.3

Namespace: <http://cpe.mitre.org/language/2.0>

Specification URI: TBD

Applicable Classes: PlatformID

4.1.7. CVE_1.0

ID: CVE_1.0

Specification Name: Common Vulnerability and Exposures

Version: 1.0

Namespace: <http://cve.mitre.org/cve/downloads/1.0>

Specification URI: <http://cve.mitre.org/>

Applicable Classes: Vulnerability

4.1.8. CVRF_1.0

ID: CVRF_1.0

Specification Name: Common Vulnerability Reporting Format

Version: 1.0

Namespace: <http://www.icas.org/CVRF/schema/cvrf/1.0>

Specification URI: <http://www.icas.org/cvrf>

Applicable Classes: Vulnerability

4.1.9. CVSS_2.0

ID: CVSS_2.0

Specification Name: Common Vulnerability Scoring System

Version: 2

Namespace: <http://scap.nist.gov/schema/cvss-v2/1.0>

Specification URI: <http://www.first.org/cvss>

Applicable Classes: Scoring

4.1.10. CWE_5.0

ID: CWE_5.0

Specification Name: Common Weakness Enumeration

Version: 5.1

Namespace: N/A

Specification URI: <http://cwe.mitre.org/>

Applicable Classes: Weakness

4.1.11. CWSS_0.8

ID: CWSS_0.8

Specification Name: Common Weakness Scoring System

Version: 0.8

Namespace: N/A

Specification URI: <http://cwe.mitre.org/cwss/>

Applicable Classes: Scoring

4.1.12. OCIL_2.0

ID: OCIL_2.0

Specification Name: Open Checklist Interactive Language

Version: 2.0

Namespace: <http://scap.nist.gov/schema/ocil/2.0>

Specification URI: <http://scap.nist.gov/specifications/ocil/>

Applicable Classes: Verification

4.1.13. OVAL_Def_5.10.1

ID: OVAL_Def_5.10.1

Specification Name: Open Vulnerability and Assessment Language

Version: 5.10.1

Namespace: <http://oval.mitre.org/XMLSchema/oval-definitions-5>

Specification URI: <http://oval.mitre.org/>

Applicable Classes: Verification

4.1.14. OVAL_Res_5.10.1

ID: OVAL_Res_5.10.1

Specification Name: Open Vulnerability and Assessment Language

Version: 5.10.1

Namespace: <http://oval.mitre.org/XMLSchema/oval-results-5>

Specification URI: TBD

Applicable Classes: Verification

4.1.15. OVAL_Com_5.10.1

ID: OVAL_Com_5.10.1

Specification Name: Open Vulnerability and Assessment Language

Version: 5.10.1

Namespace: <http://oval.mitre.org/XMLSchema/oval-common-5>

Specification URI: TBD

Applicable Classes: Verification

4.1.16. XCCDF_1.2

ID: XCCDF_1.2

Specification Name: Extensible Configuration Checklist Description
Format

Version: 1.2

Namespace: <http://checklists.nist.gov/xccdf/1.2>

Specification URI: <http://scap.nist.gov/specifications/xccdf/>

Applicable Classes: Verification

4.2. Extended Classes

The IODEF Incident element [RFC5070] is summarized below. It is expressed in Unified Modeling Language (UML) syntax as used in the IODEF specification. The UML representation is for illustrative purposes only; elements are specified in XML as defined in Appendix A.

```

+-----+
| 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]
| | <>--[AdditionalData]
| | | <>--[AttackPattern]
| | | <>--[Vulnerability]
| | | <>--[Weakness]
| <>--{1..*}-[Contact]
| <>--{0..*}-[EventData]
| | <>--[Flow]
| | | <>--[System]
| | | | <>--[AdditionalData]
| | | | <>--[PlatformID]
| | <>--[Expectation]
| | <>--[Record]
| | | <>--[RecordData]
| | | | <>--[RecordItem]
| | | | <>--[EventReport]
| <>--{0..1}-[History]
| <>--{0..*}-[AdditionalData]
| | <>--[Verification]
| | <>--[Remediation]
+-----+

```

Figure 2: Incident class

This extension defines the following seven elements.

4.2.1. AttackPattern

An AttackPattern consists of an extension to the Incident.Method.AdditionalData element with a dtype of "xml". The extension describes attack patterns of incidents or events.

It is recommended that Method class SHOULD contain one or more of the extension elements whenever available.

An AttackPattern class is structured as follows.

```

+-----+
| AttackPattern          |
+-----+
| STRING Version         | <>--(0..*)-[ RawData ]
| ENUM SpecificationID   | <>--(0..*)-[ Reference ]
| STRING AttackPatternID | <>--(0..*)-[ PlatformID ]
+-----+

```

Figure 3: AttackPattern class

This class has the following attributes.

