Abstract

This document extends the Resource-Oriented Lightweight Information Exchange (ROLIE) core to add the information type categories and related requirements needed to support Computer Security Incident Response Team (CSIRT) use cases. The indicator and incident information types are defined as ROLIE extensions. Additional supporting requirements are also defined that describe the use of specific formats and link relations pertaining to the new information types.

Status of This Memo

This Internet-Draft is submitted to IETF 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 https://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 September 6, 2018.

Copyright Notice

Copyright (c) 2018 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 (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
Table of Contents

1. Introduction .................................................. 3
2. Terminology ................................................... 4
3. Additional Requirements for the Atom Publishing Protocol ..... 4
   3.1. Use of HTTP requests ........................................... 4
   3.1.1. / (forward slash) Resource URL ............................ 4
4. Additional Requirements for the Atom Syndication Format .... 4
5. Information-type Extensions ..................................... 4
   5.1. The "incident" information type ............................... 4
   5.2. The "indicator" information type .............................. 5
   5.3. Use of the rolie:format element ............................... 5
   5.3.1. IODEF Format ............................................... 6
   5.3.2. STIX Format ............................................... 6
6. rolie:property Extensions ....................................... 6
7. Use of the atom:link element .................................... 6
   7.1. Link relations for the 'incident' information-type ......... 7
   7.2. Link relations for the 'indicator' information-type ..... 7
   7.3. Link relations for both information-types ..................... 8
8. Other Extensions ................................................ 8
   8.1. Use of atom:category .......................................... 8
   8.1.1. Newly registered category values .......................... 8
   8.1.2. Expectation and Impact Classes ........................... 9
9. IANA Considerations .............................................. 9
   9.1. information-type registrations .............................. 9
   9.1.1. incident information-type .................................. 9
   9.1.2. indicator information-type ................................ 9
   9.2. atom:category scheme registrations .......................... 10
   9.2.1. category:csirt:iodef:purpose ................................ 10
   9.2.2. category:csirt:iodef:restriction .......................... 10
   9.3. rolie:property name registrations .......................... 10
   9.3.1. property:csirt:id .......................................... 10
10. Security Considerations ......................................... 11
11. Normative References ........................................... 11
Appendix A. Non-Normative Examples ................................. 12
   A.1. Use of Link Relations ....................................... 12
   A.1.1. Use Case: Incident Sharing ................................ 13
   A.1.2. Use Case: Collaborative Investigation ..................... 15
   A.1.3. Use Case: Cyber Data Repository .......................... 17
Authors' Addresses ................................................. 20
1. Introduction

Threats to computer security are evolving ever more rapidly as time goes on. As software increases in complexity, the number of vulnerabilities in systems and networks can increase exponentially. Threat actors looking to exploit these vulnerabilities are making more frequent and more widely distributed attacks across a large variety of systems. The adoption of liberal information sharing amongst attackers allows a discovered vulnerability to be shared and used to attack a vulnerable system within a narrow window of time. As the skills and knowledge required to identify and combat these attacks become more and more specialized, even a well established and secure system may find itself unable to quickly respond to an incident. Effective identification of and response to a sophisticated attack requires open cooperation and collaboration between defending operators, software vendors, and end-users. To improve the timeliness of responses, automation must be used to acquire, contextualize, and put to use shared computer security information.

CSIRTS share two primary forms of information: incidents and indicators. Using these forms of information, analysts are able to perform a wide range of activities both proactive and reactive to ensure the security of their systems.

Incident information describes a cyber security incident. Such information may include attack characteristics, information about the attacker, and attack vector data. Sharing this information helps analysts within the sharing community to inoculate their systems against similar attacks, providing proactive protection.

Indicator information describes the symptoms or necessary pre-conditions of an attack. Everything from system vulnerabilities to unexpected network traffic can help analysts secure systems and prepare for an attack. Making this information available for sharing aids in the proactive defense of systems both within an operating unit but also for any CSIRTs that are part of a sharing consortium.

As a means to bring automation of content discovery and dissemination into the CSIRT domain, this specification provides an extension to the Resource-Oriented Lightweight Information Exchange (ROLIE) core [RFC8322] designed to address CSIRT use cases. The primary purpose of this extension is to define two new information types: incident, and indicator, along with formats and link relations that support these information-types.
2. Terminology

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].

Definitions for some of the common computer security-related terminology used in this document can be found in Section 2 of [RFC5070].

3. Additional Requirements for the Atom Publishing Protocol

This document specifies the following additional requirements for use of the Atom Publishing Protocol. [RFC5023]

3.1. Use of HTTP requests

This document defines the following requirements on HTTP request behavior:

3.1.1. / (forward slash) Resource URL

The forward slash resource URL SHOULD be supported as defined in Section 5.5 [RFC8322]. Note that this is a stricter requirement than [RFC8322].

4. Additional Requirements for the Atom Syndication Format

This document does not specify any additional requirements for the Atom Syndication Format. [RFC4287]

5. Information-type Extensions

5.1. The "incident" information type

The "incident" information type represents any information describing or pertaining to a computer security incident. This document uses the definition of incident provided by [RFC4949]. Provided below is a non-exhaustive list of information that may be considered to be an incident information type.

- Timing information: start and end times for the incident and/or the response.
- Descriptive information: plain text or machine readable data that provides some degree of description of the incident itself.
o Response information: the methods and results of a response to the incident.

o Meta and contact information: data about the CSIRT that recorded the information, or the operator that enacted the response.

o Effect and result information: data that describes the effects of an incident, or what the final results of the incident are.

Note again that this list is not exhaustive, any information that is in the abstract realm of an incident should be classified under this information-type.

5.2. The "indicator" information type

The "indicator" information type represents computer security indicators or any information surrounding them. This document uses the definition of indicator provided by [RFC4949]. Some examples of indicator information is provided below, but note that indicator is defined in an abstract sense, to be understood as a flexible and widely-applicable definition.

o Specific vulnerabilities that indicate a vector for attack.

o Signs of malicious reconnaissance.

o Definitions of patterns of other indicators.

o Events that may indicate an attack and information regarding those events.

o Meta information about the collecting agent.

This list is intended to provide examples of the indicator information-type, not to define it.

5.3. Use of the rolie:format element

This document does not contain any additional requirements for the rolie:format element; the formats that follow are provided as examples of formats that describe the incident and indicator information type. The formats are in no particular order, and are not requirements, nor suggestions by the authors.
5.3.1. IODEF Format

The Incident Object Description Exchange Format (IODEF) is a format for representing computer security information commonly exchanged between Computer Security Incident Response Teams (CSIRTs) or other operational security teams.

IODEF conveys indicators, incident reports, response activities, and related meta-data in an XML serialization. This information is formally structured in order to support and encourage automated machine-to-machine security communication, as well as enhanced processing at the endpoint.

The full IODEF specification provides further high-level discussion and technical details.

5.3.2. STIX Format

STIX is a structured language for describing a wide range of security resources. STIX approaches the problem with a focus on flexibility, automation, readability, and extensibility.

The use of STIX as the content of an Entry does not impose any additional requirements on ROLIE implementations.

6. rolie:property Extensions

This document provides new registrations for valid rolie:property names. These properties provide optional exposure point for valuable information in the linked content document. Exposing this information in a rolie:property element means that clients do not need to download the linked document to determine if it contains the information they are looking for.


Provides an XML element that can be populated with an identifier from the indicator or incident document linked to by an atom:content element. This value SHOULD be a uniquely identifying value for the document linked to in this entry’s atom:content element.

7. Use of the atom:link element

These sections define requirements for atom:link elements in Entries. Note that the requirements are determined by the information type that appears in either the Entry or in the parent Feed.
7.1. Link relations for the 'incident' information-type

If the category of an Entry is the incident information type, then the following requirements MUST be followed for inclusion of atom:link elements.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Conformance</th>
</tr>
</thead>
<tbody>
<tr>
<td>indicators</td>
<td>Provides a link to a collection of zero or more instances of cyber security indicators that are associated with the resource.</td>
<td>SHOULD</td>
</tr>
<tr>
<td>evidence</td>
<td>Provides a link to a collection of zero or more resources that provides some proof of attribution for an incident. The evidence may or may not have any identified chain of custody.</td>
<td>SHOULD</td>
</tr>
<tr>
<td>attacker</td>
<td>Provides a link to a collection of zero or more resources that provides a representation of the attacker.</td>
<td>SHOULD</td>
</tr>
<tr>
<td>vector</td>
<td>Provides a link to a collection of zero or more resources that provides a representation of the method used by the attacker.</td>
<td>SHOULD</td>
</tr>
</tbody>
</table>

Table 1: Link Relations for Resource-Oriented Lightweight Indicator Exchange

7.2. Link relations for the 'indicator' information-type

If the category of an Entry is the indicator information type, then the following requirements MUST be followed for inclusion of atom:link elements.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Conformance</th>
</tr>
</thead>
<tbody>
<tr>
<td>incidents</td>
<td>Provides a link to a collection of zero or more instances of incident representations associated with the resource.</td>
<td>SHOULD</td>
</tr>
</tbody>
</table>

Table 2: Link Relations for Resource-Oriented Lightweight Indicator Exchange
7.3. Link relations for both information-types

If the category of an Entry is either information-type, the following requirements MUST be followed for inclusion of atom:link elements.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Conformance</th>
</tr>
</thead>
<tbody>
<tr>
<td>assessments</td>
<td>Provides a link to a collection of zero or more resources that represent the results of executing a benchmark.</td>
<td>MAY</td>
</tr>
<tr>
<td>reports</td>
<td>Provides a link to a collection of zero or more resources that represent RID reports.</td>
<td>MAY</td>
</tr>
<tr>
<td>traceRequests</td>
<td>Provides a link to a collection of zero or more resources that represent RID traceRequests.</td>
<td>MAY</td>
</tr>
<tr>
<td>investigationRequests</td>
<td>Provides a link to a collection of zero or more resources that represent RID investigationRequests.</td>
<td>MAY</td>
</tr>
</tbody>
</table>

Table 3: Link Relations for Resource-Oriented Lightweight Indicator Exchange

8. Other Extensions

This document defines additional extensions as follows:

8.1. Use of atom:category

8.1.1. Newly registered category values


When the name attribute of the category is ‘urn:ietf:params:rolie:category:csirt:iodef:purpose’, the value attribute SHOULD be constrained as per section 3.2 of IODEF [RFC7970], e.g. traceback, mitigation, reporting, or other.
When the name attribute of the category is
'urn:ietf:params:rolie:category:csirt:iodef:restriction', the value
attribute SHOULD be constrained as per section 3.2 of IODEF
[RFC7970], e.g. public, need-to-know, private, default.

8.1.2. Expectation and Impact Classes

It is frequently the case that an organization will need to triage
their investigation and response activities based upon, e.g., the
state of the current threat environment, or simply as a result of
having limited resources.

In order to enable operators to effectively prioritize their response
activity, it is RECOMMENDED that feed implementers provide Atom
categories that correspond to the IODEF Expectation and Impact
classes. The availability of these feed categories will enable
clients to more easily retrieve and prioritize cyber security
information that has already been identified as having a specific
potential impact, or having a specific expectation.

Support for these categories may also enable efficiencies for
organizations that already have established (or plan to establish)
operational processes and workflows that are based on these IODEF
classes.

9. IANA Considerations

9.1. information-type registrations

IANA has added the following entries to the "ROLIE Security Resource
Information Type Sub-Registry" registry located at
<https://www.iana.org/assignments/rolie/category/information-type> .

9.1.1. incident information-type

The entry is as follows:

name: incident
index: TBD
reference: This document, Section 5.1

9.1.2. indicator information-type

The entry is as follows:

name: indicator
9.2. atom:category scheme registrations

IANA has added the following entries to the "ROLIE URN Parameters" registry located in <https://www.iana.org/assignments/rolie/>.

9.2.1. category:csirt:iodef:purpose

The entry is as follows:

name: category:csirt:iodef:purpose
Reference: This document, Section 8.1.1
Subregistry: None

9.2.2. category:csirt:iodef:restriction

The entry is as follows:

name: category:csirt:iodef:restriction
Reference: This document, Section 8.1.1
Subregistry: None

9.3. rolie:property name registrations

IANA has added the following entries to the "ROLIE URN Parameters" registry located in <https://www.iana.org/assignments/rolie/>.

9.3.1. property:csirt:id

The entry is as follows:

name: property:csirt:id
Reference: This document, section 6.3.1
10. Security Considerations

This document implies the use of ROLIE in high-security use cases, as such, added care should be taken to fortify and secure ROLIE repositories and clients using this extension. The guidance in the ROLIE core specification is strongly recommended, and implementers should consider adding additional security measures as they see fit.

When providing a private workspace for closed sharing, it is recommended that the ROLIE repository checks user authorization when the user sends a GET request to the service document. If the user is not authorized to send any requests to a given workspace or collection, that workspace or collection should be truncated from the service document in the response. In this way the existence of unauthorized content remains unknown to potential attackers, hopefully reducing attack surface.

11. Normative References


Appendix A. Non-Normative Examples

The following provide examples of some potential use cases of the CSIRT ROLIE extension, and provides a showcase for some of its benefits over traditional solutions.

The general non-normative examples provided in the core ROLIE document remain an excellent reference resource for typical ROLIE usage.

A.1. Use of Link Relations

A key benefit of using the RESTful architectural style is the ability to enable the client to navigate to related resources through the use of hypermedia links. In the Atom Syndication Format, the type of the related resource identified in a <link> element is indicated via the "rel" attribute, where the value of this attribute identifies the kind of related resource available at the corresponding "href" attribute. Thus, in lieu of a well-known URI template the URI itself is effectively opaque to the client, and therefore the client must understand the semantic meaning of the "rel" attribute in order to successfully navigate. Broad interoperability may be based upon a sharing consortium defining a well-known set of Atom Link Relation types. These Link Relation types may either be registered with IANA, or held in a private registry.

Individual CSIRTs may always define their own link relation types in order to support specific use cases, however support for a core set of well-known link relation types is encouraged as this will maximize interoperability.

In addition, it may be beneficial to define use case profiles that correspond to specific groupings of supported link relationship types. In this way, a CSIRT may unambiguously specify the classes of use cases for which a client can expect to find support.

The following sections provide non-normative examples of link relation usage. Three distinct cyber security information sharing use case scenarios are described. In each use case, the unique benefits of adopting a resource-oriented approach to information sharing are illustrated. It is important to note that these use cases are intended to be a small representative set and is by no means meant to be an exhaustive list. The intent is to illustrate
how the use of link relationship types will enable this resource-oriented approach to cyber security information sharing to successfully support the complete range of existing use cases, and also to motivate an initial list of well-defined link relationship types.

A.1.1. Use Case: Incident Sharing

This section provides a non-normative example of an incident sharing use case.

In this use case, a member CSIRT shares incident information with another member CSIRT in the same consortium. The client CSIRT retrieves a feed of incidents, and is able to identify one particular entry of interest. The client then does an HTTP GET on that entry, and the representation of that resource contains link relationships for both the associated "indicators" and the incident "history", and so on. The client CSIRT recognizes that some of the indicator and history may be relevant within her local environment, and can respond proactively.

Example HTTP GET response for an incident entry:
As can be seen in the example response, the Atom <link> elements enable the client to navigate to the related indicator resources, and/or the history entries associated with this incident.
A.1.2.  Use Case: Collaborative Investigation

This section provides a non-normative example of a collaborative investigation use case.

In this use case, two member CSIRTs that belong to a closed sharing consortium are collaborating on an incident investigation. The initiating CSIRT performs an HTTP GET to retrieve the service document of the peer CSIRT, and determines the collection name to be used for creating a new investigation request. The initiating CSIRT then POSTs a new incident entry to the appropriate collection URL. The target CSIRT acknowledges the request by responding with an HTTP status code 201 Created.

Example HTTP GET response for the service document:

HTTP/1.1 200 OK
Date: Fri, 24 Aug 2012 17:09:11 GMT
Content-Length: 934
Content-Type: application/atomsvc+xml;charset="utf-8"

<?xml version="1.0" encoding="UTF-8"?>
<service xmlns="http://www.w3.org/2007/app"
   xmlns:atom="http://www.w3.org/2005/Atom">
   <workspace xml:lang="en-US"
      <atom:title type="text">RID Use Case Requests</atom:title>
      <collection href="http://www.example.org/csirt/RID/InvestigationRequests">
         <atom:title type="text">Investigation Requests</atom:title>
         <accept>application/atom+xml; type=entry</accept>
      </collection>
      <collection href="http://www.example.org/csirt/RID/TraceRequests">
         <atom:title type="text">Trace Requests</atom:title>
         <accept>application/atom+xml; type=entry</accept>
      </collection>
   </workspace>
</service>

As can be seen in the example response, the Atom <collection> elements enable the client to determine the appropriate collection URL to request an investigation or a trace.

The client CSIRT then POSTs a new entry to the appropriate feed collection. Note that the <content> element of the new entry may contain a RID message of type "InvestigationRequest" if desired, however this would NOT be required. The entry content itself need
only be an IODEF document, with the choice of the target collection
resource URL indicating the callers intent. A CSIRT would be free to
use any URI template to accept investigationRequests.

POST /csirt/RID/InvestigationRequests HTTP/1.1
Host: www.example.org
Content-Type: application/atom+xml;type=entry
Content-Length: 852

<?xml version="1.0" encoding="UTF-8"?>
<entry xmlns="http://www.w3.org/2005/Atom"
 xmlns:rolie="urn:ietf:params:xml:ns:rolie-1.0">
 <title>New Investigation Request</title>
 <id>http://www.example2.org/csirt/private/incidents/123456</id>
 <!-- id and updated not guaranteed to be preserved -->
 <!-- may want to profile that behavior in this document -->
 <updated>2012-08-12T11:08:22Z</updated>
 <author><name>Name of peer CSIRT</name></author>
 <rolie:format ns="urn:example:iodef"/>
 <content type="application/xml">
 <iodef:IODEF-Document lang="en"
 xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
 <iodef:Incident purpose="traceback" restriction="need-to-know">
 <iodef:IncidentID name="http://www.example2.org/csirt/
 private/incidents">123</iodef:IncidentID>
 <!-- ...additional incident data... -->
 </iodef:Incident>
 </iodef:IODEF-Document>
 </content>
</entry>

The receiving CSIRT acknowledges the request with HTTP return code
201 Created.
HTTP/1.1 201 Created
Date: Fri, 24 Aug 2012 19:17:11 GMT
Content-Length: 906
Content-Type: application/atom+xml;type=entry
Location: http://www.example.org/csirt/RID/InvestigationRequests/823
ETag: "8a9h9he4qphqh"

<?xml version="1.0" encoding="UTF-8"?>
<entry xmlns="http://www.w3.org/2005/Atom"
xmlns:rolie="urn:ietf:params:xml:ns:rolie-1.0">
<title>New Investigation Request</title>
<id>http://www.example.org/csirt/RID/InvestigationRequests/823</id>
<!-- id and updated not guaranteed to be preserved -->
<!-- may want to profile that behavior in this document -->
<updated>2012-08-12T11:08:30Z</updated>
<published>2012-08-12T11:08:30Z</published>
<author><name>Name of peer CSIRT</name></author>
<rolie:format ns="urn:example:iodef"/>
<content type="application/xml">
<iodef:IODEF-Document lang="en"
xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
<iodef:Incident purpose="traceback" restriction="need-to-know">
<iodef:IncidentID name="http://www.example.org/csirt/private/incidents">123</iodef:IncidentID>
<!-- ...additional incident data.... -->
</iodef:Incident>
</iodef:IODEF-Document>
</content>
</entry>

Consistent with HTTP/1.1 RFC, the location header indicates the URL of the newly created InvestigationRequest. If for some reason the request were not authorized, the client would receive an HTTP status code 403 Unauthorized. In this case the HTTP response body may contain additional details, if an as appropriate.

A.1.3. Use Case: Cyber Data Repository

This section provides a non-normative example of a cyber security data repository use case.

In this use case a client accesses a persistent repository of cyber security data via a RESTful usage model. Retrieving a feed collection is analogous to an SQL SELECT statement producing a result set. Retrieving an individual Atom Entry is analogous to a SQL SELECT statement based upon a primary key producing a unique record. The cyber security data contained in the repository may include different data types, including indicators, incidents, benchmarks, or
any other related resources. In this use case, the repository is queried via HTTP GET, and the results that are returned to the client may optionally contain URL references to other cyber security resources that are known to be related. These related resources may also be persisted locally, or they may exist at another (remote) cyber data repository.

Example HTTP GET request to a persistent repository for any resources representing Distributed Denial of Service (DDOS) attacks:

GET /csirt/repository/ddos
Host: www.example.org
Accept: application/atom+xml

The corresponding HTTP response would be an XML document containing the DDOS feed.

Example HTTP GET response for a DDOS feed:

HTTP/1.1 200 OK
Date: Fri, 24 Aug 2012 17:20:11 GMT
Content-Length: nnnn
Content-Type: application/atom+xml;type=feed;charset="utf-8"

<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:rolie="urn:ietf:params:xml:ns:rolie-1.0"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://www.w3.org/2005/Atom
file:/C:/schemas/atom.xsd
urn:ietf:params:xml:ns:iodef-1.0
file:/C:/schemas/iodef-1.0.xsd"
xml:lang="en-US">
  <generator version="1.0" xml:lang="en-US">
    emc-csirt-iodef-feed-service</generator>
  <id>http://www.example.org/csirt/repository/ddos</id>
  <title type="text" xml:lang="en-US">
    Atom formatted representation of a feed of known ddos resources.
  </title>
  <author>
    <email>csirt@example.org</email>
    <name>EMC CSIRT</name>
  </author>

  <!-- By convention there is usually a self link for the feed -->
This feed document has two atom entries, one of which has been elided. The completed entry illustrates an Atom <entry> element that provides a summary of essential details about one particular DDOS incident. Based upon this summary information and the provided category information, a client may choose to do an HTTP GET operation to retrieve the full details of the DDOS incident. This example shows how a persistent repository may provide links to additional resources, both local and remote.

Note that the provider of a persistent repository is not obligated to follow any particular URL template scheme. The repository available
at the hypothetical provider "www.example.com" uses a different URL pattern than the hypothetical repository available at "www.cyber-agency.gov". When a client de-references a link to resource that is located in a remote repository the client may be challenged for authentication credentials acceptable to that provider. If the two repository providers choose to support a federated identity scheme or some other form of single-sign-on technology, then the user experience can be improved for interactive clients (e.g., a human user at a browser). However, this is not required and is an implementation choice that is out of scope for this specification.

Authors’ Addresses

Stephen A. Banghart
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland
USA

Phone: (301)975-4288
Email: sab3@nist.gov

John P. Field
Pivotal Software, Inc.
625 Avenue of the Americas
New York, New York
USA

Phone: (646)792-5770
Email: jfield@pivotal.io
Abstract

RFC7970 specified an information model and a corresponding XML data model for exchanging incident and indicator information. This draft provides an alternative data model implementation in JSON.
# 1. Introduction

[RFC7970] defines a data representation for security incident reports and indicators commonly exchanged by operational security teams. It facilitates the automated exchange of this information to enable mitigation and watch-and-warning. Section 3 of [RFC7970] defined an information model using Unified Modeling Language (UML) and a corresponding Extensible Markup Language (XML) schema data model in Section 8. This UML-based information model and XML-based data model are referred to as IODEF UML and IODEF XML, respectively in this document.

