IODEF-extension to support structured cybersecurity information
draft-takahashi-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™, CEE™, CPE®, CVE®, CVRF, CVSS, CWE™, CWSS™, ISO/IEC 19770-2,
OCIL, OVAL®, XCCDF, and XDAS.

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 April 7, 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
2. Terminology
3. Applicability
4. Extension Definition
   4.1. Structured Cybersecurity Information Formats
   4.2. Extended Data Types
      4.2.1. EM.XML
   4.3. Extended Classes
      4.3.1. AttackPattern
      4.3.2. PlatformID
      4.3.3. Vulnerability
      4.3.4. Scoring
      4.3.5. Weakness
      4.3.6. EventReport
      4.3.7. Remediation
5. Examples
6. Security Considerations
   6.1. Transport-Specific Concerns
6.2. Using the iodef:restriction Attribute
7. IANA Considerations
8. Acknowledgment
9. Appendix: XML Schema Definition for Extension
10. References
    10.1. Normative References
    10.2. Informative References
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, CEE, CPE, CVE, CVRF, CVSS, CWE, CWSS, ISO/IEC 19770-2, OCLL, OVAL, XCCDF, and XDAS. Since such structured description facilitates cybersecurity operations, it would be beneficial to embed and convey this 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 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 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, 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.

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 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. Structured Cybersecurity Information Formats

This extension intends to embed various structured cybersecurity information. The below table describes the initial list of supported specifications and their IDs, versions, and namespaces; future assignments are to be made through Expert Review, as requested in...
This extension inherits all of the data types defined in the IODEF model. One data type is added: EM_XML.

**4.2.1. EM_XML**

An embedded complete XML document is represented by the EM_XML data type. The elements of the document must match its root namespace element.

**4.3. Extended Classes**

The IODEF Incident element ([RFC5070], Section 3.2) 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.

```mermaid
diagram
+-------------------+
| Incident           |
+-------------------+
| ENUM purpose       |<--[0..1]--[IncidentID ] |
| STRING ext-purpose |<--[0..1]--[ AlternativeID ] |
| ENUM lang          |<--[0..1]--[ RelatedActivity ] |
| ENUM restriction   |<--[0..1]--[ DetectTime ] |
|                  |<--[0..1]--[ StartTime ] |
|                  |<--[0..1]--[ EndTime ] |
|                  |<--[0..*]--[ ReportTime ] |
|                  |<--[0..*]--[ Description ] |
|                  |<--[1..*]--[ Assessment ] |
|                  |<--[0..*]--[ Method ] |
|                  |<--[ AdditionalData ] |
|                  |<--[ AttackPattern ] |
|                  |<--[ Vulnerability ] |
|                  |<--[ Weakness ] |
|                  |<--[ Contact ] |
|                  |<--[0..*]--[ EventData ] |
```
This extension defines the following seven elements.