Version: OPTIONAL. STRING. The version number of the extension specification to which this class conforms. This value should be 1.00, to be compliant with this document. Its default value is 1.00.

SpecificationID: REQUIRED. ENUM. The ID of the specification and its version specifying the format of the RawData element. The value should be chosen from the IDs listed in Figure 1, such as CAPEC_1.6. Note that the lists in Figure 1 will be developed further by IANA.

AttackPatternID: OPTIONAL. STRING. An ID of an attack pattern to be reported. This attribute SHOULD be used whenever such ID is available. In case a RawData or Reference element is provided along with this attribute, writers/senders MUST ensure that this ID is consistent with the one provided by the element; if a reader/receiver detects an inconsistency, it SHOULD prefer the value of this attribute, and SHOULD log the inconsistency so a human can correct the problem. Note that this attribute could be omitted if no such ID is available. In this case, either RawData or Reference elements, or both of them, MUST be provided.

The AttackPattern class is composed of the following aggregate classes.

RawData: Zero or more. xml. A complete document that is formatted according to the specification and its version identified by the value of the SpecificationID with the Figure 1.

Reference: Zero or more of iodef:Reference [RFC5070]. This element allows an IODEF document to include a link to a structured information instead of directly embedding it into a RawData element.

PlatformID: Zero or more. An identifier of software platform involved in the specific attack pattern, which is elaborated in Section 4.2.2. Some of the structured information embedded in the RawData element may include the identifier within it. In this case, this PlatformID element SHOULD NOT be used. If a reader/receiver detects the identifiers in both RawData and PlatformID elements and their inconsistency, it SHOULD prefer the identifiers derived from the PlatformID element, and SHOULD log the inconsistency so a human can correct the problem.

Writers/senders MUST ensure the specification name and version identified by the SpecificationID are consistent with the contents of the RawData; if a reader/receiver detects an inconsistency, it SHOULD prefer the specification name and version derived from the content, and SHOULD log the inconsistency so a human can correct the problem.

4.2.2. PlatformID

A PlatformID identifies a software platform. It is recommended that AttackPattern, Vulnerability, Weakness, and System classes contain this elements whenever available.

A PlatformID element is structured as follows.

```
+-----+
| PlatformID          |
+-----+
| STRING Version      | <>--(1..*)-[ ID ]
| ENUM SpecificationID |
+-----+
```

Figure 4: PlatformID class

This class has the following attributes.

Version: OPTIONAL. STRING. The version number of the extension specification to which this class conforms. This value should be 1.00, to be compliant with this document. Its default value is 1.00.

SpecificationID: REQUIRED. ENUM. The ID of the specification and its version specifying the format of the ID element. The value should be chosen from the IDs listed in Figure 1, such as CPE_2.3 and ISO/IEC 19770-2. Note that the lists in Figure 1 will be developed further by IANA.

This class is composed of the following aggregate classes.

ID: One or more. ML_STRING. An ID that is formatted according to the rule defined by the specification and its version identified by the value of the SpecificationID with the Figure 1.

Writers/senders MUST ensure the specification name and version identified by the SpecificationID are consistent with the contents of the ID; if a reader/receiver detects an inconsistency, it SHOULD prefer the specification name and version derived from the content, and SHOULD log the inconsistency so a human can correct the problem.

4.2.3. Vulnerability

A Vulnerability consists of an extension to the Incident.Method.AdditionalData element with a dtype of "xml". The extension describes the (candidate) vulnerabilities of incidents or events.

It is recommended that Method class SHOULD contain one or more of the extension elements whenever available.

A Vulnerability element is structured as follows.

```
+-----+
| Vulnerability          |
+-----+
| STRING Version         | <>--(0..*)-[ RawData ]
| ENUM SpecificationID   | <>--(0..*)-[ Reference ]
| STRING VulnerabilityID | <>--(0..*)-[ PlatformID ]
|                        | <>--(0..*)-[ Scoring ]
+-----+
```

Figure 5: Vulnerability class

This class has the following attributes.

Version: OPTIONAL. STRING. The version number of the extension specification to which this class conforms. This value should be 1.00, to be compliant with this document. Its default value is 1.00.

SpecificationID: REQUIRED. ENUM. The ID of the specification and its version specifying the format of the RawData element. The value should be chosen from the IDs listed in Figure 1, such as CVE_1.0 and CVRF_1.0. Note that the lists in Figure 1 will be developed further by IANA.

VulnerabilityID: OPTIONAL. STRING. An ID of a vulnerability to be reported. This attribute SHOULD be used whenever such ID is available. In case a RawData or Reference element is provided along with this attribute, writers/senders MUST ensure that this ID is consistent with the one provided by the element; if a reader/receiver detects an inconsistency, it SHOULD prefer the value of this attribute, and SHOULD log the inconsistency so a human can correct the problem. Note that this attribute could be omitted if no such ID is available. In this case, either RawData or Reference elements, or both of them, MUST be provided.