This document defines an alternate implementation of the IODEF UML information model by specifying a JavaScript Object Notation (JSON) data model using JSON Schema [jsonschema]. This JSON data model is referred to as IODEF JSON in this document.

IODEF JSON provides all of the expressivity of IODEF XML. It gives implementers and operators an alternative format to exchange the same information.
The normative IODEF JSON data model is found in Section 5. Section 2 and Section 3 describe the data types and elements of this data model. Section 4 provides examples.

1.1. Requirements Language

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].

2. IODEF Data Types

The abstract IODEF JSON implements the abstract data types specified in Section 2 of [RFC7970].

2.1. Abstract Data Type to JSON Data Type Mapping

IODEF JSON uses native and derived JSON data types. Figure 1 describes the mapping between the abstract data types in Section 2 of [RFC7970] and their corresponding implementations in IODEF JSON.
<table>
<thead>
<tr>
<th>IODEF Data Type</th>
<th>RFC7970 Reference</th>
<th>JSON Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTEGER</td>
<td>Section 2.1</td>
<td>&quot;integer&quot; per [jsonschema]</td>
</tr>
<tr>
<td>REAL</td>
<td>Section 2.2</td>
<td>&quot;number&quot; per [jsonschema]</td>
</tr>
<tr>
<td>CHARACTER</td>
<td>Section 2.3</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>STRING</td>
<td>Section 2.3</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>ML_STRING</td>
<td>Section 2.4</td>
<td>see Section 2.2.1</td>
</tr>
<tr>
<td>BYTE</td>
<td>Section 2.5.1</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>BYTE[]</td>
<td>Section 2.5.1</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>HEXBIN</td>
<td>Section 2.5.2</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>HEXBIN[]</td>
<td>Section 2.5.2</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>ENUM</td>
<td>Section 2.6</td>
<td>&quot;enum&quot; array per [jsonschema]</td>
</tr>
<tr>
<td>DATETIME</td>
<td>Section 2.7</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>TIMEZONE</td>
<td>Section 2.8</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>PORTLIST</td>
<td>Section 2.9</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>POSTAL</td>
<td>Section 2.10</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>POSTAL_ML</td>
<td>Section 2.10</td>
<td>see ML_STRING, Section 2.2.1</td>
</tr>
<tr>
<td>PHONE</td>
<td>Section 2.11</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>EMAIL</td>
<td>Section 2.12</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>URL</td>
<td>Section 2.13</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>IDREF</td>
<td>Section 2.14</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>SOFTWARE</td>
<td>Section 2.15</td>
<td>see Section 2.2.2</td>
</tr>
<tr>
<td>STRUCTURED</td>
<td>N/A</td>
<td>see Section 2.2.3</td>
</tr>
</tbody>
</table>

Figure 1

### 2.2. Complex JSON Types

#### 2.2.1. Multilingual Strings

A string that needs to be represented in a human-readable language different than the default encoding of the document is represented in the information model by the ML_STRING data type. This data type is implemented as an object with "value", "lang", and "translation-id" elements as defined in Section 5. Examples are shown below.

```
"MLStringType": {
    "value": "free-form text", //STRING
    "lang": "en",             //ENUM
    "translation-id": "jp2en0023" //STRING
}
```
2.2.2. Software

A particular version of software is represented in the information model by the SOFTWARE data type. This software can be described by using a reference, a URL, or with free-form text. The SOFTWARE data type is implemented as an object with "SoftwareReference", "URL", "Description", and "Description_ML" elements as defined in Section 5. Examples are shown below.

"SoftwareType": {
  "SoftwareReference": {...},          //SoftwareReference
  "Description": ["MS Windows"]        //STRING
}

2.2.3. StructuredInfo

Information provided in a form of structured string, such as ID, or structured information, such as XML documents, is represented in the information model by the StructuredInfo data type. Note that this type was originally specified in RFC7203. The StructuredInfo data type is implemented as an object with "SpecID", "ext-SpecID", "ContentID", "RawData", "Reference" elements. An example for embedding a structured ID is shown below.

"StructuredInformation": {
  "SpecID": "cve",                                          //ENUM
  "ContentID": "CVE-2007-5000"                            //STRING
}

When embedding the raw data, base64 conversion should be used for encoding the data, as shown below.

"StructuredInformation": {
  "SpecID": "oval",                                         //ENUM
  "RawData": "<<<strings encoded with base64>>>"            //BYTE
}

3. IODEF JSON Data Model

3.1. Classes and Elements

The following table shows the list of IODEF Classes, their elements, and the corresponding section in [RFC7970]. Note that the complete JSON schema is defined in Section 5.

<table>
<thead>
<tr>
<th>IODEF Class</th>
<th>Class</th>
<th>Corresponding Elements and Section</th>
</tr>
</thead>
</table>

Takahashi, et al. Expires September 19, 2018
<table>
<thead>
<tr>
<th>Attribute</th>
<th>in [RFC7970]</th>
</tr>
</thead>
<tbody>
<tr>
<td>IODEF-Document</td>
<td>version</td>
</tr>
<tr>
<td></td>
<td>lang?</td>
</tr>
<tr>
<td></td>
<td>format-id?</td>
</tr>
<tr>
<td></td>
<td>private-enum-name?</td>
</tr>
<tr>
<td></td>
<td>private-enum-id?</td>
</tr>
<tr>
<td></td>
<td>Incident+</td>
</tr>
<tr>
<td></td>
<td>AdditionalData*</td>
</tr>
<tr>
<td>Incident</td>
<td>purpose</td>
</tr>
<tr>
<td></td>
<td>ext-purpose?</td>
</tr>
<tr>
<td></td>
<td>status?</td>
</tr>
<tr>
<td></td>
<td>ext-status?</td>
</tr>
<tr>
<td></td>
<td>lang?</td>
</tr>
<tr>
<td></td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
</tr>
<tr>
<td></td>
<td>observable-id?</td>
</tr>
<tr>
<td></td>
<td>IncidentID</td>
</tr>
<tr>
<td></td>
<td>AlternativeID?</td>
</tr>
<tr>
<td></td>
<td>RelatedActivity*</td>
</tr>
<tr>
<td></td>
<td>DetectTime?</td>
</tr>
<tr>
<td></td>
<td>StartTime?</td>
</tr>
<tr>
<td></td>
<td>EndTime?</td>
</tr>
<tr>
<td></td>
<td>RecoveryTime?</td>
</tr>
<tr>
<td></td>
<td>ReportTime?</td>
</tr>
<tr>
<td></td>
<td>GenerationTime?</td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td>Discovery*</td>
</tr>
<tr>
<td></td>
<td>Assessment*</td>
</tr>
<tr>
<td></td>
<td>Method*</td>
</tr>
<tr>
<td></td>
<td>Contact+</td>
</tr>
<tr>
<td></td>
<td>EventData*</td>
</tr>
<tr>
<td></td>
<td>Indicator*</td>
</tr>
<tr>
<td></td>
<td>History?</td>
</tr>
<tr>
<td></td>
<td>AdditionalData*</td>
</tr>
<tr>
<td>IncidentID</td>
<td>id</td>
</tr>
<tr>
<td></td>
<td>name</td>
</tr>
<tr>
<td></td>
<td>instance?</td>
</tr>
<tr>
<td></td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
</tr>
<tr>
<td>AlternativeID</td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
</tr>
<tr>
<td></td>
<td>IncidentID+</td>
</tr>
<tr>
<td>RelatedActivity</td>
<td>restriction?</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
</tr>
<tr>
<td></td>
<td>IncidentID*</td>
</tr>
<tr>
<td></td>
<td>URL*</td>
</tr>
<tr>
<td></td>
<td>ThreatActor*</td>
</tr>
<tr>
<td></td>
<td>Campaign*</td>
</tr>
<tr>
<td></td>
<td>IndicatorID*</td>
</tr>
<tr>
<td></td>
<td>Confidence?</td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>AdditionalData*</td>
</tr>
<tr>
<td>ThreatActor</td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
</tr>
<tr>
<td></td>
<td>ThreatActorID*</td>
</tr>
<tr>
<td></td>
<td>URL*</td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td>AdditionalData*</td>
</tr>
<tr>
<td>Campaign</td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
</tr>
<tr>
<td></td>
<td>CampaignID*</td>
</tr>
<tr>
<td></td>
<td>URL*</td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td>AdditionalData*</td>
</tr>
<tr>
<td>Contact</td>
<td>role</td>
</tr>
<tr>
<td></td>
<td>ext-role?</td>
</tr>
<tr>
<td></td>
<td>type</td>
</tr>
<tr>
<td></td>
<td>ext-type?</td>
</tr>
<tr>
<td></td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
</tr>
<tr>
<td></td>
<td>ContactName*,ContactName_ML*</td>
</tr>
<tr>
<td></td>
<td>ContactTitle*</td>
</tr>
<tr>
<td></td>
<td>ContactTitle_ML*</td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td>RegistryHandle*</td>
</tr>
<tr>
<td></td>
<td>PostalAddress*</td>
</tr>
<tr>
<td></td>
<td>Email*</td>
</tr>
<tr>
<td></td>
<td>Telephone*</td>
</tr>
<tr>
<td></td>
<td>Timezone?</td>
</tr>
<tr>
<td></td>
<td>Contact*</td>
</tr>
<tr>
<td></td>
<td>AdditionalData*</td>
</tr>
<tr>
<td>RegistryHandle</td>
<td>handle</td>
</tr>
<tr>
<td></td>
<td>registry</td>
</tr>
<tr>
<td></td>
<td>ext-registry?</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>PostalAddress</td>
<td>type?</td>
</tr>
<tr>
<td></td>
<td>ext-type?</td>
</tr>
<tr>
<td>PAddress</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>type?</td>
</tr>
<tr>
<td></td>
<td>ext-type?</td>
</tr>
<tr>
<td>EmailTo</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>type?</td>
</tr>
<tr>
<td></td>
<td>ext-type?</td>
</tr>
<tr>
<td>TelephoneNumber</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>source?</td>
</tr>
<tr>
<td></td>
<td>ext-source?</td>
</tr>
<tr>
<td></td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td>Contact*</td>
</tr>
<tr>
<td></td>
<td>DetectionPattern*</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>DetectionPattern</td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
</tr>
<tr>
<td></td>
<td>observable-id?</td>
</tr>
<tr>
<td></td>
<td>Application</td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td>DetectionConfiguration*</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Method</td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
</tr>
<tr>
<td></td>
<td>Reference*</td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td>AttackPattern*</td>
</tr>
<tr>
<td></td>
<td>Vulnerability*</td>
</tr>
<tr>
<td></td>
<td>Weakness*</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Reference</td>
<td>observable-id?</td>
</tr>
<tr>
<td></td>
<td>ReferenceName?</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>SystemImpact</td>
<td>severity?</td>
</tr>
<tr>
<td>BusinessImpact</td>
<td>severity?</td>
</tr>
<tr>
<td>MonetaryImpact</td>
<td>value</td>
</tr>
<tr>
<td>Confidence</td>
<td>value</td>
</tr>
<tr>
<td></td>
<td>rating</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>History</td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>HistoryItem+</td>
</tr>
<tr>
<td>HistoryItem</td>
<td>action</td>
</tr>
<tr>
<td></td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>observable-id?</td>
</tr>
<tr>
<td></td>
<td>IncidentID?</td>
</tr>
<tr>
<td></td>
<td>Description*</td>
</tr>
<tr>
<td></td>
<td>DefinedCOA*</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>EventData</td>
<td>restriction?</td>
</tr>
<tr>
<td></td>
<td>observable-id?</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Expectation</td>
<td>action?</td>
</tr>
<tr>
<td></td>
<td>severity?</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EndTime?</td>
<td>Contact?</td>
</tr>
<tr>
<td></td>
<td>3.15</td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>category?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ext-category?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>spoofed?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>virtual?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ownership?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ext-ownership?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>restriction?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Node</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NodeRole*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OperatingSystem*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Counter*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AssetID*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AdditionalData*</td>
<td>3.16</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node</td>
<td>DomainData*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Address*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PostalAddress?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Location*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Location_ML*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Counter*</td>
<td>3.17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td>value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ext-category?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-name?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-num?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>observable-id?</td>
<td>3.17.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NodeRole</td>
<td>category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ext-category?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
<td>3.17.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Counter</td>
<td>value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ext-type?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>unit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ext-unit?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>meaning?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>meaning_ML?</td>
<td></td>
</tr>
</tbody>
</table>

Internet-Draft                 JSON-IODEF                     March 2018

<table>
<thead>
<tr>
<th>duration?</th>
<th>ext-duration?</th>
<th>3.17.3</th>
</tr>
</thead>
</table>
+-----------------------------+----------------|--------|
| DomainData                  | system-status |        |
| ext-system-status?          |               |        |
| domain-status               |               |        |
| ext-domain-status?          |               |        |
| observable-id?              | Name          |        |
| DateDomainWasChecked?       | RegistrationDate? |  |
| ExpirationDate             | RelatedDNS*   |        |
| Nameservers*                | DomainContacts? | 3.18  |
|                            | 3.18          |        |
+-----------------------------+----------------|--------|
| Nameserver                  | Server        |        |
| Address*                   | 3.18.1        |        |
+-----------------------------+----------------|--------|
| DomainContacts              | SameDomainContact? | 3.18.2 |
|                            | Contact+      |        |
+-----------------------------+----------------|--------|
| Service                     | ip-protocol?  |        |
| observable-id?              | ServiceName?  |        |
| Port?                      | Port?         |        |
| Portlist?                  | ProtoCode?    |        |
| ProtoType?                 | ProtoField?   |        |
| ApplicationHeaderField+    | EmailData?    |        |
| Application?               | 3.19          |        |
+-----------------------------+----------------|--------|
| ServiceName                 | IANAService?  |        |
| URL*                       | Description*  |        |
|                           | Description_ML* | 3.19.1 |
+-----------------------------+----------------|--------|
| EmailData                   | observable-id?|        |
| EmailTo*                    | EmailFrom?    |        |
| EmailSubject?              | EmailX-Mailer?|       |
| EmailX-Mailer?             | EmailHeaderField* |   |
| EmailHeaders?               | EmailHeaders? |        |
| EmailBody?                  | EmailBody?    |        |
| EmailMessage?              |               |        |

<table>
<thead>
<tr>
<th></th>
<th>HashData*</th>
<th>Signature*</th>
<th>3.19.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>RecordData</td>
<td>restriction?</td>
<td>ext-restriction?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>observable-id?</td>
<td>DateTime?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
<td>Description_ML*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application?</td>
<td>RecordPattern*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RecordItem*</td>
<td>URL*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FileData*</td>
<td>WindowsRegistryKeysModified*</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CertificateData*</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AdditionalData*</td>
<td>3.19.3</td>
</tr>
</tbody>
</table>

|              | type               | ext-type?                          |        |
|              | offset?            | offsetunit?                        |        |
|              | ext-offsetunit?    | ext-restriction?                   |        |
|              | instance?          | value                              |        |
| 3.19.4       |                    |                                    |        |

| WindowsRegistryKeysModified | observable-id? | 3.20 |
|                            | Key+           |      |

| Key                       | registryaction?| ext-registryaction?                |        |
|                          | observable-id? | KeyName                            |        |
|                          | KeyName        | KeyValue?                          |        |
|                          |                |                                    |        |

| CertificateData          | restriction?   | ext-restriction?                   |        |
|                          | observable-id? | Certificate+                       | 3.21   |
|                          |                |                                    |        |

| Certificate              | observable-id? | X509Data                           |        |
|                          | Description*   | Description_ML*                    | 3.21.1 |

<p>| FileData                 | restriction?   | ext-restriction?                   |        |
|                         | observable-id? |                                    |        |</p>
<table>
<thead>
<tr>
<th></th>
<th>observable-id?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>FileName?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FileSize?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FileType?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HashData?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Signature*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AssociatedSoftware?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FileProperties*</td>
<td>3.22.1</td>
</tr>
<tr>
<td></td>
<td>scope</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HashTargetID?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hash*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FuzzyHash*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DigestMethod</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DigestValue</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CanonicalizationMethod?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application?</td>
<td>3.23.1</td>
</tr>
<tr>
<td></td>
<td>FuzzyHashValue+</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AdditionalData?</td>
<td>3.23.2</td>
</tr>
<tr>
<td></td>
<td>id</td>
<td></td>
</tr>
<tr>
<td></td>
<td>name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>version</td>
<td>3.24.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AlternativeIndicatorID</th>
<th>restriction?</th>
<th>ext-restriction?</th>
<th>IndicatorReference+</th>
<th>3.24.2</th>
</tr>
</thead>
</table>

|------------------------|--------------|------------------|---------|----------|-------------|---------|------------|-----------------------------|---------|-----------------|-----------------|------------|------------|----------|--------------|------------|----------------|----------------|---------|----------------|------------------|--------|

<table>
<thead>
<tr>
<th>BulkObservable</th>
<th>type?</th>
<th>ext-type?</th>
<th>BulkObservableFormat?</th>
<th>BulkObservableList</th>
<th>AdditionalData*</th>
<th>3.24.4</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>BulkObservableFormat</th>
<th>Hash?</th>
<th>AdditionalData*</th>
<th>3.24.5</th>
</tr>
</thead>
</table>

|-----------------------|--------------|------------------|----------------------|------------|---------|-------------------|-------------|----------------|--------|

|-----------------------|--------------|------------------|----------------------|------------|
3.2. Mapping between JSON and XML IODEF

- This document treats attributes and elements of each class defined in [RFC7970] equally and is agnostic on the order of their appearances.

- Flow class is deleted, and classes with its instances now directly have instances of EventData class that used to belong to the Flow class.

- ApplicationHeader class is deleted, and classes with its instances now directly have instances of ApplicationHeaderField class that used to belong to the ApplicationHeader class.

- SignatureData class is deleted, and classes with its instances now directly have the instances of Signature class that used to belong to the SignatureData class.

- IndicatorData class is deleted, and classes with its instances now directly have the instances of Indicator class that used to belong to the IndicatorData class.

- ObservableReference class is deleted, and classes with its instances now directly have uid-ref as an element.

- Record class is deleted, and classes with its instances now directly have the instances of RecordData class that used to belong to the Record class.

- The elements of ML_STRING type are prepared as two separate elements: one of STRING type and another of ML_STRING type, in order to maintain the simplicity of IODEF documents when writing with only STRING type characters.

4. Examples

This section provides example of IODEF documents. These examples do not represent the full capabilities of the data model or the the only way to encode particular information.
4.1. Minimal Example

A document containing only the mandatory elements and attributes.

```
{
  "version": "2.0",
  "lang": "en",
  "Incident": [
    {
      "purpose": "reporting",
      "restriction": "private",
      "IncidentID": {
        "id": 492382,
        "name": "csirt.example.com"
      },
      "GenerationTime": "2015-07-18T09:00:00-05:00",
      "Contact": [
        {
          "type": "organization",
          "role": "creator",
          "email": {
            "emailTo": "contact@csirt.example.com"
          }
        }
      ]
    }
  ]
}
```

4.2. Indicators from a Campaign

An example of C2 domains from a given campaign.

```
{
  "version": "2.0",
  "lang": "en",
  "Incidents": [
    {
      "purpose": "watch",
      "restriction": "green",
      "IncidentID": {
        "id": "897923",
        "name": "csirt.example.com"
      },
      "RelatedActivity": [
        {
          "ThreatActor": [
            {
              "hostname": "example.com"
            }
          ]
        }
      ]
    }
  ]
}
```
"ThreatActorID": "TA-12-AGGRESSIVE-BUTTERFLY",
"Description": "Aggressive Butterfly"
],
"Campaign": [
{
"CampaignID": "C-2015-59405",
"Description": "Orange Giraffe"
}
],
"GenerationTime": "2015-10-02T11:18:00-05:00",
"Description": "Summarizes the Indicators of Compromise for the Orange Giraffe campaign of the Aggressive Butterfly crime gang."
],
"Assessment": [
{
"BusinessImpact": {
"type": "breach-proprietary"
}
}
],
"Contacts": [
{
"type": "organization",
"role": "creator",
"ContactName": "CSIRT for example.com",
"Email": {
"emailTo": "contact@csirt.example.com"
}
}
],
"IndicatorList": [
{
"IndicatorID": {
"id": "G90823490",
"name": "csirt.example.com",
"version": "1"
},
"Description": "C2 domains",
"StartTime": "2014-12-02T11:18:00-05:00",
"Observable": {
"BulkObservable": {
"type": "fqdn"
},
"BulkObservableList": [
"kj290023j09r34.example.com",
""}
5. The IODEF Data Model (JSON Schema)

{ "$schema": "http://json-schema.org/draft-04/schema#",
 "definitions": {
 "action": {"enum": ["nothing","contact-source-site","contact-target-site",
 "contact-sender","investigate","block-host","block-network",
 "block-port","rate-limit-host","rate-limit-network",
 "rate-limit-port","redirect-traffic","honeypot",
 "upgrade-software","rebuild-asset","harden-asset",
 "remediate-other","status-triage","status-new-info",
 "watch-and-report","training","defined-coa","ext-value"]},
 "duration": {"enum": ["second","minute","hour","day","month","quarter",
 "year","ext-value"]},
 "lang": {"enum": ["en","jp"]},
 "purpose": {"enum": ["traceback","mitigation","reporting","watch","other",
 "ext-value"]},
 "restriction": {"enum": ["public","partner","need-to-know","private",
 "default","white","green","amber","red","ext-value"]},
 "status": {"enum": ["new","in-progress","forwarded","resolved","future",
 "ext-value"]},
 "DATETIME": {"type": "string"},
 "PORTLIST": {"type": "string"},
 "URLtype": {"type": "string"},
 "IDtype": {"type": "string"},
 "ExtensionType": {
 "type": "object",
 "properties": {
 "name": {"type": "string"},
 "dtype": {"enum": ["boolean","byte","bytes","character","date-time",
 "ntpstamp","integer","portlist","real","string","file",
 "path","frame","packet","ipv4-packet","ipv6-packet","url",
 "csv","winreg","xml","ext-value"]},
 "ext-dtype": {"type": "string"},
 "meaning": {"type": "string"},
 "formatid": {"type": "string"},
 "restriction": {"$ref": "#/definitions/restriction"},
 "ext-restriction": {"type": "string"}
}
"observable-id": {"$ref": "/definitions/IDtype"},

"ExtensionTypeList": {
  "type": "array",
  "items": {"$ref": "/definitions/ExtensionType"},

"SoftwareType": {
  "type": "object",
  "properties": {
    "SoftwareReference": {"$ref": "/definitions/SoftwareReference"},
    "URL": {"$ref": "/definitions/URLtype"},
    "Description": {"type": "array", "items": {"type": "string"}}
  }
}

"SoftwareReference": {
  "type": "object",
  "properties": {
    "value": {"type": "string"},
    "spec-name": {"type": "string"},
    "ext-spec-name": {"type": "string"},
    "dtype": {"type": "string"},
    "ext-dtype": {"type": "string"}
  }
}

"StructuredInfo": {
  "type": "object",
  "properties": {
    "specID": {"type": "string"},
    "ext-specID": {"type": "string"},
    "contentID": {"type": "string"},
    "RawData": {"type": "string"},
    "URL": {"$ref": "/definitions/URLtype"}
  }
}