### 4.3.1. 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..*)--[ Record ]
| ENUM SpecificationID   |<--(0..*)--[ Reference ]
| STRING AttackPatternID |<--(0..*)--[ PlatformID ]
+------------------------+
```

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 Record 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 attack pattern to be reported. This attribute SHOULD be used whenever such ID is available, but could be omitted if no such ID is available. In case Record or Reference elements are provided, writers/senders MUST ensure that this ID is consistent with the one provided by the Record or Reference elements; if a reader/receiver detects an inconsistency, it SHOULD prefer the AttackPatternID, and SHOULD log the inconsistency so a human can correct the problem.

The AttackPattern class is composed of the following aggregate classes.

**Record:**
- Zero or more. EM_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 Record element.

**PlatformID:**
- Zero or more. An identifier of software platform involved in the specific attack pattern, which is elaborated in Section 4.3.2.

Writers/senders MUST ensure the specification name and version identified by the SpecificationID are consistent with the contents of the Record; 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.

### 4.3.2. PlatformID
A PlatformID identifies a software platform. It is recommended that AttackPattern, Vulnerability, Weakness, and System classes contain this element 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 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.

4.3.3. 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..*)--[ Record ]
| 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 Record 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, but could be omitted if no such ID is available. In case Record or Reference elements are provided, writers/senders MUST ensure that this ID is consistent with the one provided by the Record or Reference elements; if a reader/receiver detects an inconsistency, it SHOULD prefer the AttackPatternID, and SHOULD log the inconsistency so a human can correct the problem.
This class is composed of the following aggregate classes.

Record:
Zero or one. EM_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 Record element.

PlatformID:
Zero or more. An identifier of software platform affected by the vulnerability, which is elaborated in Section 4.3.2. Some of the structured information may include platform ids within it. In this case, the PlatformID element SHOULD NOT be used since the Record element contains the platform ids. If a reader/receiver detects platform ids in both Record and PlatformID elements and their inconsistency, it SHOULD prefer the platform ids derived from the Record 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 score, which is elaborated in Section 4.3.4. Some of the structured information may include scores within it. In this case, the Scoring element SHOULD NOT be used since the Record element contains the scores. If a reader/receiver detects scores in both Record and Scoring elements and their inconsistency, it SHOULD prefer the scores derived from the Record element, and SHOULD log the inconsistency so a human can correct the problem.

4.3.4. 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 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. EM_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.

4.3.5. 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.
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 Record 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 attack pattern to be reported. This element SHOULD be used whenever such ID is available, but could be omitted if no such ID is available. In case Record or Reference elements are provided, writers/senders MUST ensure that this ID is consistent with the one provided by the Record or Reference elements; if a reader/receiver detects an inconsistency, it SHOULD prefer the AttackPatternID, and SHOULD log the inconsistency so a human can correct the problem.

This class is composed of the following aggregate classes.

Record:
  Zero or more. EM.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 Record element.

PlatformID:
  Zero or more. An identifier of software platform affected by the weakness, which is elaborated in Section 4.3.2. Some of the structured information may include platform ids within it. In this case, the PlatformID element SHOULD NOT be used since the Record element contains the platform ids. If a reader/receiver detects platform ids in both Record and PlatformID elements and their inconsistency, it SHOULD prefer the platform ids derived from the Record 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 4.3.4. Some of the structured information may include scores within it. In this case, the Scoring element SHOULD NOT be used since the Record element contains the scores. If a reader/receiver detects scores in both Record and Scoring elements and their inconsistency, it SHOULD prefer the scores derived from the Record element, and SHOULD log the inconsistency so a human can correct the problem.

4.3.6. 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.

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 Record element. The value should be chosen from the IDs listed in Figure 1, such as CEE_0.6 and XDAS_1998. Note that the lists in Figure 1 will be developed further by IANA.

This class is composed of three aggregate classes.

Record:
Zero or one. EM_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 Record element.

This class MUST contain at least one of Record or Reference elements. Writers/senders MUST ensure the specification name and version identified by the SpecificationID are consistent with the contents of the Record; 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.

4.3.7. 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..*)--[ Record ]
| ENUM SpecificationID |<>--(0..*)--[ Reference ]
+----------------------+
```

Figure 9: Remediation class

This class has an attribute.

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 Record 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 three aggregate classes.

Record:
Zero or one. EM_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 Record element.

This class MUST contain at least one of Record or Reference elements. Writers/senders MUST ensure the specification name and version identified by the SpecificationID are consistent with the contents of the Record; 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. [Note: this section will be thoroughly checked later.]
5.1. Reporting an attack

An example of a CSIRT reporting an attack.

```xml
<?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="iodef-sci.xsd"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:ietf:params:xml:schema:iodef-1.0"
 <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>
    <AdditionalData>
      <iodef-sci:AttackPattern SpecificationID="CAPEC_1.6" AttackPatternID="CAPEC-14">
        <Record>[embed data in CAPEC format, if necessary]</Record>
      </iodef-sci:AttackPattern>
      <iodef-sci:Vulnerability SpecificationID="CVE_1.0" VulnerabilityID="CVE-2010-3654">
        <Record>[embed data in CVE format]</Record>
        <Scoring>[describe CVSS scores of the CVE entry]</Scoring>
        <PlatformID>[describe CPE ID relevant to the CVE entry]</PlatformID>
      </iodef-sci:Vulnerability>
      <iodef-sci:Weakness SpecificationID="CWE_5.0" WeaknessID="CWE-119">
        <Record>[embed data in CWE format]</Record>
        <Scoring>[describe CWSS scores of the CWE entry]</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</SpecificationID>
            <ID>[embed identifier in CPE format]</ID>
          </iodef-sci:PlatformID>
        </AdditionalData>
      </System>
    </Flow>
  </EventData>
</Incident>
```

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 conforming to a registry mechanism described in [RFC3688].