This class is composed of the following aggregate classes.

RawData: Zero or one. xml. A complete document that is formatted according to the specification and its version identified by the value of the SpecificationID with the Figure 1.

Reference: Zero or one of iodef:Reference [RFC5070]. This element allows an IODEF document to include a link to a structured information instead of directly embedding it into a RawData element.

PlatformID: Zero or more. An identifier of software platform affected by the vulnerability, which is elaborated in Section 4.2.2. Some of the structured information embedded in the RawData element may include the identifier within it. In this case, this PlatformID element SHOULD NOT be used. If a reader/receiver detects the identifiers in both RawData and PlatformID elements and their inconsistency, it SHOULD prefer the identifiers derived from the PlatformID element, and SHOULD log the inconsistency so a human can correct the problem.

Scoring: Zero or more. An indicator of the severity of the vulnerability, such as CVSS and CCSS scores, which is elaborated in Section 4.2.4. Some of the structured information may include scores within it. In this case, the Scoring element SHOULD NOT be used since the RawData element contains the scores. If a reader/receiver detects scores in both RawData and Scoring elements and their inconsistency, it SHOULD prefer the scores derived from the RawData element, and SHOULD log the inconsistency so a human can correct the problem.

4.2.4. Scoring

A Scoring class describes the scores of the severity in terms of security. It is recommended that Vulnerability and Weakness classes contain the elements whenever available.

A Scoring class is structured as follows.

```

+-----+
| Scoring |
+-----+
| STRING Version | <>-----[ Score ]
| ENUM SpecificationID |
+-----+

```

Figure 6: Scoring class

This class has two attributes.

Version: OPTIONAL. STRING. The version number of the extension specification to which this class conforms. This value should be 1.00, to be compliant with this document. Its default value is 1.00.

SpecificationID: REQUIRED. STRING. The ID of the specification and its version specifying the format of the Score element. The value should be chosen from the IDs listed in Figure 1, such as CCSS, CVSS_2.0 and CWSS_0.8. Note that the lists in Figure 1 will be developed further by IANA.

This class is composed of an aggregate class.

Score: One. xml. Arbitrary information structured by the specification identified by the specification and its version identified by the value of the SpecificationID with the Figure 1.

Writers/senders MUST ensure the specification name and version identified by the SpecificationID are consistent with the contents of the Score; if a reader/receiver detects an inconsistency, it SHOULD prefer the specification name and version derived from the content, and SHOULD log the inconsistency so a human can correct the problem.

4.2.5. Weakness

A Weakness consists of an extension to the Incident.Method.AdditionalData element with a dtype of "xml". The extension describes the weakness types of incidents or events.

It is recommended that Method class SHOULD contain one or more of the extension elements whenever available.

A Weakness element is structured as follows.

```

+-----+
| Weakness |
+-----+
| STRING Version | <>--(0..*)-[ RawData ]
| ENUM SpecificationID | <>--(0..*)-[ Reference ]
| STRING WeaknessID | <>--(0..*)-[ PlatformID ]
| | <>--(0..*)-[ Scoring ]
+-----+

```

Figure 7: Weakness class

This class has the following attributes.

Version: OPTIONAL. STRING. The version number of the extension specification to which this class conforms. This value should be 1.00, to be compliant with this document. Its default value is 1.00.

SpecificationID: REQUIRED. ENUM. The ID of the specification and its version specifying the format of the RawData element. The value should be chosen from the IDs listed in Figure 1, such as CWE_5.0. Note that the lists in Figure 1 will be developed further by IANA.

WeaknessID: OPTIONAL. STRING. An ID of a weakness to be reported. This attribute SHOULD be used whenever such ID is available. In case a RawData or Reference elements is provided along with this attribute, writers/senders MUST ensure that this ID is consistent with the one provided by the element; if a reader/receiver detects an inconsistency, it SHOULD prefer the value of this attribute, and SHOULD log the inconsistency so a human can correct the problem. Note that this attribute could be omitted if no such ID is available. In this case, either RawData or Reference elements, or both of them, MUST be provided.

This class is composed of the following aggregate classes.

RawData: Zero or more. xml. A complete document that is formatted according to the specification and its version identified by the value of the SpecificationID with the Figure 1.

Reference: Zero or one of iodef:Reference [RFC5070]. This element allows an IODEF document to include a link to a structured information instead of directly embedding it into a RawData element.