"Incident": {
  "title": "Incident",
  "description": "JSON schema for Incident class",
  "type": "object",
  "properties": {
    "purpose": {"$ref": "/definitions/purpose"},
    "ext-purpose": {"type": "string"},
    "status": {"$ref": "/definitions/status"},
    "ext-status": {"type": "string"},
    "lang": {"$ref": "/definitions/lang"},
    "restriction": {"$ref": "/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "observable-id": {"$ref": "/definitions/IDtype"},
    "IncidentID": {"$ref": "/definitions/IncidentID"},
    "AlternativeID": {"$ref": "/definitions/AlternativeID"},
    "RelatedActivity": {
      "type": "array",
      "items": {
        "$ref": "/definitions/RelatedActivity"}  
    }
  }
}
"type": "array","items": {"$ref": "/definitions/RelatedActivity"},
"DetectTime": {"type": "string"},
"StartTime": {"type": "string"},
"EndTime": {"type": "string"},
"RecoveryTime": {"type": "string"},
"ReportTime": {"type": "string"},
"GenerationTime": {"type": "string"},
"Description": {"type": "array","items": {"type": "string"}},
"Discovery": {
  "type": "array","items": {"$ref": "/definitions/Discovery"}},
"Assessment": {
  "type": "array","items": {"$ref": "/definitions/Assessment"}},
"Methods": {
  "type": "array","items": {"$ref": "/definitions/Method"}},
"Contacts": {
  "type": "array","items": {"$ref": "/definitions/Contact"}},
"EventData": {
  "type": "array","items": {"$ref": "/definitions/EventData"}},
"IndicatorList": {
  "type": "array","items": {"$ref": "/definitions/Indicator"}},
"History": {"$ref": "/#/definitions/History"},
"AdditionalData": {"$ref": "/#/definitions/ExtensionTypeList"},
"required": ["IncidentID","GenerationTime","Contacts","purpose"],
"additionalProperties": false},
"IncidentID": {
  "title": "IncidentID",
  "description": "JSON schema for IncidentID class",
  "type": "object",
  "properties": {
    "id": {"type": "string"},
    "name": {"type": "string"},
    "instance": {"type": "string"},
    "restriction": {"$ref": "/#/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "required": ["name"],
    "additionalProperties": false},
"AlternativeID": {
  "title": "AlternativeID",
  "description": "JSON schema for AlternativeID class",
  "type": "object",
  "properties": {
    "IncidentID": {
      "type": "array","items": {"$ref": "/#/definitions/IncidentID"},
    "restriction": {"$ref": "/#/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "required": ["IncidentID"],
    "additionalProperties": false},
"RelatedActivity": {

"properties": {
"restriction": {"$ref": "/#definitions/restriction"},
"ext-restriction": {"type": "string"},
"IncidentID": {
"type": "array","items": {"$ref": "/#definitions/IncidentID"}},
"URL": {
"type": "array","items": {"$ref": "/#definitions/URLType"}},
"ThreatActor": {
"type": "array","items": {"$ref": "/#definitions/ThreatActor"}},
"Campaign": {
"type": "array","items": {"$ref": "/#definitions/Campaign"}},
"IndicatorID": {
"type": "array","items": {"$ref": "/#definitions/IndicatorID"}},
"Confidence": {"$ref": "/#definitions/Confidence"},
"Description": {
"type": "array","items": {"type": "string"}},
"AdditionalData": {"$ref": "/#definitions/ExtensionTypeList"},
"additionalProperties": false},
"ThreatActor": {
"properties": {
"restriction": {"$ref": "/#definitions/restriction"},
"ext-restriction": {"type": "string"},
"ThreatActorID": {"type": "array","items": {"type": "string"}},
"Description": {"type": "array","items": {"type": "string"}},
"URL": {"type": "array","items": {"$ref": "/#definitions/URLType"}},
"AdditionalData": {"$ref": "/#definitions/ExtensionTypeList"},
"additionalProperties": false},
"Campaign": {
"properties": {
"restriction": {"$ref": "/#definitions/restriction"},
"ext-restriction": {"type": "string"},
"CampaignID": {"type": "array","items": {"type": "string"}},
"URL": {"type": "array","items": {"$ref": "/#definitions/URLType"}},
"Description": {"type": "array","items": {"type": "string"}},
"AdditionalData": {"$ref": "/#definitions/ExtensionTypeList"}}},
"Contact": {
"type": "object"},
"properties": {
"role": {
"enum": ["creator","reporter","admin","tech","provider","user","billing","legal","irt","abuse","cc","cc-irt","leo","vendor","vendor-support","victim","victim-notified","ext-value"],
"ext-role": {"type": "string"},
"type": {"enum": ["person","organization","ext-value"],
"ext-type": {"type": "string"},
"restriction": {"$ref": "/#definitions/restriction"},
"ext-restriction": {"type": "string"},
"ContactName": {"type": "array","items": {"type": "string"}}}
"ContactTitle": {"type": "array", "items": {"type": "string"}},
"Description": {"type": "array", "items": {"type": "string"}},
"RegistryHandle": {
  "type": "array", "items": {"$ref": "/#definitions/RegistryHandle"}},
"PostalAddress": {
  "type": "array", "items": {"$ref": "/#definitions/PostalAddress"}},
"Email": {"type": "array", "items": {"$ref": "/#definitions/Email"}},
"Telephone": {
  "type": "array", "items": {"$ref": "/#definitions/Telephone"}},
"Timezone": {"type": "string"},
"Contact": {
  "type": "array", "items": {"$ref": "/#definitions/Contact"}},
"AdditionalData": {"$ref": "/#definitions/ExtensionTypeList"},
"RegistryHandle": {
  "type": "object",
  "properties": {
    "handle": {"type": "string"},
    "registry": {
      "enum": ["internic", "apnic", "arin", "lacnic", "ripe", "afrinic", "local", "ext-value"],
      "ext-registry": {"type": "string"},
      "required": ["registry"],
      "additionalProperties": false},
    "PostalAddress": {
      "type": "object",
      "properties": {
        "PAddress": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}}},
        "required": ["PAddress"],
        "additionalProperties": false},
        "Email": {
          "type": "object",
          "properties": {
            "EmailTo": {"type": "string"},
            "Description": {"type": "array", "items": {"type": "string"}}},
            "required": ["EmailTo"],
            "additionalProperties": false},
            "Telephone": {
              "type": "object",
              "properties": {
                "Telephone": {"type": "string"},
                "Description": {"type": "array", "items": {"type": "string"}}}
                "required": ["Telephone"],
                "additionalProperties": false}
"enum": ["wired", "mobile", "fax", "hotline", "ext-value"],
"ext-type": {"type": "string"},
"TelephoneNumber": {"type": "string"},
"Description": {"type": "array", "items": {"type": "string"}},
"required": ["TelephoneNumber"],
"additionalProperties": false,
"Discovery": {
  "type": "object",
  "properties": {
    "source": {
      "enum": ["nidps", "hips", "siem", "av", "third-party-monitoring",
                "incident", "os-log", "application-log", "device-log",
                "network-flow", "passive-dns", "investigation", "audit",
                "internal-notification", "external-notification", "leo",
                "partner", "actor", "unknown", "ext-value"],
      "ext-source": {"type": "string"},
      "restriction": {"$ref": "#/definitions/restriction"},
      "ext-restriction": {"type": "string"},
      "Description": {"type": "array", "items": {"type": "string"}},
      "Contact": {
        "type": "array", "items": {"$ref": "#/definitions/Contact"},
        "DetectionPattern": {
          "type": "array", "items": {"$ref": "#/definitions/DetectionPattern"}
        },
        "required": [],
        "additionalProperties": false,
      },
      "DetectionPattern": {
        "type": "object",
        "properties": {
          "restriction": {"$ref": "#/definitions/restriction"},
          "ext-restriction": {"type": "string"},
          "observable-id": {"$ref": "#/definitions/IDtype"},
          "Application": {"$ref": "#/definitions/SoftwareType"},
          "Description": {"type": "array", "items": {"type": "string"}},
          "DetectionConfiguration": {
            "type": "array", "items": {"type": "string"}
          },
          "required": ["Application"],
          "additionalProperties": false,
        },
        "Method": {
          "type": "object",
          "properties": {
            "restriction": {"$ref": "#/definitions/restriction"},
            "ext-restriction": {"type": "string"},
            "References": {
              "type": "array", "items": {"$ref": "#/definitions/Reference"}
            },
            "Description": {"type": "array", "items": {"type": "string"}},
            "AttackPattern": {
              "type": "array", "items": {"$ref": "#/definitions/StructuredInfo"}
            },
            "Vulnerability": {
              "type": "array", "items": {"$ref": "#/definitions/StructuredInfo"}
            },
          },
          "additionalProperties": false,
        },
      },
      "internal": false,
      "external": false,
      "unknown": false,
      "strict": false,
      "source": "internal",
      "restriction": "internal",
      "Description": ["Internal source", "Internal restriction", "Internal description"],
      "Contact": ["Internal contact", "Internal description"],
      "DetectionPattern": ["Internal detection pattern", "Internal description"],
      "Method": ["Internal method", "Internal description"],
      "Vulnerability": ["Internal vulnerability", "Internal description"],
      "observable-id": "internal"
    },
    "external": {
      "type": "string"},
    "unknown": {
      "type": "string"},
    "strict": {
      "type": "string"},
    "source": {
      "type": "string"},
    "restriction": {
      "type": "string"},
    "Description": {
      "type": "string"},
    "Contact": {
      "type": "string"},
    "DetectionPattern": {
      "type": "string"},
    "Method": {
      "type": "string"},
    "Vulnerability": {
      "type": "string"
    },
    "observable-id": {
      "type": "string"},
    "Application": {
      "type": "string"},
    "DetectionConfiguration": {
      "type": "string"}
  }
}
"type": "array", "items": {"$ref": "/definitions/StructuredInfo"},

"Reference": {
  "type": "object",
  "properties": {
    "observable-id": {"$ref": "/definitions/IDtype"},
    "ReferenceName": {"type": "string"},
    "URL": {"type": "array", "items": {"$ref": "/definitions/URLtype"}},
    "Description": {"type": "array", "items": {"type": "string"}}
  },
  "required": [],
  "additionalProperties": false
},

"Reference": {
  "type": "object",
  "properties": {
    "observable-id": {"$ref": "/definitions/IDtype"},
    "ReferenceName": {"type": "string"},
    "URL": {"type": "array", "items": {"$ref": "/definitions/URLtype"}},
    "Description": {"type": "array", "items": {"type": "string"}}
  },
  "required": [],
  "additionalProperties": false
},

"Assessment": {
  "type": "object",
  "properties": {
    "occurrence": {"enum": ["actual", "potential"]},
    "restriction": {"$ref": "/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "observable-id": {"$ref": "/definitions/IDtype"},
    "IncidentCategory": {"type": "array", "items": {"type": "string"}}
  },
  "required": [],
  "additionalProperties": false
},

"SystemImpact": {
  "type": "array", "items": {"$ref": "/definitions/SystemImpact"},
  "BusinessImpact": {
    "type": "array", "items": {"$ref": "/definitions/BusinessImpact"},
    "TimeImpact": {
      "type": "array", "items": {"$ref": "/definitions/TimeImpact"},
      "MonetaryImpact": {
        "type": "array", "items": {"$ref": "/definitions/MonetaryImpact"},
        "IntendedImpact": {
          "type": "array", "items": {"$ref": "/definitions/IntendedImpact"}
        }
      }
    }
  }
}

"Counter": {
  "type": "array", "items": {"$ref": "/definitions/Counter"},
  "MitigatingFactor": {
    "type": "array", "items": {"$type": "string"}
  },
  "Cause": {"type": "array", "items": {"$type": "string"},
  "Confidence": {"$ref": "/definitions/Confidence"},
  "AdditionalData": {"$ref": "/definitions/ExtensionTypeList"},
  "required": [],
  "additionalProperties": false
},

"SystemImpact": {
  "type": "object",
  "properties": {
    "severity": {
      "enum": ["low", "medium", "high"]
    },
    "completion": {"enum": ["failed", "succeeded"]}
  }
}
"type": {
    "ext-type": {"type": "string"},
    "Description": {"type": "array", "items": {"type": "string"}}},
"required": ["type"],
"additionalProperties": false},
"BusinessImpact": {
    "type": "object",
    "properties": {
        "severity": {
            "enum": ["none", "low", "medium", "high", "unknown", "ext-value"],
            "ext-severity": {"type": "string"},
            "type": {
                "ext-type": {"type": "string"},
                "Description": {"type": "array", "items": {"type": "string"}}},
        "required": ["type"],
        "additionalProperties": false},
"TimeImpact": {
    "type": "object",
    "properties": {
        "value": {"type": "number"},
        "severity": {"enum": ["low", "medium", "high"]},
        "metric": {"enum": ["labor", "elapsed", "downtime", "ext-value"]},
        "ext-metric": {"type": "string"},
        "duration": {"$ref": "/#definitions/duration"},
        "ext-duration": {"type": "string"},
        "required": ["metric"],
        "additionalProperties": false},
"MonetaryImpact": {
    "type": "object",
    "properties": {
        "value": {"type": "number"},
        "severity": {"enum": ["low", "medium", "high"]},
        "currency": {"type": "string"},
        "required": []},
"additionalProperties": false,
"Confidence": {
  "type": "object",
  "properties": {
    "value": {"type": "number"},
    "rating": {
      "enum": ["low","medium","high","numeric","unknown","ext-value"],
      "ext-rating": {"type": "string"},
      "required": ["rating"],
      "additionalProperties": false
    }
  }
}

"History": {
  "type": "object",
  "properties": {
    "restriction": {"$ref": "/#/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "HistoryItem": {
      "type": "array","items": {"$ref": "/#/definitions/HistoryItem"}}},
    "required": ["HistoryItem"],
    "additionalProperties": false
  }
}

"HistoryItem": {
  "type": "object",
  "properties": {
    "action": {"$ref": "/#/definitions/action"},
    "ext-action": {"type": "string"},
    "restriction": {"$ref": "/#/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "observable-id": {"$ref": "/#/definitions/IDtype"},
    "DateTime": {"$ref": "/#/definitions/DATETIME"},
    "IncidentID": {"$ref": "/#/definitions/IncidentID"},
    "Contact": {"$ref": "/#/definitions/Contact"},
    "Description": {"type": "array","items": {"type": "string"}},
    "DefinedCOA": {"type": "array","items": {"type": "string"}},
    "AdditionalData": {"$ref": "/#/definitions/ExtensionTypeList"},
    "required": ["DateTime","action"],
    "additionalProperties": false
  }
}

"EventData": {
  "type": "object",
  "properties": {
    "restriction": {"$ref": "/#/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "observable-id": {"$ref": "/#/definitions/IDtype"},
    "Description": {"type": "array","items": {"type": "string"}},
    "DetectTime": {"type": "string"},
    "StartTime": {"type": "string"},
    "EndTime": {"type": "string"},
    "RecoveryTime": {"type": "string"},
    "ReportTime": {"type": "string"},
    "Contact": {
      "additionalProperties": false
    }
  }
}
"type": "array","items": {"$ref": "#/definitions/Contact"},
"Discovery": {  
"type": "array","items": {"$ref": "#/definitions/Discovery"},
"Assessment": {"$ref": "#/definitions_Assessment"},
"Method": { 
"type": "array","items": {"$ref": "#/definitions/Method"},
"System": {  
"type": "array","items": {"$ref": "#/definitions/System"},
"Expectation": { 
"type": "array","items": {"$ref": "#/definitions/Expectation"},
"RecordData": {"type": "array", "items": {"$ref": "#/definitions/RecordData"},
"EventData": {  
"type": "array","items": {"$ref": "#/definitions/EventData"},
"AdditionalData": {"$ref": "/definitions/ExtensionTypeList"},
"required": ["ReportTime"],
"additionalProperties": false,
"Expectation": {  
"type": "object",
"properties": {  
"action": {"$ref": "/definitions/action"},
"ext-action": {"type": "string"},
"severity": {"enum": ["low","medium","high"]},
"restriction": {"$ref": "/definitions/restriction"},
"ext-restriction": {"type": "string"},
"observable-id": {"$ref": "/definitions/IDtype"},
"Description": {"type": "array","items": {"type": "string"}},
"DefinedCOA": {"type": "array","items": {"type": "string"}},
"StartTime": {"type": "string"},
"EndTime": {"type": "string"},
"Contact": {"$ref": "/definitions/Contact"},
"required": [],
"additionalProperties": false,
"System": {  
"type": "object",
"properties": {  
"category": {  
"enum": ["source","target","intermediate","sensor","infrastructure","infrastructure"],
"ext-category": {"type": "string"},
"interface": {"type": "string"},
"spoofed": {"enum": ["unknown","yes","no"]},
"virtual": {"enum": ["yes","no","unknown"]},
"ownership": {  
"enum": ["organization","personal","partner","customer","no-relationship","unknown","ext-value"]},
"ext-ownership": {"type": "string"},
"restriction": {"$ref": "/definitions/restriction"},
"ext-restriction": {"type": "string"},