Registration request for the IODEF structured cybersecurity information extension namespace:

- URN: 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:

- URN: 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.
Request for managing a namespace list: the schemata of the embedded structured information are maintained outside of the IETF currently, but the list of the embedded specifications' IDs and namespaces need to be registered to IANA repository.

8. Acknowledgment

The following groups and individuals, listed alphabetically, contributed substantially to this document and should be recognized for their efforts.

Paul Cichonski, NIST
Black David, EMC
Robert Martin, MITRE
Kathleen Moriarty, EMC
Lagadec Philippe, NATO
Anthony Rutkowski, Yaana Technology
Brian Trammell, CERT/NetSA

9. Appendix: 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. [Note: this section will be thoroughly checked later.]

```xml
<?xml version="1.0"?>
<xs:schema
 xmlns:iodef-sci="iodef-sci.xsd"
 targetNamespace="iodef-sci.xsd"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema">
 <xs:import
 namespace="urn:ietf:params:xml:ns:iodef-1.0"
 schemaLocation="urn:ietf:params:xml:schema:iodef-1.0"/>
 <xs:element name="Scoring">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Score" type="xsd:string"/>
   </xs:sequence>
   <xs:attribute name="Version" type="xsd:string" use="required" default="1.00"/>
   <xs:attribute name="SpecificationID" type="xsd:string" use="required"/>
  </xs:complexType>
 </xs:element>
 <xs:element name="AttackPattern">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Record" type="xsd:string" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="Reference" type="iodef:Reference" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="PlatformID" type="iodef-sci:PlatformID" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:attribute name="Version" type="xsd:string" use="required" default="1.00"/>
   <xs:attribute name="SpecificationID" type="xsd:string" use="required"/>
   <xs:attribute name="AttackPatternID" type="xsd:string" use="optional"/>
  </xs:complexType>
 </xs:element>
 <xs:element name="Vulnerability">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Record" type="xsd:string" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="Reference" type="iodef:Reference" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="PlatformID" type="iodef-sci:PlatformID" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="Scoring" type="iodef-sci:Scoring" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:attribute name="Version" type="xsd:string" use="required" default="1.00"/>
   <xs:attribute name="SpecificationID" type="xsd:string" use="required"/>
   <xs:attribute name="VulnerabilityID" type="xsd:string" use="optional"/>
  </xs:complexType>
 </xs:element>
 <xs:element name="Weakness">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="Record" type="xsd:string" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="Reference" type="iodef:Reference" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
 </xs:element>
</xs:schema>
```
<xsd:element name="PlatformID" type="iodef-sci:PlatformID" minOccurs="0" maxOccurs="unbounded"/>
<xsd:element name="Scoring" type="iodef-sci:Scoring" minOccurs="0" maxOccurs="unbounded"/>
</xsd:sequence>
<xsd:attribute name="Version" type="xsd:string" use="required" 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>

<xsd:element name="EventReport">
<xsd:complexType>
<xsd:sequence>
<xsd:choice>
<xsd:element name="Record" type="xsd:string"/>
<xsd:element name="Reference" type="iodef:Reference"/>
</xsd:choice>
</xsd:sequence>
<xsd:attribute name="Version" type="xsd:string" use="required" default="1.00"/>
<xsd:attribute name="SpecificationID" type="xsd:string" use="required"/>
</xsd:complexType>
</xsd:element>

<xsd:element name="Remediation">
<xsd:complexType>
<xsd:sequence>
<xsd:choice>
<xsd:element name="Record" type="xsd:string"/>
<xsd:element name="Reference" type="iodef:Reference"/>
</xsd:choice>
</xsd:sequence>
<xsd:attribute name="Version" type="xsd:string" use="required" 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


10.2. Informative References


[CAPEC] The MITRE Corporation, "Common Attack Pattern Enumeration and Classification (CAPEC)."

[CPE] The MITRE Corporation, "Common Event Expression (CEE)."

[CVE] The MITRE Corporation, "Common Vulnerability and Exposures (CVE)."