PlatformID: Zero or more. An identifier of software platform affected by the weakness, which is elaborated in Section 4.2.2. Some of the structured information embedded in the RawData element may include the identifier within it. In this case, this PlatformID element SHOULD NOT be used. If a reader/receiver detects the identifiers in both RawData and PlatformID elements and their inconsistency, it SHOULD prefer the identifiers derived from the PlatformID element, and SHOULD log the inconsistency so a human can correct the problem.

Scoring: Zero or more. An indicator of the severity of the weakness, such as CWSS score, which is elaborated in Section 4.2.4. Some of the structured information may include scores within it. In this case, the Scoring element SHOULD NOT be used since the RawData element contains the scores. If a reader/receiver detects scores in both RawData and Scoring elements and their inconsistency, it SHOULD prefer the scores derived from the RawData element, and SHOULD log the inconsistency so a human can correct the problem.

4.2.6. EventReport

An EventReport consists of an extension to the Incident.EventData.Record.RecordData.RecordItem element with a dtype of "xml". The extension embeds structured event reports.

It is recommended that RecordItem class SHOULD contain one or more of the extension elements whenever available.

An EventReport element is structured as follows.

```
+-----+
| EventReport          |
+-----+
| STRING Version       | <>--(0..*)-[ RawData ]
| ENUM SpecificationID | <>--(0..*)-[ Reference ]
+-----+
```

Figure 8: EventReport class

This class has the following attributes.

Version: OPTIONAL. STRING. The version number of the extension specification to which this class conforms. This value should be 1.00, to be compliant with this document. Its default value is 1.00.

SpecificationID: REQUIRED. ENUM. The ID of the specification and its version specifying the format of the RawData element. The value should be chosen from the IDs listed in Figure 1, such as CEE_0.6. Note that the lists in Figure 1 will be developed further by IANA.

This class is composed of three aggregate classes.

RawData: Zero or one. xml. A complete document that is formatted according to the specification and its version identified by the value of the SpecificationID with the Figure 1.

Reference: Zero or one of iodef:Reference [RFC5070]. This element allows an IODEF document to include a link to a structured information instead of directly embedding it into a RawData element.

This class MUST contain at least one of RawData or Reference elements. Writers/senders MUST ensure the specification name and version identified by the SpecificationID are consistent with the contents of the RawData; if a reader/receiver detects an inconsistency, it SHOULD prefer the specification name and version derived from the content, and SHOULD log the inconsistency so a human can correct the problem.

4.2.7. Verification

A Verification consists of an extension to the Incident.AdditionalData element with a dtype of "xml". The extension elements describes incident on vefifying incidents.

A Verification class is structured as follows.

```
+-----+
| Verification |
+-----+
| STRING Version | <>--(0..*)-[ RawData ]
| ENUM SpecificationID | <>--(0..*)-[ Reference ]
+-----+
```

Figure 9: Verification class

This class has the following attributes.

Version: OPTIONAL. STRING. The version number of the extension specification to which this class conforms. This value should be 1.00, to be compliant with this document. Its default value is 1.00.

SpecificationID: REQUIRED. ENUM. The ID of the specification and its version specifying the format of the RawData element. The value should be chosen from the IDs listed in Figure 1, such as OVAL_5.10, OCIL_2.0, and XCCDF_1.2. Note that the lists in Figure 1 will be developed further by IANA.

This class is composed of two aggregate classes.

RawData: Zero or one. xml. A complete document that is formatted according to the specification and its version identified by the value of the SpecificationID with the Figure 1.

Reference: Zero or one of iodef:Reference [RFC5070]. This element allows an IODEF document to include a link to a structured information instead of directly embedding it into a RawData element.

This class MUST contain at least either of RawData and Reference elements. Writers/senders MUST ensure the specification name and version identified by the SpecificationID are consistent with the contents of the RawData; if a reader/receiver detects an inconsistency, it SHOULD prefer the specification name and version derived from the content, and SHOULD log the inconsistency so a human can correct the problem.

4.2.8. Remediation

A Remediation consists of an extension to the Incident.AdditionalData element with a dtype of "xml". The extension elements describes incident remediation information including instructions.

It is recommended that Incident class SHOULD contain one or more of this extension elements whenever available.

A Remediation class is structured as follows.

```
+-----+
| Remediation |
+-----+
| STRING Version | <>--(0..*)-[ RawData ]
| ENUM SpecificationID | <>--(0..*)-[ Reference ]
+-----+
```

Figure 10: Remediation class

This class has the following attributes.

Version: OPTIONAL. STRING. The version number of the extension specification to which this class conforms. This value should be 1.00, to be compliant with this document. Its default value is 1.00.

SpecificationID: REQUIRED. ENUM. The ID of the specification and its version specifying the format of the RawData element. The value should be chosen from the IDs listed in Figure 1. Note that the lists in Figure 1 will be developed further by IANA.