"observable-id": {"$ref": "#/definitions/IDtype"},
"Node": {"$ref": "#/definitions/Node"},
"NodeRole": {
  "type": "array","items": {"$ref": "#/definitions/NodeRole"},
"Service": {
  "type": "array","items": {"$ref": "#/definitions/Service"},
"OperatingSystem": {
  "type": "array","items": {"$ref": "#/definitions/SoftwareType"},
"Counter": {
  "type": "array","items": {"$ref": "#/definitions/Counter"},
"AssetID": {"type": "array","items": {"type": "string"},
"Description": {"type": "array","items": {"type": "string"},
"AdditionalData": {"$ref": "#/definitions/ExtensionTypeList"},
"required": ["Node"],
"additionalProperties": false},
"Node": {
  "type": "object",
  "properties": {
    "DomainData": {
      "type": "array","items": {"$ref": "#/definitions/DomainData"},
    "Address": {
      "type": "array","items": {"$ref": "#/definitions/Address"},
    "PostalAddress": {"type": "string"},
    "Location": {"type": "array","items": {"type": "string"},
    "Counter": {"type": "array","items": {"$ref": "#/definitions/Counter"}}
  },
  "required": [],
  "additionalProperties": false},
"Address": {
  "type": "object",
  "properties": {
    "value": {"type": "string"},
    "category": {
      "enum": ["asn","atm","e-mail","ipv4-addr","ipv4-net",
        "ipv4-net-masked","ipv4-net-mask","ipv6-addr","ipv6-net",
        "ipv6-net-masked","mac","site-url","ext-value"],
    "ext-category": {"type": "string"},
    "vlan-name": {"type": "string"},
    "vlan-num": {"type": "integer"},
    "observable-id": {"$ref": "#/definitions/IDtype"},
  "required": ["category"],
  "additionalProperties": false},
"NodeRole": {
  "type": "object",
  "properties": {
    "category": {
      "enum": ["client","client-enterprise","client-partner","client-remote",
        "client-kiosk","client-mobile","server-internal",
        "server-public","www","mail","webmail","messaging"],
"streaming","voice","file","ftp","p2p","name","directory","credential","print","application","database","backup","dhcp","assessment","source-control","config-management","monitoring","infra","infra-firewall","infra-router","infra-switch","camera","proxy","remote-access","log","virtualization","pos","scada","scada-supervisory","sinkhole","honeypot","anomyzation","c2-server","malware-distribution","drop-server","hot-point","reflector","phishing-site","spear-phishing-site","recruiting-site","fraudulent-site","ext-value"},
"ext-category": {"type": "string"},
"Description": {"type": "array","items": {"type": "string"}},
"required": ["category"],
"additionalProperties": false},
"Counter": {
  "type": "object",
  "properties": {
    "value": {"type": "string"},
    "type": {"enum": ["count","peak","average","ext-value"]},
    "ext-type": {"type": "string"},
    "unit": {"enum": ["byte","mbit","packet","flow","session","alert",
      "message","event","host","site","organization","ext-value"]},
    "ext-unit": {"type": "string"},
    "meaning": {"type": "string"},
    "duration": {"$ref": "#/definitions/duration"},
    "ext-duration": {"type": "string"},
    "required": ["type","unit"],
    "additionalProperties": false},
"DomainData": {
  "type": "object",
  "properties": {
    "system-status": {
      "enum": ["spoofed","fraudulent","innocent-hacked",
        "innocent-hijacked","unknown","ext-value"],
      "ext-system-status": {"type": "string"},
      "domain-status": {
        "enum": ["reservedDelegation","assignedAndActive","assignedAndInactive",
          "assignedAndOnHold","revoked","transferPending","registryLock",
          "registrarLock","other","unknown","ext-value"],
        "ext-domain-status": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Name": {"type": "string"},
        "DateDomainWasChecked": {"$ref": "#/definitions/DATETIME"},
        "RegistrationDate": {"$ref": "#/definitions/DATETIME"},
        "ExpirationDate": {"$ref": "#/definitions/DATETIME"},
        "RelatedDNS": {
          "type": "array","items": {"$ref": "#/definitions/ExtensionType"}
      }
  }
}
"NameServers": {
  "type": "array", "items": {
    "$ref": "/definitions/NameServers"  
},  
"DomainContacts": {
  "$ref": "/definitions/DomainContacts"},  
"required": ["Name", "system-status", "domain-status"],  
"additionalProperties": false},  
"NameServers": {
  "type": "object",  
  "properties": {
    "Server": {
      "type": "string"},  
    "Address": {
      "type": "array", "items": {
        "$ref": "/definitions/Address"}}},  
  "required": ["Server", "Address"],  
  "additionalProperties": false},  
"DomainContacts": {
  "type": "object",  
  "properties": {
    "SameDomainContact": {
      "type": "string"},  
    "Contact": {
      "type": "array", "items": {
        "$ref": "/definitions/Contact"}}},  
  "required": ["Contact"],  
  "additionalProperties": false},  
"Service": {
  "type": "object",  
  "properties": {
    "ip-protocol": {
      "type": "integer"},  
    "observable-id": {
      "$ref": "/definitions/IDtype"},  
    "ServiceName": {
      "$ref": "/definitions/ServiceName"},  
    "Port": {
      "type": "integer"},  
    "Portlist": {
      "$ref": "/definitions/PORTLIST"},  
    "ProtoCode": {
      "type": "integer"},  
    "ProtoType": {
      "type": "integer"},  
    "ProtoField": {
      "type": "integer"},  
    "ApplicationHeaderField": {
      "$ref": "/definitions/ExtensionTypeList"},  
    "EmailData": {
      "$ref": "/definitions/EmailData"},  
    "Application": {
      "$ref": "/definitions/SoftwareType"},  
  "required": [],  
  "additionalProperties": false},  
"ServiceName": {
  "type": "object",  
  "properties": {
    "IANAService": {
      "type": "string"},  
    "URL": {
      "type": "array", "items": {
        "$ref": "/definitions/URLtype"},  
    "Description": {
      "type": "array", "items": {
        "type": "string"}}},  
  "required": [],  
  "additionalProperties": false},  
"EmailData": {
  "type": "object",  
  "properties": {
    "observable-id": {
      "$ref": "/definitions/IDtype"},
"EmailTo": {"type": "array","items": {"type": "string"}},
"EmailFrom": {"type": "string"},
"EmailSubject": {"type": "string"},
"EmailX-Mailer": {"type": "string"},
"EmailHeaderField": {
  "type": "array","items": {"$ref": "/definitions/ExtensionType"},
"EmailHeaders": {"type": "string"},
"EmailBody": {"type": "string"},
"EmailMessage": {"type": "string"},
"HashData": {
  "type": "array","items": {"$ref": "/definitions/HashData"},
"Signature": {"type": "array","items": {"type": "string"}},
  "required": [],
  "additionalProperties": false
},
"RecordData": {
  "type": "object",
  "properties": {
    "restriction": {"$ref": "/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "observable-id": {"$ref": "/definitions/IDtype"},
    "DateTime": {"$ref": "/definitions/DATETIME"},
    "Description": {"type": "array","items": {"type": "string"}},
    "Application": {"$ref": "/definitions/SoftwareType"},
    "RecordPattern": {
      "type": "array","items": {"$ref": "/definitions/RecordPattern"},
    "RecordItem": {
      "type": "array","items": {"$ref": "/definitions/ExtensionType"},
      "URL": {
        "type": "array","items": {"$ref": "/definitions/URLtype"},
        "FileData": {
          "type": "array","items": {"$ref": "/definitions/FileData"},
          "WindowsRegistryKeysModified": {
            "type": "array",
            "items": {"$ref": "/definitions/WindowsRegistryKeysModified"},
          "CertificateData": {
            "type": "array","items": {"$ref": "/definitions/CertificateData"},
          "AdditionalData": {"$ref": "/definitions/ExtensionTypeList"},
          "required": [],
          "additionalProperties": false
        },
      "RecordPattern": {
        "type": "object",
        "properties": {
          "value": {"type": "string"},
          "type": {"enum": ["regex","binary","xpath","ext-value"],
        "ext-type": {"type": "string"},
        "offset": {"type": "integer"},
        "offsetunit": {"enum": ["line","byte","ext-value"]},
"ext-offsetunit": {"type": "string"},
"instance": {"type": "integer"},
"required": ["type"],
"additionalProperties": false},
"WindowsRegistryKeysModified": {
"type": "object",
"properties": {
"observable-id": {"$ref": "#/definitions/IDtype"},
"Key": {"type": "array","items": {"$ref": "#/definitions/Key"}}},
"required": ["Key"],
"additionalProperties": false},
"Key": {
"type": "object",
"properties": {
"registryaction": {"enum": ["add-key","add-value","delete-key",
"delete-value","modify-key","modify-value",
"ext-value"]},
"ext-registryaction": {"type": "string"},
"observable-id": {"$ref": "#/definitions/IDtype"},
"KeyName": {"type": "string"},
"KeyValue": {"type": "string"},
"required": ["KeyName"],
"additionalProperties": false},
"CertificateData": {
"type": "object",
"properties": {
"restriction": {"$ref": "#/definitions/restriction"},
"ext-restriction": {"type": "string"},
"observable-id": {"$ref": "#/definitions/IDtype"},
"Certificate": {
"type": "array","items": {"$ref": "#/definitions/Certificate"}}},
"required": ["Certificate"],
"additionalProperties": false},
"Certificate": {
"type": "object",
"properties": {
"observable-id": {"$ref": "#/definitions/IDtype"},
"X509Data": {"type": "string"},
"Description": {"type": "array","items": {"type": "string"}}},
"required": ["X509Data"],
"additionalProperties": false},
"FileData": {
"type": "object",
"properties": {
"restriction": {"$ref": "#/definitions/restriction"},
"ext-restriction": {"type": "string"},
"observable-id": {"$ref": "#/definitions/IDtype"},
"File": {"type": "array","items": {"$ref": "#/definitions/File"}}}
"required": ["File"],
"additionalProperties": false},
"File": {
  "type": "object",
  "properties": {
    "FileName": {"type": "string"},
    "FileSize": {"type": "integer"},
    "FileType": {"type": "string"},
    "URL": {"type": "array","items": {"$ref": "#/definitions/URLtype"}},
    "HashData": {"$ref": "#/definitions/HashData"},
    "Signature": {"type": "array","items": {"type": "string"}},
    "AssociatedSoftware": {"$ref": "#/definitions/SoftwareType"},
    "FileProperties": {
      "type": "array","items": {"$ref": "#/definitions/ExtensionType"}},
    "required": [],
    "additionalProperties": false},
  "HashData": {,
    "type": "object",
    "properties": {
      "scope": {"enum": ["file-contents","file-pe-section","file-pe-iat",
                      "file-pe-resource","file-pdf-object","email-hash",
                      "email-hash-header","email-hash-body"],
      "HashTargetID": {"type": "string"},
      "Hash": {"type": "array","items": {"$ref": "#/definitions/Hash"}},
      "FuzzyHash": {
        "type": "array","items": {"$ref": "#/definitions/FuzzyHash"}},
      "required": ["scope"],
      "additionalProperties": false},
    "Hash": {
      "type": "object",
      "properties": {
        "DigestMethod": {"type": "string"},
        "DigestValue": {"type": "string"},
        "CanonicalizationMethod": {},
        "Application": {"$ref": "#/definitions/SoftwareType"},
        "required": ["DigestMethod","DigestValue"],
        "additionalProperties": false},
    "FuzzyHash": {
      "type": "object",
      "properties": {
        "FuzzyHashValue": {"type": "array","items": {"$ref": "#/definitions/ExtensionType"}},
        "Application": {"$ref": "#/definitions/SoftwareType"},
        "AdditionalData": {"$ref": "#/definitions/ExtensionTypeList"},
        "required": ["FuzzyHashValue"],
        "additionalProperties": false},
      "Indicator": {
        "type": "object"},
Takahashi, et al. Expires September 19, 2018 [Page 34]
"properties": {
    "restriction": {"$ref": "#/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "IndicatorID": {"$ref": "#/definitions/IndicatorID"},
    "AlternativeIndicatorID": {
        "type": "array",
        "items": {"$ref": "#/definitions/AlternativeIndicatorID"},
    "Description": {"type": "array", "items": {"type": "string"}},
    "StartTime": {"$ref": "#/definitions/DATETIME"},
    "EndTime": {"$ref": "#/definitions/DATETIME"},
    "Confidence": {"$ref": "#/definitions/Confidence"},
    "Contact": {
        "type": "array", "items": {"$ref": "#/definitions/Contact"},
    "Observable": {"$ref": "#/definitions/Observable"},
    "uid-ref": {"type": "string"},
    "IndicatorExpression": {"$ref": "#/definitions/IndicatorExpression"},
    "IndicatorReference": {"$ref": "#/definitions/IndicatorReference"},
    "NodeRole": {
        "type": "array", "items": {"$ref": "#/definitions/NodeRole"},
    "AttackPhase": {
        "type": "array", "items": {"$ref": "#/definitions/AttackPhase"},
    "Reference": {
        "type": "array", "items": {"$ref": "#/definitions/Reference"},
    "AdditionalData": {"$ref": "#/definitions/ExtensionTypeList"},
    "required": ["IndicatorID"],
    "additionalProperties": false},
"IndicatorID": {
    "type": "object",
    "properties": {
        "id": {"type": "string"},
        "name": {"type": "string"},
        "version": {"type": "string"},
        "required": ["name", "version"],
        "additionalProperties": false},
"AlternativeIndicatorID": {
    "type": "object",
    "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "IndicatorReference": {
            "type": "array",
            "items": {"$ref": "#/definitions/IndicatorReference"}}},
    "required": ["IndicatorReference"],
    "additionalProperties": false},
"Observable": {
    "type": "object",
    "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "IndicatorReference": {
            "type": "array",
            "items": {"$ref": "#/definitions/IndicatorReference"}}},
    "required": ["IndicatorReference"],
    "additionalProperties": false}
"ext-restriction": {"type": "string"},
"System": {"$ref": "#/definitions/System"},
"Address": {"$ref": "#/definitions/Address"},
"DomainData": {"$ref": "#/definitions/DomainData"},
"EmailData": {"$ref": "#/definitions/EmailData"},
"Service": {"$ref": "#/definitions/Service"},
"WindowsRegistryKeysModified": {
  "$ref": "#/definitions/WindowsRegistryKeysModified"},
"FileData": {"$ref": "#/definitions/FileData"},
"CertificateData": {"$ref": "#/definitions/CertificateData"},
"RegistryHandle": {"$ref": "#/definitions/RegistryHandle"},
"RecordData": {"type": "array", "item": {"$ref": "#/definitions/Record"}},
"EventData": {"$ref": "#/definitions/EventData"},
"Incident": {"$ref": "#/definitions/Incident"},
"Expectation": {"$ref": "#/definitions/Expectation"},
"Reference": {"$ref": "#/definitions/Reference"},
"Assessment": {"$ref": "#/definitions/Assessment"},
"DetectionPattern": {"$ref": "#/definitions/DetectionPattern"},
"HistoryItem": {"$ref": "#/definitions/HistoryItem"},
"BulkObservable": {"$ref": "#/definitions/BulkObservable"},
"AdditionalData": {"$ref": "#/definitions/ExtensionTypeList"},
"required": [],
"additionalProperties": false,
"BulkObservable": {
  "type": "object",
  "properties": {
    "ext-type": {"type": "string"},
    "BulkObservableFormat": {"$ref": "#/definitions/BulkObservableFormat"},
    "BulkObservableList": {"type": "array", "item": {"$ref": "#/definitions/ExtensionTypeList"}},
    "AdditionalData": {"$ref": "#/definitions/ExtensionTypeList"},
  }},
"IndicatorExpression": {
  "type": "object",
  "properties": {
    "Hash": {"$ref": "#/definitions/Hash"},
    "AdditionalData": {"$ref": "#/definitions/ExtensionTypeList"},
  }},
"required": []
"additionalProperties": false,
"IndicatorExpression": {
"type": "object",
"properties": {
  "operator": {"enum": ["not","and","or","xor"]},
  "ext-operator": {"type": "string"},
  "IndicatorExpression": {
    "type": "array",
    "items": {"$ref": "/#/definitions/IndicatorExpression"},
  
  "Observable": {
    "type": "array",
    "items": {"$ref": "/#/definitions/Observable"},
  
  "uid-ref": {"type": "string"},
  "IndicatorReference": {
    "type": "array",
    "items": {"$ref": "/#/definitions/IndicatorReference"},
  
  "AdditionalData": {"$ref": "/#/definitions/ExtensionTypeList"},
  "required": [],
  "additionalProperties": false
},

"IndicatorReference": {
  "type": "object",
  "properties": {
    "uid-ref": {"type": "string"},
    "euid-ref": {"type": "string"},
    "version": {"type": "string"},
    "required": [],
    "additionalProperties": false
},

"AttackPhase": {
  "type": "object",
  "properties": {
    "AttackPhaseID": {"type": "array",
    "items": {"type": "string"}},
    "URL": {"type": "array",
    "items": {"$ref": "/#/definitions/URLtype"}},
    "Description": {"type": "array",
    "items": {"type": "string"}},
    "AdditionalData": {"$ref": "/#/definitions/ExtensionTypeList"},
    "required": [],
    "additionalProperties": false
},

"title": ".JSON-teach-Doc",,
"description": ".JSON schema for IODEF-Doc class",
"type": "object",
"properties": {
  "version": {"type": "string"},
  "lang": {"$ref": "/#/definitions/lang"},
  "format-id": {"type": "string"},
  "private-enum-name": {"type": "string"},
  "private-enum-id": {"type": "string"},
  "Incident": {
    "type": "array",
    "items": {"$ref": "/#/definitions/Incident"},
  
  "AdditionalData": {"$ref": "/#/definitions/ExtensionTypeList"},
  "required": [{"version"}, "Incident"],
  "additionalProperties": false
}
6. Acknowledgements

TBD.

7. IANA Considerations

This memo includes no request to IANA.

8. Security Considerations

This memo does not provide any further security considerations than the one described in [RFC7970].

9. Normative References

[jsonschema]

http://json-schema.org/


Authors’ Addresses

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

Phone: +81 42 327 5862
Email: takeshi_takahashi@nict.go.jp
Roman Danyliw  
CERT, Software Engineering Institute, Carnegie Mellon University  
4500 Fifth Avenue  
Pittsburgh, PA  
USA  
Email: rdd@cert.org

Mio Suzuki  
National Institute of Information and Communications Technology  
4-2-1 Nukui-Kitamachi  
Koganei, Tokyo 184-8795  
Japan  
Email: mio@nict.go.jp
JSON binding of IODEF

draft-ietf-mile-jsoniodef-04

Abstract

RFC7970 specified an information model and a corresponding XML data model for exchanging incident and indicator information. This draft provides an alternative data model implementation in JSON.

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 https://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 January 18, 2019.

Copyright Notice

Copyright (c) 2018 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 (https://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
   1.1. Requirements Language .................... 3
2. IODEF Data Types .............................. 3
   2.1. Abstract Data Type to JSON Data Type Mapping 3
   2.2. Complex JSON Types ....................... 4
       2.2.1. Multilingual Strings .................. 4
       2.2.2. Software and SoftwareReference ......... 5
       2.2.3. StructuredInfo ......................... 5
       2.2.4. EXTENSION .............................. 6
3. IODEF JSON Data Model ......................... 6
   3.1. Classes and Elements ..................... 6
   3.2. Mapping between JSON and XML IODEF .......... 16
4. Examples ....................................... 17
   4.1. Minimal Example ............................ 17
   4.2. Indicators from a Campaign ................. 18
5. The IODEF Data Model (CDDL) .................. 20
6. Acknowledgements .............................. 35
7. IANA Considerations ........................... 35
8. Security Considerations ....................... 35
9. Normative References ........................... 35
Appendix A. The IODEF Data Model (JSON Schema) .. 35
Authors’ Addresses ............................. 55

1. Introduction

[RFC7970] defines a data representation for security incident reports and indicators commonly exchanged by operational security teams. It facilitates the automated exchange of this information to enable mitigation and watch-and-warning. Section 3 of [RFC7970] defined an information model using Unified Modeling Language (UML) and a corresponding Extensible Markup Language (XML) schema data model in Section 8. This UML-based information model and XML-based data model are referred to as IODEF UML and IODEF XML, respectively in this document.

This document defines an alternate implementation of the IODEF UML information model by specifying a JavaScript Object Notation (JSON) data model using JSON Schema [jsonschema]. This JSON data model is referred to as IODEF JSON in this document.

IODEF JSON provides all of the expressivity of IODEF XML. It gives implementers and operators an alternative format to exchange the same information.
The normative IODEF JSON data model is found in Section 5. Section 2 and Section 3 describe the data types and elements of this data model. Section 4 provides examples.

1.1. Requirements Language

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].

2. IODEF Data Types

The abstract IODEF JSON implements the abstract data types specified in Section 2 of [RFC7970].

2.1. Abstract Data Type to JSON Data Type Mapping

IODEF JSON uses native and derived JSON data types. Figure 1 describes the mapping between the abstract data types in Section 2 of [RFC7970] and their corresponding implementations in IODEF JSON.
<table>
<thead>
<tr>
<th>IODEF Data Type</th>
<th>[RFC7970] Reference</th>
<th>JSON Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTEGER</td>
<td>Section 2.1</td>
<td>&quot;integer&quot; per [jsonschema]</td>
</tr>
<tr>
<td>REAL</td>
<td>Section 2.2</td>
<td>&quot;number&quot; per [jsonschema]</td>
</tr>
<tr>
<td>CHARACTER</td>
<td>Section 2.3</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>STRING</td>
<td>Section 2.3</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>ML_STRING</td>
<td>Section 2.4</td>
<td>see Section 2.2.1</td>
</tr>
<tr>
<td>BYTE</td>
<td>Section 2.5.1</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>BYTE[]</td>
<td>Section 2.5.1</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>HEXBIN</td>
<td>Section 2.5.2</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>HEXBIN[]</td>
<td>Section 2.5.2</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>ENUM</td>
<td>Section 2.6</td>
<td>&quot;enum&quot; array per [jsonschema]</td>
</tr>
<tr>
<td>DATETIME</td>
<td>Section 2.7</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>TIMEZONE</td>
<td>Section 2.8</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>PORTLIST</td>
<td>Section 2.9</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>POSTAL</td>
<td>Section 2.10</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>POSTAL_ML</td>
<td>Section 2.10</td>
<td>see ML_STRING, Section 2.2.1</td>
</tr>
<tr>
<td>PHONE</td>
<td>Section 2.11</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>EMAIL</td>
<td>Section 2.12</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>URL</td>
<td>Section 2.13</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>ID</td>
<td>Section 2.14</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>IDREF</td>
<td>Section 2.14</td>
<td>&quot;string&quot; per [jsonschema]</td>
</tr>
<tr>
<td>SOFTWARE</td>
<td>Section 2.15</td>
<td>see Section 2.2.2</td>
</tr>
<tr>
<td>STRUCTURED</td>
<td>RFC 7213</td>
<td>see Section 2.2.3</td>
</tr>
<tr>
<td>EXTENSION</td>
<td>Section 2.16</td>
<td>see Section 2.2.4</td>
</tr>
</tbody>
</table>

Figure 1

2.2. Complex JSON Types

2.2.1. Multilingual Strings

A string that needs to be represented in a human-readable language different than the default encoding of the document is represented in the information model by the ML_STRING data type. This data type is implemented as an object with "value", "lang", and "translation-id" elements as defined in Section 5. Examples are shown below.

"MLStringType": {
  "value": "free-form text", //STRING
  "lang": "en", //ENUM
  "translation-id": "jp2en0023" //STRING
}
2.2.2. Software and SoftwareReference

A particular version of software is represented in the information model by the SOFTWARE data type. This software can be described by using a reference, a URL, or with free-form text. The SOFTWARE data type is implemented as an object with "SoftwareReference", "URL", "Description", and "Description_ML" elements as defined in Section 5. Examples are shown below.

"SoftwareType": {
  "SoftwareReference": {...},  //SoftwareReference
  "Description": ["MS Windows"]  //STRING
}

SoftwareReference class is a reference to a particular version of software. Examples are shown below.

"SoftwareReference": {
  "value": "cpe:/a:google:chrome:59.0.3071.115 ",  //STRING
  "spec-name": "cpe",  //ENUM
  "dtype": "string",  //ENUM
}

2.2.3. StructuredInfo

Information provided in a form of structured string, such as ID, or structured information, such as XML documents, is represented in the information model by the StructuredInfo data type. Note that this type was originally specified in RFC7203. The StructuredInfo data type is implemented as an object with "SpecID", "ext-SpecID", "ContentID", "RawData", "Reference" elements. An example for embedding a structured ID is shown below.

"StructuredInformation": {
  "SpecID": "cve",  //ENUM
  "ContentID": "CVE-2007-5000"  //STRING
}

When embedding the raw data, base64 conversion should be used for encoding the data, as shown below.

"StructuredInformation": {
  "SpecID": "oval",  //ENUM
  "RawData": "<<<strings encoded with base64>>>"  //BYTE
}
2.2.4. EXTENSION

Information not otherwise represented in the IODEF can be added using the EXTENSION data type. This data type is a generic extension mechanism. The EXTENSION data type is implemented as an ExtensionType object with "value", "name", "dtype", "ext-dtype", "meaning", "formatid", "restriction", "ext-restriction", and "observable-id" elements. An example for embedding a structured ID is shown below.

"ExtensionType": {
   "value": "xxxxxxx",                          //String
   "name": "Syslog",                            //String
   "dtype": "string",                           //String
   "meaning": "Syslog from the security appliance X",     //String
}

3. IODEF JSON Data Model

3.1. Classes and Elements

The following table shows the list of IODEF Classes, their elements, and the corresponding section in [RFC7970]. Note that the complete JSON schema is defined in Section 5.

<table>
<thead>
<tr>
<th>IODEF Class</th>
<th>Class Elements and Attribute</th>
<th>Corresponding Section in [RFC7970]</th>
</tr>
</thead>
<tbody>
<tr>
<td>IODEF-Document</td>
<td>version lang? format-id?</td>
<td>3.1</td>
</tr>
<tr>
<td></td>
<td>private-enum-name?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>private-enum-id?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incident+ AdditionalData*</td>
<td></td>
</tr>
<tr>
<td>Incident</td>
<td>purpose ext-purpose? status?</td>
<td>3.2</td>
</tr>
<tr>
<td>IncidentID</td>
<td>id</td>
<td>3.4</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------</td>
<td>-----</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>instance?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>restriction?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
<td></td>
</tr>
<tr>
<td>AlternativeID</td>
<td>restriction?</td>
<td>3.5</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IncidentID+</td>
<td></td>
</tr>
<tr>
<td>RelatedActivity</td>
<td>restriction?</td>
<td>3.6</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IncidentID*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ThreatActor*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Campaign*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IndicatorID*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidence?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
<td></td>
</tr>
<tr>
<td>ThreatActor</td>
<td>restriction?</td>
<td>3.7</td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ThreatActorID*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AdditionalData*</td>
<td></td>
</tr>
<tr>
<td>Campaign</td>
<td>restriction?</td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>source?</td>
<td>ext-source?</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>DetectionPattern</td>
<td>restriction?</td>
<td>ext-restriction?</td>
</tr>
<tr>
<td>Method</td>
<td>restriction?</td>
<td>ext-restriction?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reference</td>
<td>observable-id?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cause_ML*  Confidence?  AdditionalData*  3.12

SystemImpact  severity?  completion?  type  ext-type?  Description*  Description_ML*  3.12.1

BusinessImpact  severity?  ext-severity?  type  ext-type?  Description*  Description_ML*  3.12.2


MonetaryImpact  value  severity?  currency?  3.12.4

Confidence  value  rating  ext-rating?  3.12.5

History  restriction?  ext-restriction?  HistoryItem+  3.13

HistoryItem  action  ext-action?  restriction?  ext-restriction?  observable-id?  DateTime  IncidentID?  Contact?  Description*  Description_ML*  DefinedCOA*
<table>
<thead>
<tr>
<th></th>
<th>AdditionalData*</th>
<th>3.13.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventData</td>
<td>restriction?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>observable-id?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DetectTime?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>StartTime?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EndTime?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RecoveryTime?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ReportTime?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contact*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Discovery*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assessment?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Method*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Expectation*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DefinedCOA*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>StartTime?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EndTime?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contact*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.14</td>
<td></td>
</tr>
</tbody>
</table>

|          | 3.14            |        |

|          | action?         |        |
|          | ext-action?     |        |
|          | severity?       |        |
|          | restriction?    |        |
|          | ext-restriction?|        |
|          | Description*    |        |
|          | Description_ML* |        |
|          | DefinedCOA*     |        |
|          | StartTime?      |        |
|          | EndTime?        |        |
|          | Contact*        |        |
|          | 3.15            |        |

|          | category?       |        |
|          | ext-category?   |        |
|          | interface?      |        |
|          | spoofed?        |        |
|          | virtual?        |        |
|          | ownership?      |        |
|          | ext-ownership?  |        |
|          | restriction?    |        |
|          | ext-restriction?|        |
|          | Node*           |        |
|          | NodeRole*       |        |
|          | Service*        |        |
|          | OperatingSystem*|        |
|          | Counter*        |        |

<p>|          | 3.14            |        |</p>
<table>
<thead>
<tr>
<th></th>
<th>AssetID*</th>
<th>Description*</th>
<th>Description.Middle*</th>
<th>AdditionalData*</th>
<th>3.16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>DomainData*</td>
<td>Address*</td>
<td>PostalAddress?</td>
<td>Location*</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Location.Middle*</td>
<td>Counter*</td>
<td>3.17</td>
</tr>
<tr>
<td>Address</td>
<td>value</td>
<td>category</td>
<td>ext-category?</td>
<td>vlan-name?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vlan-num?</td>
<td>observable-id?</td>
<td>3.17.1</td>
</tr>
<tr>
<td>NodeRole</td>
<td>category</td>
<td>ext-category?</td>
<td>Description*</td>
<td>Description.Middle*</td>
<td>3.17.2</td>
</tr>
<tr>
<td>Counter</td>
<td>value</td>
<td>type</td>
<td>ext-type?</td>
<td>unit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ext-unit?</td>
<td>meaning?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>meaning.Middle?</td>
<td>duration?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ext-duration?</td>
<td>3.17.3</td>
<td></td>
</tr>
<tr>
<td>DomainData</td>
<td>system-status</td>
<td>ext-system-status?</td>
<td>domain-status</td>
<td>ext-domain-status?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>observable-id?</td>
<td>Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DateDomainWasChecked?</td>
<td>RegistrationDate?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ExpirationDate?</td>
<td>RelatedDNS*</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Nameservers*</td>
<td>DomainContacts?</td>
<td>3.18</td>
</tr>
<tr>
<td>Nameserver</td>
<td>Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address*</td>
<td>3.18.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DomainContacts</td>
<td>SameDomainContact?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contact+</td>
<td>3.18.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>ip-protocol?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>observable-id?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ServiceName?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Portlist?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ProtoCode?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ProtoType?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ProtoField?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ApplicationHeaderField*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EmailData?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application?</td>
<td>3.18.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ServiceName</td>
<td>IANAService?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
<td>3.18.4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EmailData</td>
<td>observable-id?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EmailTo*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EmailFrom?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EmailSubject?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EmailX-Mailer?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EmailHeaderField*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EmailHeaders?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EmailBody?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EmailMessage?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HashData*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Signature*</td>
<td>3.18.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RecordData</td>
<td>restriction?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>observable-id?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DateTime?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description_ML*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RecordPattern*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RecordItem*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FileData*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>WindowsRegistryKeysModified*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CertificateData*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AdditionalData*</td>
<td>3.18.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>-----------</td>
<td>---------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>WindowsRegistryKeysModified</td>
<td>observable-id?</td>
<td>Key+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key</td>
<td>registryaction?</td>
<td>ext-registryaction?</td>
<td>observable-id?</td>
<td>KeyName</td>
<td>KeyValue?</td>
</tr>
<tr>
<td>Certificate</td>
<td>observable-id?</td>
<td>X509Data</td>
<td>Description*</td>
<td>Description_ML*</td>
<td></td>
</tr>
<tr>
<td>HashData</td>
<td>scope</td>
<td>HashTargetID?</td>
<td>Hash*</td>
<td>FuzzyHash*</td>
<td></td>
</tr>
<tr>
<td>Hash</td>
<td>DigestMethod</td>
<td>DigestValue</td>
<td>CanonicalizationMethod?</td>
<td>Application?</td>
<td>3.23.1</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------</td>
<td>-------------</td>
<td>-------------------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>FuzzyHash</td>
<td>FuzzyHashValue+</td>
<td>Application?</td>
<td>AdditionalData*</td>
<td></td>
<td>3.23.2</td>
</tr>
<tr>
<td>Indicator</td>
<td>restriction?</td>
<td>ext-restriction?</td>
<td>IndicatorID</td>
<td>IndicatorID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description*</td>
<td>Description_ML*</td>
<td>StartTime?</td>
<td>EndTime?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidence?</td>
<td>Contact*</td>
<td>Observable?</td>
<td>uid-ref?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ext-restriction?</td>
<td>IndicatorExpression?</td>
<td>IndicatorReference?</td>
<td>NodeRole*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IndicatorReference*</td>
<td>AttackPhase*</td>
<td>Reference*</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AdditionalData*</td>
<td></td>
<td></td>
<td>3.24</td>
<td></td>
</tr>
<tr>
<td>IndicatorID</td>
<td>id</td>
<td>name</td>
<td>version</td>
<td>3.24.1</td>
<td></td>
</tr>
<tr>
<td>AlternativeIndicatorID</td>
<td>restriction?</td>
<td>ext-restriction?</td>
<td>IndicatorReference+</td>
<td>3.24.2</td>
<td></td>
</tr>
<tr>
<td>Observable</td>
<td>restriction?</td>
<td>ext-restriction?</td>
<td>System?</td>
<td>Address?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DomainData?</td>
<td>Service?</td>
<td>EmailData?</td>
<td>WindowsRegistryKeysModified?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RecordData?</td>
<td>CertificateData?</td>
<td>RegistryHandle?</td>
<td>RecordData?</td>
<td></td>
</tr>
</tbody>
</table>
3.2. Mapping between JSON and XML IODEF

- This document treats attributes and elements of each class defined in [RFC7970] equally and is agnostic on the order of their appearances.

- Flow class is deleted, and classes with its instances now directly have instances of EventData class that used to belong to the Flow classs.

o ApplicationHeader class is deleted, and classes with its instances now directly have instances of ApplicationHeaderField class that used to belong to the ApplicationHeader class.

o SignatureData class is deleted, and classes with its instances now directly have instance of Signature class that used to belong to the SignatureData class.

o IndicatorData class is deleted, and classes with its instances now directly have the instances of Indicator class that used to belong to the IndicatorData class.

o ObservableReference class is deleted, and classes with its instances now directly have uid-ref as an element.

o Record class is replaced by RecordData class, and RecordData class is renamed to Record class.

o Record class is deleted, and classes with its instances now directly have the instances of RecordData class that used to belong to the Record class.

o The elements of ML_STRING type are prepared as two separate elements: one of STRING type and another of ML_STRING type, in order to maintain the simplicity of IODEF documents when writing with only STRING type characters.

4. Examples

This section provides example of IODEF documents. These examples do not represent the full capabilities of the data model or the only way to encode particular information.

4.1. Minimal Example

A document containing only the mandatory elements and attributes.
4.2. Indicators from a Campaign

An example of C2 domains from a given campaign.

{  
  "version": "2.0",
  "lang": "en",
  "Incidents": [
    {  
      "purpose": "watch",
      "restriction": "green",
      "IncidentID": {
        "id": "897923",
        "name": "csirt.example.com"
      },
      "RelatedActivity": [
        {  
          "ThreatActor": [
            {  
              "ThreatActorID": "TA-12-AGGRESSIVE-BUTTERFLY",
              "Description": "Aggressive Butterfly"
            }
          ],
          "Campaign": [
            {  
              "CampaignID": "C-2015-59405",
              "Description": "Orange Giraffe"
            }
          ]
        }
      ]
    }
  ]
}
"GenerationTime": "2015-10-02T11:18:00-05:00",
"Description": 
"Summarizes the Indicators of Compromise for the Orange Giraffe campaign
of the Aggressive Butterfly crime gang."
],
"Assessment": [
{
"BusinessImpact": {
"type": "breach-proprietary"
}
},
"Contacts": [
{
"type": "organization",
"role": "creator",
"ContactName": "CSIRT for example.com",
"Email": {
"emailTo": "contact@csirt.example.com"
}
}
]
],
"IndicatorList": [
{
"IndicatorID": {
"id": "G90823490",
"name": "csirt.example.com",
"version": "1"
},
"Description": "C2 domains",
"StartTime": "2014-12-02T11:18:00-05:00",
"Observable": {
"BulkObservable": {
"type": "fqdn"
},
"BulkObservableList": [
"kj290023j09r34.example.com",
"09ijk23jffj0k8.example.net",
"klknjwfiowjefr923.example.org",
"oimireik79msd.example.org"
]
}
}
]
5. The IODEF Data Model (CDDL)

start = iodef

;;; iodef.json: IODEF-Document

iodef = {
  version: text
  ? lang: lang
  ? format-id: text
  ? private-enum-name: text
  ? private-enum-id: text
  Incident: [+ Incident]
  ? AdditionalData: [+ ExtensionType]
}

duration = "second" / "minute" / "hour" / "day" / "month" / "quarter" / "year" / "ext-value"
lang = "en" / "jp"
restriction = "public" / "partner" / "need-to-know" / "private" / "default" / "white" / "green" / "amber" / "red" / "ext-value"
DATETIME = text
URLtype = text
IDtype = text

action = "nothing" / "contact-source-site" / "contact-target-site" / "contact-sender" / "investigate" / "block-host" / "block-network" / "block-port" / "rate-limit-host" / "rate-limit-network" / "rate-limit-port" / "redirect-traffic" / "honeypot" / "upgrade-software" / "rebuild-asset" / "harden-asset" / "remediate-other" / "status-triage" / "status-new-info" / "watch-and-report" / "training" / "defined-coa" / "other" / "ext-value"

ExtensionType = {
  ? Name: text
  ? dtype: "boolean" / "byte" / "bytes" / "character" / "date-time" / "ntpstamp" / "integer" / "portlist" / "real" / "string" / "file" / "path" / "frame" / "packet" / "ipv4-packet" / "ipv6-packet" / "url" / "csv" / "winreg" / "xml" / "ext-value"
  ? ext-dtype: text
  ? meaning: text
  ? formatid: text
  ? restriction: restriction
}
SoftwareType = {
    ? SoftwareReference: SoftwareReference
    ? URL: URLtype
    ? Description: text
}

SoftwareReference = {
    ? value: text
    spec-name: "custom" / "cpe" / "swid" / "ext-value"
    ? ext-spec-name: text
    ? dtype: "bytes" / "integer" / "real" / "string" / "xml" / "ext-value"
    ? ext-dtype: text
}

Incident = {
    ? purpose: "traceback" / "mitigation" / "reporting" / "watch" / "other" / "ext-value"
    ? ext-purpose: text
    ? status: "new" / "in-progress" / "forwarded" / "resolved" / "future" / "ext-value"
    ? ext-status: text
    ? lang: lang
    ? restriction: restriction
    ? ext-restriction: text
    ? observable-id: IDtype
    IncidentID: IncidentID
    ? AlternativeID: AlternativeID
    ? RelatedActivity: [+ RelatedActivity]
    ? DetectTime: text
    ? StartTime: text
    ? EndTime: text
    ? RecoveryTime: text
    ? ReportTime: text
    GenerationTime: text
    ? Description: [+ text]
    ? Description_ML: [+ text]
    ? Discovery: [+ Discovery]
    ? Assessment: [+ Assessment]
    ? Method: [+ Method]
    Contact: [+ Contact]
    ? EventData: [+ EventData]
    ? Indicator: [+ Indicator]
    ? History: History
    ? AdditionalData: [+ ExtensionType]
IncidentID = {
  id: text
  name: text
  ? instance: text
  ? restriction: restriction
  ? ext-restriction: text
}

AlternativeID = {
  ? restriction: restriction
  ? ext-restriction: text
  IncidentID: [+ IncidentID]
}

RelatedActivity = {
  ? restriction: restriction
  ? ext-restriction: text
  ? IncidentID: [+ IncidentID]
  ? URL: [+ URLType]
  ? ThreatActor: [+ ThreatActor]
  ? Campaign: [+ Campaign]
  ? IndicatorID: [+ IndicatorID]
  ? Confidence: Confidence
  ? Description: [+ text]
  ? AdditionalData: [+ ExtensionType]
}

ThreatActor = {
  ? restriction: restriction
  ? ext-restriction: text
  ? ThreatActorID: [+ text]
  ? URL: [+ URLType]
  ? Description: [+ text]
  ? Description_ML: [+ text]
  ? AdditionalData: [+ ExtensionType]
}

Campaign = {
  ? restriction: restriction
  ? ext-restriction: text
  ? CampaignID: [+ text]
  ? URL: [+ URLType]
  ? Description: [+ text]
  ? Description_ML: [+ text]
  ? AdditionalData: [+ ExtensionType]
}
Contact = {
  role: "creator" / "reporter" / "admin" / "tech" / "provider" / "user" / "billing" / "legal" / "irt" / "abuse" / "cc" / "cc-irt" / "leo" / "vendor" / "vendor-support" / "victim" / "victim-notified" / "ext-value"
  ? ext-role: text
  type: "person" / "organization" / "ext-value"
  ? ext-type: text
  ? restriction: restriction
  ? ext-restriction: text
  ? ContactName: [+ text]
  ? ContactName_ML: [+ text]
  ? ContactTitle: [+ text]
  ? ContactTitle_ML: [+ text]
  ? Description: [+ text]
  ? Description_ML: [+ text]
  ? RegistryHandle: [+ RegistryHandle]
  ? PostalAddress: [+ PostalAddress]
  ? Email: [+ Email]
  ? Telephone: [+ Telephone]
  ? Timezone: text
  ? Contact: [+ Contact]
  ? AdditionalData: [+ ExtensionType]
}

RegistryHandle = {
  handle: text
  registry: "internic" / "apnic" / "arin" / "lacnic" / "ripe" / "afrinic" / "local" / "ext-value"
  ? ext-registry: text
}

PostalAddress = {
  ? type: text
  ? ext-type: text
  PAddress: text
  ? Description: [+ text]
  ? Description_ML: [+ text]
}

Email = {
  ? type: "direct" / "hotline" / "ext-value"
  ? ext-type: text
  EmailTo: text
  ? Description: [+ text]
  ? Description_ML: [+ text]
}

Telephone = {
? type: "wired" / "mobile" / "fax" / "hotline" / "ext-value"
? ext-type: text
TelephoneNumber: text
? Description: [+ text]
? Description_ML: [+ text]
}

Discovery = {
? source: "nidps" / "hips" / "siem" / "av" / "third-party-monitoring" / "incident" / "os-log" / "application-log" / "device-log" / "network-flow" / "passive-dns" / "investigation" / "audit" / "international-notification" / "external-notification" / "leo" / "partner" / "actor" / "unknown" / "ext-value"
? ext-source: text
? restriction: restriction
? ext-restriction: text
? Description: [+ text]
? Description_ML: [+ text]
? Contact: [+ Contact]
? DetectionPattern: [+ DetectionPattern]
}

DetectionPattern = {
? restriction: restriction
? ext-restriction: text
? observable-id: IDtype
Application: SoftwareType
? Description: [+ text]
? Description_ML: [+ text]
? DetectionConfiguration: [+ text]
}

Method = {
? restriction: restriction
? ext-restriction: text
? Reference: [+ Reference]
? Description: [+ text]
? Description_ML: [+ text]
? AttackPattern: [+ StructuredInformation]
? Vulnerability: [+ StructuredInformation]
? Weakness: [+ StructuredInformation]
? AdditionalData: [+ ExtensionType]
}

StructuredInformation = {
specID: text
? ext-specID: text
? contentID: text
? RawData: any
? URL: URLtype
}

Reference = {
? observable-id: IDtype
? ReferenceName: ReferenceName
? URL: [+ URLtype]
? Description: [+ text]
? Description_ML: [+ text]
}

ReferenceName = {
  specIndex: int
  ID: text
}

Assessment = {
? occurrence: "actual" / "potential"
? restriction: restriction
? ext-restriction: text
? observable-id: IDtype
? IncidentCategory: [+ text]
? SystemImpact: [+ SystemImpact]
? BusinessImpact: [+ BusinessImpact]
? TimeImpact: [+ TimeImpact]
? MonetaryImpact: [+ MonetaryImpact]
? IntendedImpact: [+ BusinessImpact]
? Counter: [+ Counter]
? MitigatingFactor: [+ text]
? MitigatingFactor_ML: [+ text]
? Cause: [+ text]
? Cause_ML: [+ text]
? Confidence: Confidence
? AdditionalData: [+ ExtensionType]
}

SystemImpact = {
? severity: "low" / "medium" / "high"
? completion: "failed" / "succeeded"
type: "takeover-account" / "takeover-service" / "takeover-system" / 
"cps-manipulation" / "cps-damage" / "availability-data" / 
"availability-account" / "availability-service" / 
"availability-system" / "damaged-system" / "damaged-data" / 
"breach-proprietary" / "breach-privacy" / "breach-credential" / 
"breach-configuration" / "integrity-data" / 
"integrity-configuration" / "integrity-hardware" /
"traffic-redirection" / "monitoring-traffic" / "monitoring-host" / "policy" / "unknown" / "ext-value"

? ext-type: text
? Description: [+ text]
? Description_ML: [+ text]
}

BusinessImpact = {
? severity: "none" / "low" / "medium" / "high" / "unknown" / "ext-value"
? ext-severity: text
type: "breach-proprietary" / "breach-privacy" / "breach-credential" / "loss-of-integrity" / "loss-of-service" / "theft-financial" / "theft-service" / "degraded-reputation" / "asset-damage" / "asset-manipulation" / "legal" / "extortion" / "unknown" / "ext-value"
? ext-type: text
? Description: [+ text]
? Description_ML: [+ text]
}

TimeImpact = {
value: int
? severity: "low" / "medium" / "high"
metric: "labor" / "elapsed" / "downtime" / "ext-value"
? ext-metric: text
? duration: duration
? ext-duration: text
}

MonetaryImpact = {
value: int
? severity: "low" / "medium" / "high"
? currency: text
}

Confidence = {
value: int
rating: "low" / "medium" / "high" / "numeric" / "unknown" / "ext-value"
? ext-rating: text
}

History = {
? restriction: restriction
? ext-restriction: text
HistoryItem: [+ HistoryItem]
}

HistoryItem = {

action: action
? ext-action: text
? restriction: restriction
? ext-restriction: text
? observable-id: IDtype
DateTime: DATETIME
? IncidentID: IncidentID
? Contact: Contact
? Description: [+ text]
? Description_ML: [+ text]
? DefinedCOA: [+ text]
? AdditionalData: [+ ExtensionType]
}

EventData = {
? restriction: restriction
? ext-restriction: text
? observable-id: IDtype
? Description: [+ text]
? Description_ML: [+ text]
? DetectTime: DATETIME
? StartTime: DATETIME
? EndTime: DATETIME
? RecoveryTime: DATETIME
? ReportTime: DATETIME
? Contact: [+ Contact]
? Discovery: [+ Discovery]
? Assessment: Assessment
? Method: [+ Method]
? System: [+ System]
? Expectation: [+ Expectation]
? RecordData: [+ RecordData]
? EventData: [+ EventData]
? AdditionalData: [+ ExtensionType]
}

Expectation = {
? action: action
? ext-action: text
? severity: "low" / "medium" / "high"
? restriction: restriction
? ext-restriction: text
? observable-id: IDtype
? Description: [+ text]
? Description_ML: [+ text]
? DefinedCOA: [+ text]
? StartTime: DATETIME
? EndTime: DATETIME
System = {
  ? category: "source" / "target" / "intermediate" / "sensor" / "infrastructure" / "ext-value"
  ? ext-category: text
  ? interface: text
  ? spoofed: "unknown" / "yes" / "no"
  ? virtual: "yes" / "no" / "unknown"
  ? ownership: "organization" / "personal" / "partner" / "customer" / "no-relationship" / "unknown" / "ext-value"
  ? ext-ownership: text
  ? restriction: restriction
  ? ext-restriction: text
  ? observable-id: IDtype

Node: Node
  ? NodeRole: [+ NodeRole]
  ? Service: [+ Service]
  ? OperatingSystem: [+ SoftwareType]
  ? Counter: [+ Counter]
  ? AssetID: [+ text]
  ? Description: [+ text]
  ? Description_ML: [+ text]
  ? AdditionalData: [+ ExtensionType]
}

Node = {
  ? DomainData: [+ DomainData]
  ? Address: [+ Address]
  ? PostalAddress: PostalAddress
  ? Location: [+ text]
  ? Location_ML: [+ text]
  ? Counter: [+ Counter]
}

Address = {
  value: text
  category: "asn" / "atm" / "e-mail" / "ipv4-addr" / "ipv4-net" / "ipv4-net-masked" / "ipv4-net-mask" / "ipv6-addr" / "ipv6-net" / "ipv6-net-masked" / "mac" / "site-url" / "ext-value"
  ? ext-category: text
  ? vlan-name: text
  ? vlan-num: int
  ? observable-id: IDtype
}
NodeRole = {
  ? ext-category: text
  ? Description: [+ text]
  ? Description_ML: [+ text]
}

Counter = {
  value: text
  type: "count" / "peak" / "average" / "ext-value"
  ? ext-type: text
  unit: "byte" / "mbit" / "packet" / "flow" / "session" / "alert" / "message" / "event" / "host" / "site" / "organization" / "ext-value"
  ? ext-unit: text
  ? meaning: text
  ? meaning_ML: text
  ? duration: duration
  ? ext-duration: text
}

DomainData = {
  system-status: "spoofed" / "fraudulent" / "innocent-hacked" / "innocent-hijacked" / "unknown" / "ext-value"
  ? ext-system-status: text
  domain-status: "reservedDelegation" / "assignedAndActive" / "assignedAndInactive" / "assignedAndOnHold" / "revoked" / "transferPending" / "registryLock" / "registrarLock" / "other" / "unknown" / "ext-value"
  ? ext-domain-status: text
  ? observable-id: IDtype
  Name: text
  ? DateDomainWasChecked: DATETIME
  ? RegistrationDate: DATETIME
}
? ExpirationDate: DATETIME
? RelatedDNS: [+ ExtensionType]
? NameServers: [+ NameServers]
? DomainContacts: DomainContacts

NameServers = {
    Server: text
    ? Address: [+ Address]
}

DomainContacts = {
    ? SameDomainContact: text
    Contact: [+ Contact]
}

Service = {
    ? ip-protocol: int
    ? observable-id: IDtype
    ? ServiceName: ServiceName
    ? Port: int
    ? Portlist: text
    ? ProtoCode: int
    ? ProtoType: int
    ? ProtoField: int
    ? ApplicationHeaderField: [+ ExtensionType]
    ? EmailData: EmailData
    ? Application: SoftwareType
}

ServiceName = {
    ? IANAService: text
    ? URL: [+ URLtype]
    ? Description: [+ text]
    ? Description_ML: [+ text]
}

EmailData = {
    ? observable-id: IDtype
    ? EmailTo: [+ text]
    ? EmailFrom: text
    ? EmailSubject: text
    ? EmailX-Mailer: text
    ? EmailHeaderField: [+ ExtensionType]
    ? EmailHeaders: text
    ? EmailBody: text
    ? EmailMessage: text
    ? HashData: [+ HashData]
RecordData = {
    ? restriction: restriction
    ? ext-restriction: text
    ? observable-id: IDtype
    ? DateTime: DATETIME
    ? Description: [+ text]
    ? Description_ML: [+ text]
    ? Application: SoftwareType
    ? RecordPattern: [+ RecordPattern]
    ? RecordItem: [+ ExtensionType]
    ? URL: [+ URLtype]
    ? FileData: [+ FileData]
    ? WindowsRegistryKeysModified: [+ WindowsRegistryKeysModified]
    ? CertificateData: [+ CertificateData]
    ? AdditionalData: [+ ExtensionType]
}

RecordPattern = {
    value: text
    type: "regex" / "binary" / "xpath" / "ext-value"
    ? ext-type: text
    ? offset: int
    ? offsetunit: "line" / "byte" / "ext-value"
    ? ext-offsetunit: text
    ? instance: int
}

WindowsRegistryKeysModified = {
    ? observable-id: IDtype
    Key: [+ Key]
}

Key = {
    ? registryaction: "add-key" / "add-value" / "delete-key" / "delete-value" / "modify-key" / "modify-value" / "ext-value"
    ? ext-registryaction: text
    ? observable-id: IDtype
    KeyName: text
    ? KeyValue: text
}

CertificateData = {
    ? restriction: restriction
    ? ext-restriction: text
}
Certificate = {
    ? observable-id: IDtype
    X509Data: text
    ? Description: [+ text]
    ? Description_ML: [+ text]
}