This class is composed of two aggregate classes.

RawData: Zero or one. xml. A complete document that is formatted according to the specification and its version identified by the value of the SpecificationID with the Figure 1.

Reference: Zero or one of iodef:Reference [RFC5070]. This element allows an IODEF document to include a link to a structured information instead of directly embedding it into a RawData element.

This class MUST contain at least either of RawData and Reference elements. Writers/senders MUST ensure the specification name and version identified by the SpecificationID are consistent with the contents of the RawData; if a reader/receiver detects an inconsistency, it SHOULD prefer the specification name and version derived from the content, and SHOULD log the inconsistency so a human can correct the problem.

5. Examples

This section provides examples of an incident encoded in the IODEF. These examples do not necessarily represent the only way to encode a particular incident.

5.1. Reporting an attack

An example of a CSIRT reporting an attack.

```
<?xml version="1.0" encoding="UTF-8"?>
<IODEF-Document version="1.00" lang="en"
  xmlns="urn:ietf:params:xml:ns:iodef-1.0"
  xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0"
```

```
xmlns:iodef-sci="urn:ietf:params:xml:ns:iodef-sci-1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Incident purpose="reporting">
  <IncidentID name="csirt.example.com">189493</IncidentID>
  <ReportTime>2001-09-13T23:19:24+00:00</ReportTime>
  <Description>Incident report in company xx</Description>
  <!-- An administrative privilege was attempted, but failed -->
  <Assessment>
    <Impact completion="failed" type="admin"/>
  </Assessment>
  <Method>
    <Description>Structured information on attack pattern, exploited
      vulnerability, and weakness</Description>
  <AdditionalData dtype="xml">
    <iodef-sci:AttackPattern SpecificationID="CAPEC_1.6"
      AttackPatternID="CAPEC-14">
      <iodef-sci:RawData>[CAPEC-formatted data]</iodef-sci:RawData>
      <Reference>
        <ReferenceName>Link to Capec-14</ReferenceName>
        <URL>http://capec.mitre.org/data/definitions/14.html</URL>
      </Reference>
    </iodef-sci:AttackPattern>
    <iodef-sci:Vulnerability SpecificationID="CVE_1.0"
      VulnerabilityID="CVE-2010-3654">
      <iodef-sci:RawData>[CVE-formatted data]</iodef-sci:RawData>
      <iodef-sci:PlatformID SpecificationID="CPE_2.3">
        <iodef-sci:ID>[CPE ID]</iodef-sci:ID>
      </iodef-sci:PlatformID>
      <iodef-sci:Scoring SpecificationID="CVSS_2.0">
        <iodef-sci:Score>[CVSS scores]</iodef-sci:Score>
      </iodef-sci:Scoring>
    </iodef-sci:Vulnerability>
    <iodef-sci:Weakness SpecificationID="CWE_5.0"
      WeaknessID="CWE-119">
      <iodef-sci:RawData>[CWE-formatted data]</iodef-sci:RawData>
      <iodef-sci:Scoring SpecificationID="CWSS_0.8">
        <iodef-sci:Score>[CWSS scores]</iodef-sci:Score>
      </iodef-sci:Scoring>
    </iodef-sci:Weakness>
  </AdditionalData>
</Method>
<Contact role="creator" type="organization">
  <ContactName>Example.com CSIRT</ContactName>
  <RegistryHandle registry="arin">example-com</RegistryHandle>
  <Email>contact@csirt.example.com</Email>
</Contact>
<EventData>
  <Flow>
```

```

<System category="source">
  <Node>
    <Address category="ipv4-addr">192.0.2.200</Address>
    <Counter type="event">57</Counter>
  </Node>
</System>
<System category="target">
  <Node>
    <Address category="ipv4-net">192.0.2.16/28</Address>
  </Node>
  <Service ip_protocol="6">
    <Port>80</Port>
  </Service>
  <AdditionalData dtype="xml">
    <iodef-sci:PlatformID SpecificationID="CPE_2.3">
      <iodef-sci:ID>[CPE ID]</iodef-sci:ID>
    </iodef-sci:PlatformID>
  </AdditionalData>
</System>
</Flow>
<Expectation action="block-host" />
<Expectation action="other"/>
<!-- <RecordItem> has an excerpt from a log -->
<Record>
  <RecordData>
    <DateTime>2001-09-13T18:11:21+02:00</DateTime>
    <Description>a Web-server event record</Description>
    <RecordItem dtype="xml">
      <iodef-sci:EventReport SpecificationID="CEE_0.6">
        <iodef-sci:RawData>[CEE-formatted data]</iodef-sci:RawData>
      </iodef-sci:EventReport>
    </RecordItem>
  </RecordData>
</Record>
</EventData>
<History>
  <!-- Contact was previously made with the source network owner -->
  <HistoryItem action="contact-source-site">
    <DateTime>2001-09-14T08:19:01+00:00</DateTime>
    <Description>Notification sent to
      constituency-contact@192.0.2.200</Description>
  </HistoryItem>
</History>
<AdditionalData dtype="xml">
  <iodef-sci:Verification SpecificationID="OVAL_5.10">
    <iodef-sci:RawData>[OVAL-formatted data]</iodef-sci:RawData>
  </iodef-sci:Verification>
  <iodef-sci:Verification SpecificationID="XCCDF_1.2">

```



```
    <iodef-sci:RawData>[XCCDF-formatted data]</iodef-sci:RawData>
  </iodef-sci:Verification>
</AdditionalData>
</Incident>
</IODEF-Document>
```

Figure 11: Example UML Element Diagram

6. Security Considerations

This document specifies a format for encoding a particular class of security incidents appropriate for exchange across organizations. As merely a data representation, it does not directly introduce security issues. However, it is guaranteed that parties exchanging instances of this specification will have certain concerns. For this reason, the underlying message format and transport protocol used **MUST** ensure the appropriate degree of confidentiality, integrity, and authenticity for the specific environment.

Organizations that exchange data using this document are **URGED** to develop operating procedures that document the following areas of concern.

6.1. Transport-Specific Concerns

The underlying messaging format and protocol used to exchange instances of the IODEF **MUST** provide appropriate guarantees of confidentiality, integrity, and authenticity. The use of a standardized security protocol is encouraged. The Real-time Inter-network Defense (RID) protocol [RFC6045] and its associated transport binding [RFC6046] provide such security.

The critical security concerns are that these structured information may be falsified or they may become corrupt during transit. In areas where transmission security or secrecy is questionable, the application of a digital signature and/or message encryption on each report will counteract both of these concerns. We expect that each exchanging organization will determine the need, and mechanism, for transport protection.

6.2. Using the iodef:restriction Attribute

In some instances, data values in particular elements may contain data deemed sensitive by the reporter. Although there are no general-purpose rules on when to mark certain values as "private" or "need-to-know" via the iodef:restriction attribute, the reporter is cautioned not to apply element-level sensitivity markings unless they

believe the receiving party (i.e., the party they are exchanging the event report data with) has a mechanism to adequately safeguard and process the data as marked.

7. IANA Considerations

This document uses URNs to describe XML namespaces and XML schemata[XMLschemaPart1][XMLschemaPart2] conforming to a registry mechanism described in [RFC3688].

Registration request for the IODEF structured cybersecurity information extension namespace:

URI: urn:ietf:params:xml:ns:iodef-sci-1.0

Registrant Contact: Refer here to the authors' addresses section of the document.

XML: None

Registration request for the IODEF structured cybersecurity information extension XML schema:

URI: urn:ietf:params:xml:schema:iodef-sci-1.0

Registrant Contact: Refer here to the authors' addresses section of the document.

XML: Refer here to the XML Schema in the appendix of the document.

This memo creates the following registry for IANA to manage:

Name of the registry: "IODEF Structured Cyber Security Information Specifications"

Namespace details: A registry entry for a Structured Cyber Security Information Specification (SCI specification) consists of:

ID: A short XSD string that is used in the SpecificationID attribute of an IODEF extended class defined in this memo. The ID is usually based on the acronym and version number of the SCI specification.

Specification Name: A string containing the spelled-out name of the SCI specification in human-readable form.

Version: The version of the registered SCI specification. This is a string that SHOULD consist of numbers separated by '.' (period) characters, but additional characters and different formatting MAY be used when appropriate.

Namespace: A URI [RFC3986] that is the XML namespace name used by the registered SCI specification.

Specification URI: A URI [RFC3986] from which the registered specification can be obtained. The registered specification MUST be readily and publicly available from that URI.

Applicable Classes: A list of one or more of the Extended Classes specified in Section 4.2 of this document. The registered SCI specification MUST only be used with the Extended Classes in the registry entry.

Information that must be provided to assign a new value: The above list of information.

Assignment policy: If the requested value is not already assigned, it may be assigned to the requester.

Fields to record in the registry: ID/Specification Name/Version/ Namespace/Applicable Classes.

Initial registry contents: See sections from Section 4.1.1 through Section 4.1.16 above.

Allocation Policy: Expert Review [RFC5226] and Specification Required [RFC5226].

The Designated Expert is expected to consult with the mile (Managed Incident Lightweight Exchange) working group or its successor if any such WG exists (e.g., via email to the working group's mailing list). The Designated Expert is expected to retrieve the SCI specification from the provided URI in order to check the public availability of the specification and verify the correctness of the URI. An important responsibility of the Designated Expert is to ensure that the registered Applicable Classes are appropriate for the registered SCI specification.