FileData = {
    ? restriction: restriction
    ? ext-restriction: text
    ? observable-id: IDtype
    File: [+ File]
}

File = {
    ? observable-id: IDtype
    ? FileName: text
    ? FileSize: int
    ? FileType: text
    ? URL: [+ URLtype]
    ? HashData: HashData
    ? Signature: [+ text]
    ? AssociatedSoftware: SoftwareType
    ? FileProperties: [+ ExtensionType]
}

HashData = {
    ? HashTargetID: text
    ? Hash: [+ Hash]
    ? FuzzyHash: [+ FuzzyHash]
}

Hash = {
    DigestMethod: text
    DigestValue: text
    ? CanonicalizationMethod: any
    ? Application: SoftwareType
}

FuzzyHash = {
    FuzzyHashValue: [+ ExtensionType]"}
Indicator = {
  ? restriction: restriction
  ? ext-restriction: text
  IndicatorID: IndicatorID
  ? AlternativeIndicatorID: [+ AlternativeIndicatorID]
  ? Description: [+ text]
  ? Description_ML: [+ text]
  ? StartTime: DATETIME
  ? EndTime: DATETIME
  ? Confidence: Confidence
  ? Contact: [+ Contact]
  ? Observable: Observable
  ? uid-ref: text
  ? IndicatorExpression: IndicatorExpression
  ? IndicatorReference: IndicatorReference
  ? NodeRole: [+ NodeRole]
  ? AttackPhase: [+ AttackPhase]
  ? Reference: [+ Reference]
  ? AdditionalData: [+ ExtensionType]
}

IndicatorID = {
  id: IDtype
  name: text
  version: text
}

AlternativeIndicatorID = {
  ? restriction: restriction
  ? ext-restriction: text
  IndicatorReference: [+ IndicatorReference]
}

Observable = {
  ? restriction: restriction
  ? ext-restriction: text
  ? System: System
  ? Address: Address
  ? DomainData: DomainData
  ? EmailData: EmailData
  ? Service: Service
  ? WindowsRegistryKeysModified: WindowsRegistryKeysModified
  ? FileData: FileData
  ? CertificateData: CertificateData
? RegistryHandle: RegistryHandle
? RecordData: RecordData
? EventData: EventData
? Incident: Incident
? Expectation: Expectation
? Reference: Reference
? Assessment: Assessment
? DetectionPattern: DetectionPattern
? HistoryItem: HistoryItem
? BulkObservable: BulkObservable
? AdditionalData: [+ ExtensionType]
}

BulkObservable = {
? type: "asn" / "atm" / "e-mail" / "ipv4-addr" / "ipv4-net" / "ipv4-net-mask" / "ipv6-addr" / "ipv6-net" / "ipv6-net-mask" / "mac" / "site-url" / "domain-name" / "domain-to-ipv4" / "domain-to-ipv6" / "domain-to-ipv4-timestamp" / "domain-to-ipv6-timestamp" / "ipv4-port" / "ipv6-port" / "windows-reg-key" / "file-hash" / "email-x-mailer" / "email-subject" / "http-user-agent" / "http-request-uri" / "mutex" / "file-path" / "user-name" / "ext-value"
? ext-type: text
? BulkObservableFormat: BulkObservableFormat
BulkObservableList: [+ text]
? AdditionalData: [+ ExtensionType]
}

BulkObservableFormat = {
? Hash: Hash
? AdditionalData: [+ ExtensionType]
}

IndicatorExpression = {
? operator: "not" / "and" / "or" / "xor"
? ext-operator: text
? IndicatorExpression: [+ IndicatorExpression]
? Observable: [+ Observable]
? uid-ref: [+ text]
? IndicatorReference: [+ IndicatorReference]
? Confidence: Confidence
? AdditionalData: [+ ExtensionType]
}

IndicatorReference = {
? uid-ref: text
? euid-ref: text
? version: text

AttackPhase = {
? AttackPhaseID: [+ text]
? URL: [+ URLtype]
? Description: [+ text]
? Description_ML: [+ text]
? AdditionalData: [+ ExtensionType]
}

Figure 2: Data Model in CDDL

6. Acknowledgements

We would like to thank Henk Birkholz and Carsten Bormann for their insightful comments on CDDL.

7. IANA Considerations

This document registers a JSON schema.

8. Security Considerations

This memo does not provide any further security considerations than the one described in [RFC7970].

9. Normative References

[jsonschema]
http://json-schema.org/


Appendix A. The IODEF Data Model (JSON Schema)

This section provides a JSON schema that defines the IODEF Data Model defined in this draft.

{"$schema": "http://json-schema.org/draft-04/schema#",

"definitions": {
  "action": {
    "enum": [
      "nothing",
      "contact-source-site",
      "contact-target-site",
      "contact-sender",
      "investigate",
      "block-host",
      "block-network",
      "block-port",
      "rate-limit-host",
      "rate-limit-network",
      "rate-limit-port",
      "redirect-traffic",
      "honeypot",
      "upgrade-software",
      "rebuild-asset",
      "harden-asset",
      "remediate-other",
      "status-triage",
      "status-new-info",
      "watch-and-report",
      "training",
      "defined-coa",
      "ext-value"
    ]
  },
  "duration": {
    "enum": [
      "second",
      "minute",
      "hour",
      "day",
      "month",
      "quarter",
      "year",
      "ext-value"
    ]
  },
  "lang": {
    "enum": [
      "en",
      "jp"
    ]
  },
  "purpose": {
    "enum": [
      "traceback",
      "mitigation",
      "reporting",
      "watch",
      "other",
      "ext-value"
    ]
  },
  "restriction": {
    "enum": [
      "public",
      "partner",
      "need-to-know",
      "private",
      "default",
      "white",
      "green",
      "amber",
      "red",
      "ext-value"
    ]
  },
  "status": {
    "enum": [
      "new",
      "in-progress",
      "forwarded",
      "resolved",
      "future",
      "ext-value"
    ]
  },
  "DATETIME": {
    "type": "string"
  },
  "PORTLIST": {
    "type": "string"
  },
  "URLtype": {
    "type": "string"
  },
  "IDtype": {
    "type": "string"
  },
  "ExtensionType": {
    "type": "object",
    "properties": {
      "name": {
        "type": "string"
      },
      "dtype": {
        "enum": [
          "boolean",
          "byte",
          "bytes",
          "character",
          "date-time",
          "ntpstamp",
          "integer",
          "portlist",
          "real",
          "string",
          "file",
          "path",
          "frame",
          "packet",
          "ipv4-packet",
          "ipv6-packet",
          "url",
          "csv",
          "winreg",
          "xml",
          "ext-value"
        ]
      },
      "ext-dtype": {
        "type": "string"
      },
      "meaning": {
        "type": "string"
      },
      "formatid": {
        "type": "string"
      },
      "restriction": {
        "$ref": "#/definitions/restriction"
      },
      "ext-restriction": {
        "type": "string"
      },
      "observable-id": {
        "$ref": "#/definitions/IDtype"
      }
    }
  },
  "ExtensionTypeList": {
    "type": "array",
    "items": {
      "$ref": "#/definitions/ExtensionType"
    }
  },
  "SoftwareType": {
    "type": "object",
    "properties": {
      "SoftwareReference": {
        "$ref": "#/definitions/SoftwareReference"
      },
      "URL": {
        "$ref": "#/definitions/URLtype"
      },
      "Description": {
        "type": "array",
        "items": {
          "type": "string"
        }
      }
    }
  },
  "additionalProperties": false
}
"properties": {
    "value": {
        "type": "string"
    },
    "spec-name": {
        "type": "string"
    },
    "ext-spec-name": {
        "type": "string"
    },
    "dtype": {
        "type": "string"
    },
    "ext-dtype": {
        "type": "string"
    },
    "required": ["spec-name"],
    "additionalProperties": false
},
"StructuredInfo": {
    "type": "object",
    "properties": {
        "specID": {
            "type": "string"
        },
        "ext-specID": {
            "type": "string"
        },
        "contentID": {
            "type": "string"
        },
        "RawData": {
            "type": "string"
        },
        "URL": {
            "$ref": "#/definitions/URLtype"
        },
        "required": ["specID"],
        "additionalProperties": false
    }
},
"Incident": {
    "title": "Incident",
    "description": "JSON schema for Incident class",
    "type": "object",
    "properties": {
        "purpose": {
            "$ref": "#/definitions/purpose"
        },
        "ext-purpose": {
            "type": "string"
        },
        "status": {
            "$ref": "#/definitions/status"
        },
        "ext-status": {
            "type": "string"
        },
        "lang": {
            "$ref": "#/definitions/lang"
        },
        "restriction": {
            "$ref": "#/definitions/restriction"
        },
        "ext-restriction": {
            "type": "string"
        },
        "observable-id": {
            "$ref": "#/definitions/IDtype"
        },
        "IncidentID": {
            "$ref": "#/definitions/IncidentID"
        },
        "AlternativeID": {
            "$ref": "#/definitions/AlternativeID"
        },
        "RelatedActivity": {
            "type": "array",
            "items": {
                "$ref": "#/definitions/RelatedActivity"
            }
        },
        "DetectTime": {
            "type": "string"
        },
        "StartTime": {
            "type": "string"
        },
        "EndTime": {
            "type": "string"
        },
        "RecoveryTime": {
            "type": "string"
        },
        "ReportTime": {
            "type": "string"
        },
        "GenerationTime": {
            "type": "string"
        },
        "Description": {
            "type": "array",
            "items": {
                "type": "string"
            }
        },
        "Discovery": {
            "type": "array",
            "items": {
                "$ref": "#/definitions/Discovery"
            }
        },
        "Assessment": {
            "type": "array",
            "items": {
                "$ref": "#/definitions/Assessment"
            }
        },
        "Methods": {
            "$ref": "#/definitions/Methods"
        }
    }
}
"type": "array","items": {"$ref": "/definitions/Method"}},
"Contacts": {
  "type": "array","items": {"$ref": "/definitions/Contact"}},
"EventData": {
  "type": "array","items": {"$ref": "/definitions/EventData"}},
"IndicatorList": {
  "type": "array","items": {"$ref": "/definitions/Indicator"}},
"History": {"$ref": "/definitions/History"},
"AdditionalData": {"$ref": "/definitions/ExtensionTypeList"},
"required": ["IncidentID","GenerationTime","Contacts","purpose"],
"additionalProperties": false},
"IncidentID": {
  "title": "IncidentID",
  "description": "JSON schema for IncidentID class",
  "type": "object",
  "properties": {
    "id": {"type": "string"},
    "name": {"type": "string"},
    "instance": {"type": "string"},
    "restriction": {"$ref": "/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "required": ["name"],
    "additionalProperties": false},
"AlternativeID": {
  "title": "AlternativeID",
  "description": "JSON schema for AlternativeID class",
  "type": "object",
  "properties": {
    "IncidentID": {
      "type": "array","items":{"$ref": "/definitions/IncidentID"}},
    "restriction": {"$ref": "/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "required": ["IncidentID"],
    "additionalProperties": false},
"RelatedActivity": {
  "properties": {
    "restriction": {"$ref": "/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "IncidentID": {
      "type": "array","items":{"$ref": "/definitions/IncidentID"}},
    "URL": {
      "type": "array","items":{"$ref": "/definitions/URLtype"}},
    "ThreatActor": {
      "type": "array","items":{"$ref": "/definitions/ThreatActor"}},
    "Campaign": {
      "type": "array","items":{"$ref": "/definitions/Campaign"}},
    "IndicatorID": {
      "type": "array","items":{"$ref": "/definitions/IndicatorID"}},
"Confidence": {"$ref": "/#definitions/Confidence"},
"Description": { "type": "array", "items": { "type": "string"} },
"AdditionalData": { "$ref": "/#definitions/ExtensionTypeList" },
"additionalProperties": false},
"ThreatActor": { 
"properties": { 
"restriction": {"$ref": "/#definitions/restriction"},
"ext-restriction": {"type": "string"},
"ThreatActorID": {"type": "array", "items": {"type": "string"}},
"Description": {"type": "array", "items": {"type": "string"}},
"URL": {"type": "array", "items": "{ "$ref": "/#definitions/URLtype" }"},
"AdditionalData": { "$ref": "/#definitions/ExtensionTypeList" },
"additionalProperties": false},
"Campaign": { 
"properties": { 
"restriction": {"$ref": "/#definitions/restriction"},
"ext-restriction": {"type": "string"},
"CampaignID": {"type": "array", "items": {"type": "string"}},
"[URL]: {"type": "array", "items": "{ "$ref": "/#definitions/URLtype" }"},
"Description": {"type": "array", "items": {"type": "string"}},
"AdditionalData": { "$ref": "/#definitions/ExtensionTypeList" },
"additionalProperties": false},
"Contact": { 
"type": "object",
"properties": { 
"role": { 
"ext-role": {"type": "string"},
"type": {"enum": ["person", "organization", "ext-value"]},
"ext-type": {"type": "string"},
"restriction": {"$ref": "/#definitions/restriction"},
"ext-restriction": {"type": "string"},
"ContactName": {"type": "array", "items": {"type": "string"}},
"ContactTitle": {"type": "array", "items": {"type": "string"}},
"Description": {"type": "array", "items": {"type": "string"}},
"RegistryHandle": { 
"type": "array", "items": "{ "$ref": "/#definitions/RegistryHandle" }"},
"PostalAddress": { 
"type": "array", "items": "{ "$ref": "/#definitions/PostalAddress" }"},
"Email": {"type": "array", "items": {"$ref": "/#definitions/Email"}},
"Telephone": { 
"type": "array", "items": "{ "$ref": "/#definitions/Telephone" }"},
"Timezone": {"type": "string"},
"Contact": { 
"type": "array", "items": "{ "$ref": "/#definitions/Contact" }"},
"AdditionalData": { "$ref": "/#definitions/ExtensionTypeList" },
"required": ["role","type"],
"additionalProperties": false},
"RegistryHandle": {
  "type": "object",
  "properties": {
    "handle": {"type": "string"},
    "registry": {
      "enum": ["internic","apnic","arin","lacnic","ripe","afrinic",
               "local","ext-value"],
      "ext-registry": {"type": "string"},
      "required": ["registry"],
      "additionalProperties": false},
  "PostalAddress": {
    "type": "object",
    "properties": {
      "type": {"type": "string"},
      "PAddress": {"type": "string"},
      "Description": {"type": "array", "items": {"type": "string"}}},
      "required": ["PAddress"],
      "additionalProperties": false},
  "Email": {
    "type": "object",
    "properties": {
      "type": {
        "enum": ["direct","hotline","ext-value"],
        "ext-type": {"type": "string"},
        "EmailTo": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}}},
        "required": ["EmailTo"],
        "additionalProperties": false},
  "Telephone": {
    "type": "object",
    "properties": {
      "type": {
        "enum": ["wired","mobile","fax","hotline","ext-value"],
        "ext-type": {"type": "string"},
        "TelephoneNumber": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}}},
        "required": ["TelephoneNumber"],
        "additionalProperties": false},
  "Discovery": {
    "type": "object",
    "properties": {
      "source": {
        "enum": ["nidps","hips","siem","av","third-party-monitoring",
                  "incident","os-log","application-log","device-log",
                  "network-flow","passive-dns","investigation","audit"],
        "required": ["source"],
        "additionalProperties": false}.
"internal-notification","external-notification","leo",
"partner","actor","unknown","ext-value"},
"ext-source": {"type": "string"},
"restriction": {"$ref": "/definitions/restriction"},
"ext-restriction": {"type": "string"},
"Description": {"type": "array", "items": {"type": "string"}},
"Contact": {
  "type": "array", "items": {"$ref": "/definitions/Contact"}},
"DetectionPattern": {
  "type": "array", "items": {"$ref": "/definitions/DetectionPattern"}},
"required": [],
"additionalProperties": false},
"DetectionPattern": {
  "type": "object",
  "properties": {
    "restriction": {"$ref": "/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "observable-id": {"$ref": "/definitions/IDtype"},
    "Application": {"$ref": "/definitions/SoftwareType"},
    "Description": {"type": "array", "items": {"type": "string"}},
    "DetectionConfiguration": {
      "type": "array", "items": {"type": "string"}},
    "required": [],
    "additionalProperties": false},
"Method": {
  "type": "object",
  "properties": {
    "restriction": {"$ref": "/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "References": {
      "type": "array", "items": {"$ref": "/definitions/Reference"}},
    "Description": {"type": "array", "items": {"type": "string"}},
    "AttackPattern": {
      "type": "array", "items": {"$ref": "/definitions/StructuredInfo"}},
    "Vulnerability": {
      "type": "array", "items": {"$ref": "/definitions/StructuredInfo"}},
    "Weakness": {
      "type": "array", "items": {"$ref": "/definitions/StructuredInfo"}},
    "AdditionalData": {"$ref": "/definitions/ExtensionTypeList"},
    "required": [],
    "additionalProperties": false},
"Reference": {
  "type": "object",
  "properties": {
    "observable-id": {"$ref": "/definitions/IDtype"},
    "ReferenceName": {"type": "string"},
    "URL": {"type": "array", "items": {"$ref": "/definitions/URLtype"}},
"Description": {"type": "array", "items": {"type": "string"}},
"required": [],
"additionalProperties": false},
"Assessment": {
  "type": "object",
  "properties": {
    "occurrence": {"enum": ["actual", "potential"]},
    "restriction": {"$ref": "/#/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "observable-id": {"$ref": "/#/definitions/IDtype"},
    "IncidentCategory": {"type": "array", "items": {"type": "string"}},
    "SystemImpact": {
      "type": "array", "items": {"$ref": "/#/definitions/SystemImpact"}},
    "BusinessImpact": {
      "type": "array", "items": {"$ref": "/#/definitions/BusinessImpact"}},
    "TimeImpact": {
      "type": "array", "items": {"$ref": "/#/definitions/TimeImpact"}},
    "MonetaryImpact": {
      "type": "array", "items": {"$ref": "/#/definitions/MonetaryImpact"}},
    "IntendedImpact": {
      "type": "array", "items": {"$ref": "/#/definitions/BusinessImpact"}},
    "Counter": {
      "type": "array", "items": {"$ref": "/#/definitions/Counter"}},
    "MitigatingFactor": {
      "type": "array", "items": {"$type": "string"}},
    "Cause": {
      "type": "array", "items": {"$type": "string"}},
    "Confidence": {"$ref": "/#/definitions/Confidence"},
    "AdditionalData": {"$ref": "/#/definitions/ExtensionTypeList"},
  "required": [],
  "additionalProperties": false},
"SystemImpact": {
  "type": "object",
  "properties": {
    "severity": {
      "enum": ["low", "medium", "high"],
    "completion": {"enum": ["failed", "succeeded"]},
    "type": {
    "ext-type": {"type": "string"},
    "Description": {"type": "array", "items": {"type": "string"}},
"required": ["type"],
"additionalProperties": false,
"BusinessImpact": {
  "type": "object",
  "properties": {
    "severity": {
      "enum": ["none", "low", "medium", "high", "unknown", "ext-value"],
      "ext-severity": {"type": "string"},
      "type": {
        "enum": ["breach-proprietary", "breach-privacy", "breach-credential",
                 "loss-of-integrity", "loss-of-service", "theft-financial",
                 "theft-service", "degraded-reputation", "asset-damage",
                 "asset-manipulation", "legal", "extortion", "unknown",
                 "ext-value"],
        "ext-type": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}}
      },
      "required": ["type"],
      "additionalProperties": false
    },
    "TimeImpact": {
      "type": "object",
      "properties": {
        "value": {"type": "number"},
        "severity": {"enum": ["low", "medium", "high"]},
        "metric": {"enum": ["labor", "elapsed", "downtime", "ext-value"],
                   "ext-metric": {"type": "string"},
                   "duration": {"$ref": "/definitions/duration"},
                   "ext-duration": {"type": "string"}
                 },
        "required": ["metric"],
        "additionalProperties": false
      },
      "MonetaryImpact": {
        "type": "object",
        "properties": {
          "value": {"type": "number"},
          "severity": {"enum": ["low", "medium", "high"]},
          "currency": {"type": "string"},
          "required": [],
          "additionalProperties": false
        },
        "Confidence": {
          "type": "object",
          "properties": {
            "value": {"type": "number"},
            "rating": {"enum": ["low", "medium", "high", "numeric", "unknown", "ext-value"],
                       "ext-rating": {"type": "string"},
                       "required": ["rating"],
                       "additionalProperties": false
          },
          "History": {
            "type": "object"}
"properties": {
    "restriction": {"$ref": "#/definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "HistoryItem": {
        "type": "array","items": {"$ref": "#/definitions/HistoryItem"}},
    "required": ["HistoryItem"],
    "additionalProperties": false},
"HistoryItem": {
    "type": "object",
    "properties": {
        "action": {"$ref": "#/definitions/action"},
        "ext-action": {"type": "string"},
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "DateTime": {"$ref": "#/definitions/DATETIME"},
        "IncidentID": {"$ref": "#/definitions/IncidentID"},
        "Contact": {"$ref": "#/definitions/Contact"},
        "Description": {"type": "array","items": {"type": "string"}},
        "DefinedCOA": {"type": "array","items": {"type": "string"}},
        "AdditionalData": {"$ref": "#/definitions/ExtensionTypeList"},
        "required": ["DateTime","action"],
        "additionalProperties": false},
"EventData": {
    "type": "object",
    "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Description": {"type": "array","items": {"type": "string"}},
        "DetectTime": {"type": "string"},
        "StartTime": {"type": "string"},
        "EndTime": {"type": "string"},
        "RecoveryTime": {"type": "string"},
        "ReportTime": {"type": "string"},
        "Contact": {
            "type": "array","items": {"$ref": "#/definitions/Contact"}}
        "Discovery": {
            "type": "array","items": {"$ref": "#/definitions/Discovery"}},
        "Assessment": {"$ref": "#/definitions/Assessment"},
        "Method": {
            "type": "array","items": {"$ref": "#/definitions/Method"}},
        "System": {
            "type": "array","items": {"$ref": "#/definitions/System"}},
        "Expectation": {
            "type": "array","items": {"$ref": "#/definitions/Expectation"}},
        "RecordData": {"type": "array",
            "items": {"$ref": "#/definitions/RecordData"}},
"EventData": {
    "type": "array","items": {"$ref": "/#definitions/EventData"}},
"AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"},
"required": [{"ReportTime"}],
"additionalProperties": false},

"Expectation": {
    "type": "object",
    "properties": {
        "action": {"$ref": "/#definitions/action"},
        "ext-action": {"type": "string"},
        "severity": {"enum": ["low","medium","high"]},
        "restriction": {"$ref": "/#definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "/#definitions/IDtype"},
        "Description": {"type": "array","items": {"type": "string"}},
        "DefinedCOA": {"type": "array","items": {"type": "string"}},
        "StartTime": {"type": "string"},
        "EndTime": {"type": "string"},
        "Contact": {"$ref": "/#definitions/Contact"},
        "required": [],
        "additionalProperties": false},

"System": {
    "type": "object",
    "properties": {
        "category": {
            "enum": ["source","target","intermediate","sensor","infrastructure","ext-value"]},
        "ext-category": {"type": "string"},
        "interface": {"type": "string"},
        "spoofed": {"enum": ["unknown","yes","no"]},
        "virtual": {"enum": ["yes","no","unknown"]},
        "ownership": {
            "enum":["organization","personal","partner","customer","no-relationship","unknown","ext-value"],
            "ext-ownership": {"type": "string"},
            "restriction": {"$ref": "/#definitions/restriction"},
            "ext-restriction": {"type": "string"},
            "observable-id": {"$ref": "/#definitions/IDtype"},
            "Node": {"$ref": "/#definitions/Node"},
            "NodeRole": {
                "type": "array","items": {"$ref": "/#definitions/NodeRole"}}},
        "Service": {
            "type": "array","items": {"$ref": "/#definitions/Service"}},
        "OperatingSystem": {
            "type": "array","items": {"$ref": "/#definitions/SoftwareType"}},
        "Counter": {
            "type": "array","items": {"$ref": "/#definitions/Counter"}},
        "AssetID": {"type": "array","items": {"type": "string"}},
"Description": {"type": "array","items": {"type": "string"}},
"AdditionalData": {"$ref": "#/definitions/ExtensionTypeList"},
"required": ["Node"],
"additionalProperties": false},
"Node": {
  "type": "object",
  "properties": {
    "DomainData": {
      "type": "array","items": {"$ref": "#/definitions/DomainData"},
    "Address": {
      "type": "array","items": {"$ref": "#/definitions/Address"},
    "PostalAddress": {"type": "string"},
    "Location": {"type": "array","items": {"type": "string"}},
    "Counter": {"type": "array",
      "items": {"$ref": "#/definitions/Counter"}}},
  "required": [],
  "additionalProperties": false},
  "Address": {
    "type": "object",
    "properties": {
      "value": {"type": "string"},
      "category": {
        "enum": ["asn","atm","e-mail","ipv4-addr","ipv4-net",
          "ipv4-net-masked","ipv4-net-mask","ipv6-addr","ipv6-net",
          "ipv6-net-masked","mac","site-url","ext-value"],
        "ext-category": {"type": "string"},
        "vlan-name": {"type": "string"},
        "vlan-num": {"type": "integer"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "required": ["category"],
        "additionalProperties": false},
  "NodeRole": {
    "type": "object",
    "properties": {
      "category": {
        "enum": ["client","client-enterprise","client-partner",
          "client-remote","client-kiosk","client-mobile",
          "server-internal","server-public","www","mail","webmail",
          "messaging","streaming","voice","file","ftp","p2p","name",
          "directory","credential","print","application","database",
          "backup","dhcp","assessment","source-control",
          "config-management","monitoring","infra","infra-firewall",
          "infra-router","infra-switch","camera","proxy",
          "remote-access","log","virtualization","pos","scada",
          "scada-supervisory","sinkhole","honeypot","anomalyzation",
          "c2-server","malware-distribution","drop-server",
          "hot-point","reflector","phishing-site",
          "spear-phishing-site","recruiting-site"],
        "required": ["category"],
        "additionalProperties": false},
  "required": [],
  "additionalProperties": false}},
"fraudulent-site","ext-value"],
  "ext-category": {"type": "string"},
  "Description": {"type": "array","items": {"type": "string"}}},
  "required": ["category"],
  "additionalProperties": false},
"Counter": {
  "type": "object",
  "properties": {
    "value": {"type": "string"},
    "type": {"enum": ["count","peak","average","ext-value"],
    "ext-type": {"type": "string"},
    "unit": {"enum": ["byte","mbit","packet","flow","session","alert",
      "message","event","host","site","organization",
      "ext-value"],
    "ext-unit": {"type": "string"},
    "meaning": {"type": "string"},
    "duration": {"$ref": "/definitions/duration"},
    "ext-duration": {"type": "string"},
    "required": ["type","unit"],
    "additionalProperties": false},
"DomainData": {
  "type": "object",
  "properties": {
    "system-status": {
      "enum": ["spoofed","fraudulent","innocent-hacked",
      "innocent-hijacked","unknown","ext-value"],
    "ext-system-status": {"type": "string"},
    "domain-status": {
      "enum": ["reservedDelegation","assignedAndActive","assignedAndInactive",
      "assignedAndOnHold","revoked","transferPending","registryLock",
      "registrarLock","other","unknown","ext-value"],
    "ext-domain-status": {"type": "string"},
    "observable-id": {"$ref": "/definitions/IDtype"},
    "Name": {"type": "string"},
    "DateDomainWasChecked": {"$ref": "/definitions/DATETIME"},
    "RegistrationDate": {"$ref": "/definitions/DATETIME"},
    "ExpirationDate": {"$ref": "/definitions/DATETIME"},
    "RelatedDNS": {
      "type": "array","items": {"$ref": "/definitions/ExtensionType"},
    "NameServers": {"type": "array","items": {"$ref": "/definitions/NameServers"},
    "DomainContacts": {"$ref": "/definitions/DomainContacts"},
    "required": ["Name","system-status","domain-status"],
    "additionalProperties": false},
"NameServers": {
  "type": "object",
"properties": {
  "Server": {"type": "string"},
  "Address": {"type": "array",
    "items": {"$ref": "#/definitions/Address"}}},
  "required": ["Server", "Address"],
  "additionalProperties": false},
  "DomainContacts": {
    "type": "object",
    "properties": {
      "SameDomainContact": {"type": "string"},
      "Contact": {"type": "array",
        "items": {"$ref": "#/definitions/Contact"}}},
      "required": ["Contact"],
      "additionalProperties": false},
      "Service": {
        "type": "object",
        "properties": {
          "ip-protocol": {"type": "integer"},
          "observable-id": {"$ref": "#/definitions/IDtype"},
          "ServiceName": {"$ref": "#/definitions/ServiceName"},
          "Port": {"type": "integer"},
          "Portlist": {"$ref": "#/definitions/PORTLIST"},
          "ProtoCode": {"type": "integer"},
          "ProtoType": {"type": "integer"},
          "ProtoField": {"type": "integer"},
          "ApplicationHeaderField": {"$ref": "#/definitions/ExtensionTypeList"},
          "EmailData": {"$ref": "#/definitions/EmailData"},
          "Application": {"$ref": "#/definitions/SoftwareType"},
          "required": [],
          "additionalProperties": false},
          "ServiceName": {
            "type": "object",
            "properties": {
              "IANAService": {"type": "string"},
              "URL": {"type": "array", "items": {"$ref": "#/definitions/URLtype"}},
              "Description": {"type": "array", "items": {"type": "string"}}},
              "required": [],
              "additionalProperties": false},
              "EmailData": {
                "type": "object",
                "properties": {
                  "observable-id": {"$ref": "#/definitions/IDtype"},
                  "EmailTo": {"type": "array", "items": {"type": "string"}},
                  "EmailFrom": {"type": "string"},
                  "EmailSubject": {"type": "string"},
                  "EmailX-Mailer": {"type": "string"},
                  "EmailHeaderField": {
                    "type": "array", "items": {"$ref": "#/definitions/ExtensionType"}}},
                    "required": [],
                    "additionalProperties": false}},
"EmailHeaders": {"type": "string"},
"EmailBody": {"type": "string"},
"EmailMessage": {"type": "string"},
"HashData": {
  "type": "array", "items": {"$ref": "/#definitions/HashData"},
"Signature": {"type": "array", "items": {"type": "string"}}},
"required": [],
"additionalProperties": false},
"RecordData": {
  "type": "object",
  "properties": {
    "restriction": {"$ref": "/#definitions/restriction"},
    "ext-restriction": {"type": "string"},
    "observable-id": {"$ref": "/#definitions/IDtype"},
    "DateTime": {"$ref": "/#definitions/DATETIME"},
    "Description": {"type": "array", "items": {"type": "string"}},
    "Application": {"$ref": "/#definitions/SoftwareType"},
    "RecordPattern": {
      "type": "array", "items": {"$ref": "/#definitions/RecordPattern"}},
    "RecordItem": {
      "type": "array", "items": {"$ref": "/#definitions/ExtensionType"},
    "URL": {
      "type": "array", "items": {"$ref": "/#definitions/URLtype"}},
    "FileData": {
      "type": "array", "items": {"$ref": "/#definitions/FileData"},
    "WindowsRegistryKeysModified": {
      "type": "array",
      "items": {"$ref": "/#definitions/WindowsRegistryKeysModified"}},
    "CertificateData": {
      "type": "array", "items": {"$ref": "/#definitions/CertificateData"}},
    "AdditionalData": {"$ref": "/#definitions/ExtensionTypeList"},
  }},
  "required": [],
  "additionalProperties": false,
"RecordPattern": {
  "type": "object",
  "properties": {
    "value": {"type": "string"},
    "type": {"enum": ["regex", "binary", "xpath", "ext-value"],
    "ext-type": {"type": "string"},
    "offset": {"type": "integer"},
    "offsetunit": {"enum": ["line", "byte", "ext-value"],
    "ext-offsetunit": {"type": "string"},
    "instance": {"type": "integer"},
  }},
  "required": [],
  "additionalProperties": false,
"WindowsRegistryKeysModified": {
  "type": "object"},
"type": "array", "items": {"$ref": "/#definitions/WindowsRegistryKeysModified"},
"CertificateData": {
  "type": "array", "items": {"$ref": "/#definitions/CertificateData"}},
"AdditionalData": {"$ref": "/#definitions/ExtensionTypeList"},
  }},
  "required": [],
  "additionalProperties": false,
"RecordPattern": {
  "type": "object",
  "properties": {
    "value": {"type": "string"},
    "type": {"enum": ["regex", "binary", "xpath", "ext-value"],
    "ext-type": {"type": "string"},
    "offset": {"type": "integer"},
    "offsetunit": {"enum": ["line", "byte", "ext-value"],
    "ext-offsetunit": {"type": "string"},
    "instance": {"type": "integer"},
  }},
  "required": [],
  "additionalProperties": false,
"WindowsRegistryKeysModified": {
  "type": "object"},
"type": "array", "items": {"$ref": "/#definitions/WindowsRegistryKeysModified"},
"CertificateData": {
  "type": "array", "items": {"$ref": "/#definitions/CertificateData"}},
"AdditionalData": {"$ref": "/#definitions/ExtensionTypeList"},
  }},
  "required": [],
  "additionalProperties": false,
}
"properties": {
  "observable-id": {"$ref": "#/definitions/IDtype"},
  "Key": {"type": "array","items": {"$ref": "#/definitions/Key"},
    "required": ["Key"],
    "additionalProperties": false},
  "Key": {
    "type": "object",
    "properties": {
      "registryaction": {"enum": ["add-key","add-value","delete-key",
                                 "delete-value","modify-key","modify-value",
                                 "ext-value"]},
      "ext-registryaction": {"type": "string"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "KeyName": {"type": "string"},
      "KeyValue": {"type": "string"},
      "required": ["KeyName"],
      "additionalProperties": false},
  "CertificateData": {
    "type": "object",
    "properties": {
      "restriction": {"$ref": "#/definitions/restriction"},
      "ext-restriction": {"type": "string"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "Certificate": {
        "type": "array","items": {"$ref": "#/definitions/Certificate"},
        "required": ["Certificate"],
        "additionalProperties": false},
      "Certificate": {
        "type": "object",
        "properties": {
          "observable-id": {"$ref": "#/definitions/IDtype"},
          "X509Data": {"type": "string"},
          "Description": {"type": "array","items": {"type": "string"}}},
          "required": ["X509Data"],
          "additionalProperties": false},
          "Certificate": {
            "type": "object",
            "properties": {
              "observable-id": {"$ref": "#/definitions/IDtype"},
              "File": {
                "type": "array","items": {"$ref": "#/definitions/File"},
                "required": ["File"],
                "additionalProperties": false},
                "File": {
                  "type": "object",
                  "properties": {
                    "FileName": {"type": "string"},
                    "Description": {"type": "array","items": {"type": "string"}}}}}
"FileSize": {"type": "integer"},
"FileType": {"type": "string"},
"URL": {"type": "array", "items": {"$ref": "/definitions/URLtype"}},
"HashData": {"$ref": "/definitions/HashData"},
"Signature": {"type": "array", "items": {"type": "string"}},
"AssociatedSoftware": {"$ref": "/definitions/SoftwareType"},
"FileProperties": {
  "type": "array", "items": {"$ref": "/definitions/ExtensionType"},
  "required": [],
  "additionalProperties": false},
"HashData": {
  "type": "object",
  "properties": {
    "scope": {"enum": ["file-contents", "file-pe-section", "file-pe-iat",
      "file-pe-resource", "file-pdf-object", "email-hash",
      "email-hash-header", "email-hash-body"],
    "HashTargetID": {"type": "string"},
    "Hash": {"type": "array", "items": {"$ref": "/definitions/Hash"}},
    "FuzzyHash": {
      "type": "array", "items": {"$ref": "/definitions/FuzzyHash"},
      "required": ["scope"],
      "additionalProperties": false},
    "Hash": {
      "type": "object",
      "properties": {
        "DigestMethod": {"type": "string"},
        "DigestValue": {"type": "string"},
        "CanonicalizationMethod": {},
        "Application": {"$ref": "/definitions/SoftwareType"},
        "required": ["DigestMethod", "DigestValue"],
        "additionalProperties": false},
    "FuzzyHash": {
      "type": "object",
      "properties": {
        "FuzzyHashValue": {
          "type": "array", "items": {"$ref": "/definitions/ExtensionType"},
          "Application": {"$ref": "/definitions/SoftwareType"},
          "AdditionalData": {"$ref": "/definitions/ExtensionTypeList"},
          "required": ["FuzzyHashValue"],
          "additionalProperties": false},
    "Indicator": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "IndicatorID": {"$ref": "/definitions/IndicatorID"},
        "AlternativeIndicatorID": {
          "type": "array"}
"items": {"$ref": "#/definitions/AlternativeIndicatorID"},
"Description": {"type": "array","items": {"type": "string"}},
"StartTime": {"$ref": "#/definitions/DATETIME"},
"EndTime": {"$ref": "#/definitions/DATETIME"},
"Confidence": {"$ref": "#/definitions/Confidence"},
"Contact": { "type": "array","items": {"$ref": "#/definitions/Contact"}},
"Observable": {"$ref": "#/definitions/Observable"},
"uid-ref": {"type": "string"},
"IndicatorExpression":{"$ref": "#/definitions/IndicatorExpression"},
"IndicatorReference": {"$ref": "#/definitions/IndicatorReference"},
"NodeRole": {"type": "array","items": {"$ref": "#/definitions/NodeRole"}},
"AttackPhase": {"type": "array","items": {"$ref": "#/definitions/AttackPhase"}},
"Reference": {"type": "array","items": {"$ref": "#/definitions/Reference"}},
"additionalData": {"$ref":"#/definitions/ExtensionTypeList"},
"required": ["IndicatorID"],
"additionalProperties": false},
"IndicatorID": { "type": "object",
"properties": { "id": {"type": "string"},
"name": {"type": "string"},
"version": {"type": "string"},
"required": ["name","version"],
"additionalProperties": false},
"AlternativeIndicatorID": { "type": "object",
"properties": { "restriction": {"$ref": "#/definitions/restriction"},
"ext-restriction": {"type": "string"},
"IndicatorReference": { "type": "array", "items": {"$ref": "#/definitions/IndicatorReference"}}},
"additionalProperties": false},
"Observable": {"type": "object",
"properties": { "restriction": {"$ref": "#/definitions/restriction"},
"ext-restriction": {"type": "string"},
"System": {"$ref": "#/definitions/System"},
"Address": {"$ref": "#/definitions/Address"},
"DomainData": {"$ref": "#/definitions/DomainData"},
"EmailData": {"$ref": "#/definitions/EmailData"},
"Service": {"$ref": "#/definitions/Service"},
"required": ["IndicatorID"],
"additionalProperties": false}
"WindowsRegistryKeysModified": {
  "$ref": "#/definitions/WindowsRegistryKeysModified"},
"FileData": {
  "$ref": "#/definitions/FileData"},
"CertificateData": {
  "$ref": "#/definitions/CertificateData"},
"RegistryHandle": {
  "$ref": "#/definitions/RegistryHandle"},
"RecordData": {
  "type": "array",
  "item": {
    "$ref": "#/definitions/Record"},
"EventData": {
  "$ref": "#/definitions/EventData"},
"Incident": {
  "$ref": "#/definitions/Incident"},
"Reference": {
  "$ref": "#/definitions/Reference"},
"Assessment": {
  "$ref": "#/definitions/Assessment"},
"DetectionPattern": {
  "$ref": "#/definitions/DetectionPattern"},
"HistoryItem": {
  "$ref": "#/definitions/HistoryItem"},
"BulkObservable": {
  "$ref": "#/definitions/BulkObservable"},
"AdditionalData": {
  "$ref": "#/definitions/ExtensionTypeList"},
"required": [],
"additionalProperties": false},
"BulkObservable": {
  "type": "object",
  "properties": {
    "type": {
      "enum": ["asn", "atm", "e-mail", "ipv4-addr", "ipv4-net",
                "ipv4-net-mask", "ipv6-addr", "ipv6-net", "ipv6-net-mask",
                "mac", "site-url", "domain-name", "domain-to-ipv4",
                "domain-to-ipv6", "domain-to-ipv4-timestamp",
                "domain-to-ipv6-timestamp", "ipv4-port", "ipv6-port",
                "windows-reg-key", "file-hash", "email-x-mailer",
                "email-subject", "http-user-agent", "http-request-url",
                "mutex", "file-path", "user-name", "ext-value"],
    "ext-type": {
      "type": "string"},
    "BulkObservableFormat": {
      "$ref": "#/definitions/BulkObservableFormat"},
    "BulkObservableList": {
      "type": "array",
      "item": {
        "type": "string"},
    "AdditionalData": {
      "$ref": "#/definitions/ExtensionTypeList"},
    "required": [],
    "additionalProperties": false},
"BulkObservableFormat": {
  "type": "object",
  "properties": {
    "Hash": {
      "$ref": "#/definitions/Hash"},
    "AdditionalData": {
      "$ref": "#/definitions/ExtensionTypeList"},
    "required": [],
    "additionalProperties": false},
"IndicatorExpression": {
  "type": "object",
  "properties": {
    "operator": {
      "enum": ["not", "and", "or", "xor"],
    "ext-operator": {
      "type": "string"},
"IndicatorExpression": {  
  "type": "array",  
  "items": {"$ref": "/definitions/IndicatorExpression"},  
  "Observable": {  
    "type": "array",  
    "items": {"$ref": "/definitions/Observable"},  
    "uid-ref": {"type": "string"},  
    "IndicatorReference": {  
      "type": "array",  
      "items": {"$ref": "/definitions/IndicatorReference"},  
      "AdditionalData": {"$ref": "/definitions/ExtensionTypeList"},  
      "required": [],  
      "additionalProperties": false  
    },  
    "IndicatorReference": {  
      "type": "object",  
      "properties": {  
        "uid-ref": {"type": "string"},  
        "euid-ref": {"type": "string"},  
        "version": {"type": "string"},  
        "required": [],  
        "additionalProperties": false  
      },  
      "AttackPhase": {  
        "type": "object",  
        "properties": {  
          "AttackPhaseID": {"type": "array", "items": {"type": "string"}},  
          "URL": {"type": "array", "items": {"$ref": "/definitions/URLtype"}},  
          "Description": {"type": "array", "items": {"type": "string"}},  
          "AdditionalData": {"$ref": "/definitions/ExtensionTypeList"},  
          "required": [],  
          "additionalProperties": false  
        },  
        "title": "IODEF-Document",  
        "description": "JSON schema for IODEF-Document class",  
        "type": "object",  
        "properties": {  
          "version": {"type": "string"},  
          "lang": {"$ref": "/definitions/lang"},  
          "format-id": {"type": "string"},  
          "private-enum-name": {"type": "string"},  
          "private-enum-id": {"type": "string"},  
          "Incident": {  
            "type": "array",  
            "items": {"$ref": "/definitions/Incident"},  
            "AdditionalData": {"$ref": "/definitions/ExtensionTypeList"},  
            "required": [{"version", "Incident"}],  
            "additionalProperties": false  
          }  
        }  
      }  
    }  
  }  
}  

Figure 3: JSON schema
Authors’ Addresses

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

Phone: +81 42 327 5862
Email: takeshi_takahashi@nict.go.jp

Roman Danyliw
CERT, Software Engineering Institute, Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA
USA

Email: rdd@cert.org

Mio Suzuki
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi
Koganei, Tokyo 184-8795
Japan

Email: mio@nict.go.jp
Using XMPP for Security Information Exchange

draft-ietf-mile-xmpp-grid-05

Abstract

This document describes how to use the Extensible Messaging and Presence Protocol (XMPP) to collect and distribute security-relevant information between network-connected devices. To illustrate the principles involved, this document describes such a usage for the Incident Object Description Exchange Format (IODEF).

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 August 12, 2018.

Copyright Notice

Copyright (c) 2018 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

1. Introduction

This document describes "XMPP-Grid": a method for using the Extensible Messaging and Presence Protocol (XMPP) [RFC6120] to collect and distribute security-relevant information among network platforms, endpoints, and any other network-connected device. Among other things, XMPP provides a publish-subscribe service [XEP-0060] that acts as a broker, enabling control-plane functions by which entities can discover available information to be published or consumed. Although such information can take the form of any structured data (XML, JSON, etc.), this document illustrates the principles of XMPP-Grid with examples that use the Incident Object Description Exchange Format (IODEF) [RFC7970].

2. Terminology

This document uses XMPP terminology defined in [RFC6120] and [XEP-0060] as well as Security Automation and Continuous Monitoring (SACM) terminology defined in [I-D.ietf-sacm-terminology]. Because the intended audience for this document is those who implement and deploy security reporting systems, in general the SACM terms are used (however, mappings are provided for the benefit of XMPP developers and operators).
Broker: In SACM, a specific type of controller containing control plane functions; as used here, the term refers to an XMPP publish-subscribe service.

Broker Flow: In SACM, a method by which security-related information is published and consumed in a mediated fashion through a Broker. In this flow, the Broker handles authorization of Consumers and Providers to Topics, receives messages from Providers, and delivers published messages to Consumers.

Consumer: In SACM, an entity that contains functions to receive information from other components; as used here, the term refers to an XMPP publish-subscribe Subscriber.

Controller: In SACM, a "component containing control plane functions that manage and facilitate information sharing or execute on security functions"; as used here, the term refers to an XMPP server, which provides core message delivery [RFC6120] used by publish-subscribe entities.

Node: The XMPP term for a Topic.

Platform: Any entity that connects to the XMPP-Grid in order to publish or consume security-related data.

Provider: In SACM, an entity that contains functions to provide information to other components; as used here, the term refers to an XMPP publish-subscribe Publisher.

Publisher: The XMPP term for a Provider.

Publish-Subscribe Service: The XMPP term for the kind Broker discussed here.

Subscriber: The XMPP term for a Consumer.

Topic: A contextual information channel created on a Broker at which messages generated by a Provider are propagated in real time to one or more Consumers. Each Topic is limited to a specific type and format of security data (e.g., IODEF) and provides an XMPP interface by which the data can be obtained.

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. Architecture

The following figure illustrates the architecture of XMPP-Grid.

Platforms connect to the Controller (XMPP server) to authenticate and then establish appropriate authorizations and relationships (e.g., Provider or Consumer) at the Broker. The control plane messaging is established through XMPP and shown as "A" (control plane interface) in Figure 1. Authorized nodes can then share data either thru the...
Broker (shown as "B" in Figure 1) or in some cases directly (shown as "C" in Figure 1). This document focuses primarily on the Broker Flow for information sharing ("direct flow" interactions can be used for specialized purposes such as bulk data transfer, but methods for doing so are outside the scope of this document).