8. Acknowledgment

We would like to acknowledge Mr. David Black from EMC, who kindly provided generous support, especially on the IANA registry issues. We also would like to thank Paul Cichonski from NIST, Robert Martin

from MITRE, Kathleen Moriarty from EMC, Lagadec Philippe from NATO, Shuhei Yamaguchi from NICT, Anthony Rutkowski from Yaana Technology, and Brian Trammel from CERT/NetSA for their sincere discussion and feedback on this document.

9. Appendix I: XML Schema Definition for Extension

The XML Schema describing the elements defined in the Extension Definition section is given here. Each of the examples in Section 5 should be verified to validate against this schema by automated tools.

```
<?xml version="1.0" encoding="UTF-8"?>

<xsd:schema targetNamespace="urn:ietf:params:xml:ns:iodef-sci-1.0"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0"
  xmlns:iodef-sci="urn:ietf:params:xml:ns:iodef-sci-1.0"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

<xsd:import
  namespace="urn:ietf:params:xml:ns:iodef-1.0"
  schemaLocation="iodef_schema.xsd"/>

<!--
  schemaLocation="urn:ietf:params:xml:schema:iodef-1.0"/>
-->

<!--=====
== Scoring Class ==
=====-->

<xsd:element name="Scoring">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="Score" type="xsd:anyType"/>
    </xsd:sequence>
    <xsd:attribute name="Version" type="xsd:string" use="optional"
      default="1.00"/>
    <xsd:attribute name="SpecificationID" type="xsd:string"
      use="required"/>
  </xsd:complexType>
</xsd:element>

<!--=====
== AttackPattern Class ==
=====-->
```

=====>

```
<xsd:element name="AttackPattern">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="RawData" type="xsd:anyType" minOccurs="0"
        maxOccurs="unbounded"/>
      <xsd:element name="Reference" ref="iodef:Reference"
        minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element name="PlatformID" ref="iodef-sci:PlatformID"
        minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="Version" type="xsd:string" use="optional"
      default="1.00"/>
    <xsd:attribute name="SpecificationID" type="xsd:string" use="required"
  />
  <xsd:attribute name="AttackPatternID" type="xsd:string" use="optional"
/>
</xsd:complexType>
</xsd:element>
```

<!--=====
== Vulnerability Class ==
=====>

```
<xsd:element name="Vulnerability">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="RawData" type="xsd:anyType" minOccurs="0"
        maxOccurs="unbounded"/>
      <xsd:element name="Reference" ref="iodef:Reference"
        minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element name="PlatformID" ref="iodef-sci:PlatformID"
        minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element name="Scoring" ref="iodef-sci:Scoring"
        minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="Version" type="xsd:string"
      use="optional" default="1.00"/>
    <xsd:attribute name="SpecificationID" type="xsd:string"
      use="required"/>
    <xsd:attribute name="VulnerabilityID" type="xsd:string"
      use="optional"/>
  </xsd:complexType>
</xsd:element>
```

<!--=====
== Weakness Class ==
=====>


```

<xsd:element name="Weakness">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="RawData" type="xsd:anyType" minOccurs="0"
        maxOccurs="unbounded"/>
      <xsd:element name="Reference" ref="iodef:Reference"
        minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element name="PlatformID" ref="iodef-sci:PlatformID"
        minOccurs="0" maxOccurs="unbounded"/>
      <xsd:element name="Scoring" ref="iodef-sci:Scoring"
        minOccurs="0" maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="Version" type="xsd:string" use="optional"
      default="1.00"/>
    <xsd:attribute name="SpecificationID" type="xsd:string"
      use="required"/>
    <xsd:attribute name="WeaknessID" type="xsd:string"
      use="optional"/>
  </xsd:complexType>
</xsd:element>

```

```

<!--=====
== PlatformID Class                                     ==
=====-->

```

```

<xsd:element name="PlatformID">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="ID" type="xsd:string" minOccurs="1"
        maxOccurs="unbounded"/>
    </xsd:sequence>
    <xsd:attribute name="Version" type="xsd:string" use="optional"
      default="1.00"/>
    <xsd:attribute name="SpecificationID" type="xsd:string"
      use="required"/>
  </xsd:complexType>
</xsd:element>

```

```

<!--=====
== EventReport Class                                   ==
=====-->

```

```

<xsd:element name="EventReport">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:choice>
        <xsd:element name="RawData" type="xsd:anyType"/>
        <xsd:element name="Reference" ref="iodef:Reference"/>
      </xsd:choice>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

```

```
        </xsd:choice>
    </xsd:sequence>
    <xsd:attribute name="Version" type="xsd:string"
        use="optional" default="1.00"/>
    <xsd:attribute name="SpecificationID" type="xsd:string"
        use="required"/>
</xsd:complexType>
</xsd:element>

<!--=====
== Verification Class                                     ==
=====-->

<xsd:element name="Verification">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:choice>
        <xsd:element name="RawData" type="xsd:anyType"/>
        <xsd:element name="Reference" ref="iodef:Reference"/>
      </xsd:choice>
    </xsd:sequence>
    <xsd:attribute name="Version" type="xsd:string"
        use="optional" default="1.00"/>
    <xsd:attribute name="SpecificationID" type="xsd:string"
        use="required"/>
  </xsd:complexType>
</xsd:element>

<!--=====
== Remediation Class                                     ==
=====-->

<xsd:element name="Remediation">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:choice>
        <xsd:element name="RawData" type="xsd:anyType"/>
        <xsd:element name="Reference" ref="iodef:Reference"/>
      </xsd:choice>
    </xsd:sequence>
    <xsd:attribute name="Version" type="xsd:string"
        use="optional" default="1.00"/>
    <xsd:attribute name="SpecificationID" type="xsd:string"
        use="required"/>
  </xsd:complexType>
</xsd:element>

</xsd:schema>
```


Example Schema Diagram

10. References

10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.
- [RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, December 2007.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.
- [RFC6045] Moriarty, K., "Real-time Inter-network Defense (RID)", RFC 6045, November 2010.
- [RFC6046] Moriarty, K. and B. Trammell, "Transport of Real-time Inter-network Defense (RID) Messages", RFC 6046, November 2010.
- [XML1.0] Bray, T., Maler, E., Paoli, J., Sperberg-McQueen, C., and F. Yergeau, "Extensible Markup Language (XML) 1.0 (Fifth Edition)", W3C Recommendation, November 2008.
- [XMLschemaPart1] Thompson, H., Beech, D., Maloney, M., and N. Mendelsohn, "XML Schema Part 1: Structures Second Edition", W3C Recommendation, October 2004.
- [XMLschemaPart2] Biron, P. and A. Malhotra, "XML Schema Part 2: Datatypes Second Edition", W3C Recommendation, October 2004.
- [XMLNames] Bray, T., Hollander, D., Layman, A., Tobin, R., and H. Thomson, "Namespaces in XML (Third Edition)", W3C Recommendation, December 2009.

10.2. Informative References

- [RFC3339] Klyne, G., Ed. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, July 2002.
- [RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.
- [RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.
- [RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.
- [RFC6116] Bradner, S., Conroy, L., and K. Fujiwara, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 6116, March 2011.
- [CVSS] Peter Mell, Karen Scarfone, and Sasha Romanosky, "The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems".
- [CAPEC] The MITRE Corporation, "Common Attack Pattern Enumeration and Classification (CAPEC)".
- [CEE] The MITRE Corporation, "Common Event Expression (CEE)".
- [CPE] Brant A. Cheikes and David Waltermire and Karen Scarfone, "Common Platform Enumeration: Naming Specificatio Version 2.3", August 2011.
- [CVE] The MITRE Corporation, "Common Vulnerability and Exposures (CVE)".
- [CVRF] ICASI, "Common Vulnerability Reporting Framework (CVRF)".
- [CWE] The MITRE Corporation, "Common Weakness Enumeration (CWE)".
- [CWSS] The MITRE Corporation, "Common Weakness Scoring System (CWSS)".
- [OCIL] David Waltermire and Karen Scarfone and Maria Casipe, "The Open Checklist Interactive Language (OCIL) Version 2.0", April 2011.

- [OVAL] The MITRE Corporation, "Open Vulnerability and Assessment Language (OVAL)".
- [XCCDF] David Waltermire and Charles Schmidt and Karen Scarfone and Neal Ziring, "Specification for the Extensible Configuration Checklist Description Format (XCCDF) version 1.2 (DRAFT)", July 2011.

Authors' Addresses

Takeshi Takahashi
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi Koganei
184-8795 Tokyo
Japan

Phone: +80 423 27 5862
Email: takeshi_takahashi@nict.go.jp

Kent Landfield
McAfee, Inc
5000 Headquarters Drive
Plano, TX 75024
USA

Email: Kent_Landfield@McAfee.com

Thomas Millar
US Department of Homeland Security, NPPD/CS&C/NCSD/US-CERT
245 Murray Lane SW, Building 410, MS #732
Washington, DC 20598
USA

Phone: +1 888 282 0870
Email: thomas.millar@us-cert.gov

Youki Kadobayashi
Nara Institute of Science and Technology
8916-5 Takayama, Ikoma
630-0192 Nara
Japan

Email: youki-k@is.aist-nara.ac.jp