4. Workflow

A typical XMPP-Grid workflow is as follows:

a. A Platform with a source of security data requests connection to the XMPP-Grid via a Controller (XMPP server).

b. The Controller authenticates the Platform.

c. The Platform establishes authorized privileges (e.g. privilege to publish and/or subscribe to security data Topics) with a Broker.

d. The Platform can publish security-related data to a Topic, subscribe to a Topic, query a Topic, or any combination of these operations.

e. A Provider unicasts its Topic updates to the Grid in real time through a Broker. The Broker handles replication and distribution of the Topic to Consumers. A Provider can publish the same or different data to multiple Topics.

f. Any Platform on the Grid can subscribe to any Topics published to the Grid (as permitted by authorization policy), and as Consumers will then receive a continual, real-time stream of updates from the Topics to which it is subscribed.

The general workflow is summarized in the figure below:
<table>
<thead>
<tr>
<th>IODEF Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Consumer)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Establish XMPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Session</td>
</tr>
<tr>
<td>(RFC 6120)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Controller &amp; Broker</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>IODEF Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Provider)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Establish XMPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Session</td>
</tr>
<tr>
<td>(RFC 6120)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Request Topic List</th>
</tr>
</thead>
<tbody>
<tr>
<td>(XEP-0030)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Request Topic List</th>
</tr>
</thead>
<tbody>
<tr>
<td>(XEP-0030)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Request Topic List</th>
</tr>
</thead>
<tbody>
<tr>
<td>(XEP-0030)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subscribe to IODEF Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>(XEP-0060)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subscription Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>(XEP-0060)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Publish IODEF Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>(XEP-0060)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Receive IODEF Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>(XEP-0060)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Query Each Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>(XEP-0030)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Return Topic Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Including Topic Type</td>
</tr>
<tr>
<td>(XEP-0030)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Return Topic List</th>
</tr>
</thead>
<tbody>
<tr>
<td>(XEP-0030)</td>
</tr>
</tbody>
</table>

Figure 2: IODEF Example Workflow
The following sections provide protocol examples for the service discovery and publish-subscribe parts of the workflow.

5. Service Discovery

Using the XMPP service discovery extension [XEP-0030], a Controller enables Platforms to discover what information can be consumed through the Broker, and at which Topics. As an example, the Controller at 'security-grid.example' might provide a Broker at 'broker.security-grid.example' hosting a number of Topics. A Platform at 'xmpp-grid-client@mile-host.example' would query the Broker about its available Topics by sending an XMPP "disco#items" request to the Broker:

```
<iq type='get'
   from='xmpp-grid-client@mile-host.example/2EBE702A97D6'
   to='broker.security-grid.example'
   id='B3C17F7B-B9EF-4ABA-B08D-805DA9F34626'>
   <query xmlns='http://jabber.org/protocol/disco#items'/>
</iq>
```

The Broker responds with the Topics it hosts:

```
<iq type='result'
   from='broker.security-grid.example'
   to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
   id='B3C17F7B-B9EF-4ABA-B08D-805DA9F34626'>
   <query xmlns='http://jabber.org/protocol/disco#items'>
     <item node='NEA1'
           name='Endpoint Posture Information'
           jid='broker.security-grid.example'/>
     <item node='MILEHost'
           name='MILE Host Data'
           jid='broker.security-grid.example'/>
   </query>
</iq>
```

In order to determine the exact nature of each Topic (i.e., in order to find topics that publish incidents in the IODEF format), a Platform would send an XMPP "disco#info" request to each Topic:

```
<iq type='get'
   from='xmpp-grid-client@mile-host.example/2EBE702A97D6'
   to='broker.security-grid.example'
   id='D367D4ED-2795-489C-A83E-EAAFA07A0356'>
   <query xmlns='http://jabber.org/protocol/disco#info'
           node='MILEHost'/>
</iq>
```
The Broker responds with the "disco#info" description, which SHOULD include an XMPP Data Form [XEP-0004] including a 'pubsub#type' field that specifies the supported namespace (in this example, the IODEF namespace defined in [RFC7970]):

```xml
<iq type='result'
    from='broker.security-grid.example'
    to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    id='D367D4ED-2795-489C-A83E-EAAFA07A0356'/>
<query xmlns='http://jabber.org/protocol/disco#info'
    node='MILEHost'>
  <identity category='pubsub' type='leaf'/>
  <feature var='http://jabber.org/protocol/pubsub'/>
  <x xmlns='jabber:x:data' type='result'>
    <field var='FORM_TYPE' type='hidden'>
      <value>http://jabber.org/protocol/pubsub#meta-data</value>
    </field>
    <field var='pubsub#type' label='Payload type' type='text-single'>
      <value>urn:ietf:params:xml:ns:iodef-2.0</value>
    </field>
  </x>
</query>
</iq>

6. Publish-Subscribe

Using the XMPP publish-subscribe extension [XEP-0030], a Consumer subscribes to a Topic and a Provider publishes information to that Topic, which the Broker then distributes to all subscribed Consumers.

First, a Provider would create a Topic as follows:

```xml
<iq type='set'
    from='datasource@provider.example/F12C2EFC9BB0'
    to='broker.security-grid.example'
    id='A67507DF-2F22-4937-8D30-88D2F7DBA279'/>
<pubsub xmlns='http://jabber.org/protocol/pubsub'>
  <create node='MILEHost'/>
</pubsub>
</iq>

Note: The foregoing example is the minimal protocol needed to create a Topic with the default node configuration on the XMPP publish-subscribe service specified in the 'to' address of the creation request stanza. Depending on security requirements, the Provider might need to request a non-default configuration for the node; see [XEP-0060] for detailed examples.
Unless an error occurs (see [XEP-0060] for various error flows), the Broker responds with success:

```xml
<iq type='result'
   from='broker.security-grid.example'
   to='datasource@provider.example/F12C2EFC9BB0'
   id='A67507DF-2F22-4937-8D30-88D2F7DBA279'/>
```

Second, a Consumer would subscribe as follows:

```xml
<iq type='set'
   from='xmpp-grid-client@mile-host.example/2EBE702A97D6'
   to='broker.security-grid.example'
   id='9C6EEE9E-F09A-4418-8D68-3BA6AF852522'>
   <pubsub xmlns='http://jabber.org/protocol/pubsub'>
     <subscribe node='MILEHost'
               jid='xmpp-grid-client@mile-host.example'/>
   </pubsub>
</iq>
```

Unless an error occurs (see [XEP-0060] for various error flows), the Broker responds with success:

```xml
<iq type='result'
   from='broker.security-grid.example'
   to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
   id='9C6EEE9E-F09A-4418-8D68-3BA6AF852522'>
   <pubsub xmlns='http://jabber.org/protocol/pubsub'>
     <subscription node='MILEHost'
                   jid='xmpp-grid-client@mile-host.example'
                   subscription='subscribed'/>
   </pubsub>
</iq>
```

Third, a Provider would publish an incident as follows:
<iq type='set'
    from='datasource@provider.example/F12C2EFC9BB0'
    to='broker.security-grid.example'
    id='2A17D283-0DAE-4A6C-85A9-C10B1B40928C'>
    <pubsub xmlns='http://jabber.org/protocol/pubsub'>
        <publish node='MILEHost'>
            <item id='8bh1g27skbga47fh9wk7'>
                <IODEF-Document version="2.00" xml:lang="en"
                    xmlns="urn:ietf:params:xml:ns:iodef-2.0"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xsi:schemaLocation="http://www.iana.org/assignments/xml-registry/
                                    schema/iodef-2.0.xsd">
                    <Incident purpose="reporting" restriction="private">
                        <IncidentID name="csirt.example.com">492382</IncidentID>
                        <GenerationTime>2015-07-18T09:00:00-05:00</GenerationTime>
                        <Contact type="organization" role="creator">
                            <Email>
                                <EmailTo>contact@csirt.example.com</EmailTo>
                            </Email>
                        </Contact>
                    </Incident>
                </IODEF-Document>
            </item>
        </publish>
    </pubsub>
</iq>

(The payload in the foregoing example is from [RFC7970]; payloads for additional use cases can be found in [RFC8274].)

The Broker would then deliver that incident report to all Consumers who are subscribe to the Topic:
<message
  from='broker.security-grid.example'
  to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
  id='37B3921D-4F7F-450F-A589-56119A88BC2E'>
  <event xmlns='http://jabber.org/protocol/pubsub#event'>
    <items node='MILEHost'>
      <item id='iah37s61s964gquqy47aksbx9453ks77'>
        <IODEF-Document version="2.00" xml:lang="en"
          xmlns="urn:ietf:params:xml:ns:iodef-2.0"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation="http://www.iana.org/assignments/xml-registry/
            schema/iodef-2.0.xsd">
          <Incident purpose="reporting" restriction="private">
            <IncidentID name="csirt.example.com">492382</IncidentID>
            <GenerationTime>2015-07-18T09:00:00-05:00</GenerationTime>
            <Contact type="organization" role="creator">
              <Email>
                <EmailTo>contact@csirt.example.com</EmailTo>
              </Email>
            </Contact>
          </Incident>
        </IODEF-Document>
      </item>
    </items>
  </event>
</message>

7. IANA Considerations

This document has no actions for IANA.

8. Security Considerations

An XMPP-Grid Controller serves as a controlling broker for XMPP-Grid Platforms, such as Enforcement Points, Policy Servers, CMDBs, and Sensors, using a publish-subscribe-search model of information exchange and lookup. By increasing the ability of XMPP-Grid Platforms to learn about and respond to security-relevant events and data, XMPP-Grid can improve the timeliness and utility of the security system. However, this integrated security system can also be exploited by attackers if they can compromise it. Therefore, strong security protections for XMPP-Grid are essential.

This section provides a security analysis of the XMPP-Grid data transfer protocol and the architectural elements that employ it, specifically with respect to their use of this protocol. Three subsections define the trust model (which elements are trusted to do...
what), the threat model (attacks that can be mounted on the system), and the countermeasures (ways to address or mitigate the threats previously identified).

8.1. Trust Model

The first step in analyzing the security of the XMPP-Grid transport protocol is to describe the trust model, listing what each architectural element is trusted to do. The items listed here are assumptions, but provisions are made in the Threat Model and Countermeasures sections for elements that fail to perform as they were trusted to do.

8.1.1. Network

The network used to carry XMPP-Grid messages (i.e., the underlying network transport layer over which XMPP runs) is trusted to:

- Perform best effort delivery of network traffic

The network used to carry XMPP-Grid messages is not expected (trusted) to:

- Provide confidentiality or integrity protection for messages sent over it
- Provide timely or reliable service

8.1.2. XMPP-Grid Platforms

Authorized XMPP-Grid Platforms are trusted to:

- Preserve the confidentiality of sensitive data retrieved via the XMPP-Grid Controller

8.1.3. XMPP-Grid Controller

The XMPP-Grid Controller (including its associated Broker) is trusted to:

- Broker requests for data and enforce authorization of access to this data throughout its lifecycle
- Perform service requests in a timely and accurate manner
- Create and maintain accurate operational attributes

Only reveal data to and accept service requests from authorized parties

The XMPP-Grid Controller is not expected (trusted) to:

- Verify the truth (correctness) of data

### 8.1.4. Certification Authority

The Certification Authority (CA) that issues certificates for the XMPP-Grid Controller and/or XMPP-Grid Platforms (or each CA, if there are several) is trusted to:

- Ensure that only proper certificates are issued and that all certificates are issued in accordance with the CA’s policies
- Revoke certificates previously issued when necessary
- Regularly and securely distribute certificate revocation information
- Promptly detect and report any violations of this trust so that they can be handled

The CA is not expected (trusted) to:

- Issue certificates that go beyond the XMPP-Grid needs or other constraints imposed by a relying party.

### 8.2. Threat Model

To secure the XMPP-Grid data transfer protocol and the architectural elements that implement it, this section identifies the attacks that can be mounted against the protocol and elements.

#### 8.2.1. Network Attacks

A variety of attacks can be mounted using the network. For the purposes of this subsection the phrase "network traffic" can be taken to mean messages and/or parts of messages. Any of these attacks can be mounted by network elements, by parties who control network elements, and (in many cases) by parties who control network-attached devices.

- Network traffic can be passively monitored to glean information from any unencrypted traffic
Even if all traffic is encrypted, valuable information can be gained by traffic analysis (volume, timing, source and destination addresses, etc.)

Network traffic can be modified in transit

Previously transmitted network traffic can be replayed

New network traffic can be added

Network traffic can be blocked, perhaps selectively

A "Man In The Middle" (MITM) attack can be mounted where an attacker interposes itself between two communicating parties and poses as the other end to either party or impersonates the other end to either or both parties

Resist attacks (including denial of service and other attacks from XMPP-Grid Platforms)

Undesired network traffic can be sent in an effort to overload an architectural component, thus mounting a denial of service attack

8.2.2. XMPP-Grid Platforms

An unauthorized XMPP-Grid Platform (one which is not recognized by the XMPP-Grid Controller or is recognized but not authorized to perform any actions) cannot mount any attacks other than those listed in the Network Attacks section above.

An authorized XMPP-Grid Platform, on the other hand, can mount many attacks. These attacks might occur because the XMPP-Grid Platform is controlled by a malicious, careless, or incompetent party (whether because its owner is malicious, careless, or incompetent or because the XMPP-Grid Platform has been compromised and is now controlled by a party other than its owner). They might also occur because the XMPP-Grid Platform is running malicious software; because the XMPP-Grid Platform is running buggy software (which can fail in a state that floods the network with traffic); or because the XMPP-Grid Platform has been configured improperly. From a security standpoint, it generally makes no difference why an attack is initiated. The same countermeasures can be employed in any case.

Here is a list of attacks that can be mounted by an authorized XMPP-Grid Platform:

Cause many false alarms or otherwise overload the XMPP-Grid Controller or other elements in the network security system
(including human administrators) leading to a denial of service or disabling parts of the network security system

- Omit important actions (such as posting incriminating data), resulting in incorrect access
- Use confidential information obtained from the XMPP-Grid Controller to enable further attacks (such as using endpoint health check results to exploit vulnerable endpoints)
- Advertise data crafted to exploit vulnerabilities in the XMPP-Grid Controller or in other XMPP-Grid Platforms, with a goal of compromising those systems
- Issue a search request or set up a subscription that matches an enormous result, leading to resource exhaustion on the XMPP-Grid Controller, the publishing XMPP-Grid Platform, and/or the network
- Establish a communication channel using another XMPP-Grid Platform’s session-id

Dependencies of or vulnerabilities of authorized XMPP-Grid Platforms can be exploited to effect these attacks. Another way to effect these attacks is to gain the ability to impersonate an XMPP-Grid Platform (through theft of the XMPP-Grid Platform’s identity credentials or through other means). Even a clock skew between the XMPP-Grid Platform and XMPP-Grid Controller can cause problems if the XMPP-Grid Platform assumes that old XMPP-Grid Platform data deserves to be ignored.

8.2.3. XMPP-Grid Controllers

An unauthorized XMPP-Grid Controller (one which is not trusted by XMPP-Grid Platforms) cannot mount any attacks other than those listed in the Network Attacks section above.

An authorized XMPP-Grid Controller can mount many attacks. Similar to the XMPP-Grid Platform case described above, these attacks might occur because the XMPP-Grid Controller is controlled by a malicious, careless, or incompetent party (either an XMPP-Grid Controller administrator or an attacker who has seized control of the XMPP-Grid Controller). They might also occur because the XMPP-Grid Controller is running malicious software, because the XMPP-Grid Controller is running buggy software (which can fail in a state that corrupts data or floods the network with traffic), or because the XMPP-Grid Controller has been configured improperly.
All of the attacks listed for XMPP-Grid Platform above can be mounted by the XMPP-Grid Controller. Detection of these attacks will be more difficult since the XMPP-Grid Controller can create false operational attributes and/or logs that imply some other party created any bad data.

Additional XMPP-Grid Controller attacks can include:

- Expose different data to different XMPP-Grid Platforms to mislead investigators or cause inconsistent behavior.
- Mount an even more effective denial of service attack than a single XMPP-Grid Platform could.
- Obtain and cache XMPP-Grid Platform credentials so they can be used to impersonate XMPP-Grid Platforms even after a breach of the XMPP-Grid Controller is repaired.
- Obtain and cache XMPP-Grid Controller administrator credentials so they can be used to regain control of the XMPP-Grid Controller after the breach of the XMPP-Grid Controller is repaired.

Dependencies of or vulnerabilities of the XMPP-Grid Controller can be exploited to obtain control of the XMPP-Grid Controller and effect these attacks.

8.2.4. Certification Authority

A Certification Authority trusted to issue certificates for the XMPP-Grid Controller and/or XMPP-Grid Platforms can mount several attacks:

- Issue certificates for unauthorized parties, enabling them to impersonate authorized parties such as the XMPP-Grid Controller or an XMPP-Grid Platform. This can lead to all the threats that can be mounted by the certificate’s subject.
- Issue certificates without following all of the CA’s policies. Because this can result in issuing certificates that can be used to impersonate authorized parties, this can lead to all the threats that can be mounted by the certificate’s subject.
- Fail to revoke previously issued certificates that need to be revoked. This can lead to undetected impersonation of the certificate’s subject or failure to revoke authorization of the subject, and therefore can lead to all of the threats that can be mounted by that subject.
o Fail to regularly and securely distribute certificate revocation information. This can cause a relying party to accept a revoked certificate, leading to undetected impersonation of the certificate’s subject or failure to revoke authorization of the subject, and therefore can lead to all of the threats that can be mounted by that subject. It can also cause a relying party to refuse to proceed with a transaction because timely revocation information is not available, even though the transaction should be permitted to proceed.

o Allow the CA’s private key to be revealed to an unauthorized party. This can lead to all the threats above. Even worse, the actions taken with the private key will not be known to the CA.

o Fail to promptly detect and report errors and violations of trust so that relying parties can be promptly notified. This can cause the threats listed earlier in this section to persist longer than necessary, leading to many knock-on effects.

8.3. Countermeasures

Below are countermeasures for specific attack scenarios to the XMPP-Grid infrastructure.

8.3.1. Securing the XMPP-Grid Data Transfer Protocol

To address network attacks, the XMPP-Grid data transfer protocol described in this document requires that the XMPP-Grid messages MUST be carried over TLS (minimally TLS 1.2 [RFC5246]) as described in [RFC6120] and updated by [RFC7590]. The XMPP-Grid Platform MUST verify the XMPP-Grid Controller’s certificate and determine whether the XMPP-Grid Controller is trusted by this XMPP-Grid Platform before completing the TLS handshake. The XMPP-Grid Controller MUST authenticate the XMPP-Grid Platform either using the SASL EXTERNAL mechanism or using the SASL SCRAM mechanism (with the SCRAM-SHA-256-PLUS variant being preferred over the SCRAM-SHA-256 variant and SHA-256 variants [RFC7677] being preferred over SHA-1 variants [RFC5802]). XMPP-Grid Platforms and XMPP-Grid Controllers using mutual certificate-based authentication SHOULD each verify the revocation status of the other party’s certificate. All XMPP-Grid Controllers and XMPP-Grid Platforms MUST implement both SASL EXTERNAL and SASL SCRAM. The selection of which XMPP-Grid Platform authentication technique to use in any particular deployment is left to the administrator.

These protocol security measures provide protection against all the network attacks listed in the above document section except denial of service attacks. If protection against these denial of service
attacks is desired, ingress filtering, rate limiting per source IP address, and other denial of service mitigation measures can be employed. In addition, an XMPP-Grid Controller MAY automatically disable a misbehaving XMPP-Grid Platform.

8.3.2. Securing XMPP-Grid Platforms

XMPP-Grid Platforms can be deployed in locations that are susceptible to physical attacks. Physical security measures can be taken to avoid compromise of XMPP-Grid Platforms, but these are not always practical or completely effective. An alternative measure is to configure the XMPP-Grid Controller to provide read-only access for such systems. The XMPP-Grid Controller SHOULD also include a full authorization model so that individual XMPP-Grid Platforms can be configured to have only the privileges that they need. The XMPP-Grid Controller MAY provide functional templates so that the administrator can configure a specific XMPP-Grid Platform as a DHCP server and authorize only the operations and metadata types needed by a DHCP server to be permitted for that XMPP-Grid Platform. These techniques can reduce the negative impacts of a compromised XMPP-Grid Platform without diminishing the utility of the overall system.

To handle attacks within the bounds of this authorization model, the XMPP-Grid Controller MAY also include rate limits and alerts for unusual XMPP-Grid Platform behavior. XMPP-Grid Controllers SHOULD make it easy to revoke an XMPP-Grid Platform's authorization when necessary. Another way to detect attacks from XMPP-Grid Platforms is to create fake entries in the available data (honeytokens) which normal XMPP-Grid Platforms will not attempt to access. The XMPP-Grid Controller SHOULD include auditable logs of XMPP-Grid Platform activities.

To avoid compromise of XMPP-Grid Platform, XMPP-Grid Platform SHOULD be hardened against attack and minimized to reduce their attack surface. They should be well managed to minimize vulnerabilities in the underlying platform and in systems upon which the XMPP-Grid Platform depends. Personnel with administrative access should be carefully screened and monitored to detect problems as soon as possible.

8.3.3. Securing XMPP-Grid Controllers

Because of the serious consequences of XMPP-Grid Controller compromise, XMPP-Grid Controllers need to be especially well hardened against attack and minimized to reduce their attack surface. They need to be well managed to minimize vulnerabilities in the underlying platform and in systems upon which the XMPP-Grid Controller depends. Network security measures such as firewalls or intrusion detection
systems can be used to monitor and limit traffic to and from the
XMPP-Grid Controller. Personnel with administrative access ought to
be carefully screened and monitored to detect problems as soon as
possible. Administrators SHOULD NOT use password-based
authentication but should instead use non-reusable credentials and
multi-factor authentication (where available). Physical security
measures ought to be employed to prevent physical attacks on XMPP-
Grid Controllers.

To ease detection of XMPP-Grid Controller compromise should it occur,
XMPP-Grid Controller behavior should be monitored to detect unusual
behavior (such as a reboot, a large increase in traffic, or different
views of an information repository for similar XMPP-Grid Platforms).
XMPP-Grid Platforms should log and/or notify administrators when
peculiar XMPP-Grid Controller behavior is detected. To aid forensic
investigation, permanent read-only audit logs of security-relevant
information (especially administrative actions) should be maintained.
If XMPP-Grid Controller compromise is detected, a careful analysis
should be performed of the impact of this compromise. Any reusable
credentials that can have been compromised should be reissued.

8.3.4. Broker Access Models for Topics

The XMPP publish-subscribe specification [XEP-0060] defines five
access models for subscribing to Topics at a Broker: open, presence,
roster, authorize, and whitelist. The first model allows
uncontrolled access and the next two models are appropriate only in
instant-messaging applications. Therefore, a Broker SHOULD support
only the authorize model (under which the Topic owner needs to
approve all subscription requests and only subscribers can retrieve
data items) and the whitelist model (under which only preconfigured
Platforms can subscribe or retrieve data items). In order to ease
the deployment burden, subscription approvals and whitelist
management can be automated (e.g., the Topic "owner" can be a policy
server). The choice between "authorize" and "whitelist" as the
default access model is a matter for local service policy.

8.3.5. Limit on Search Result Size

While XMPP-Grid is designed for high scalability to 100,000s of
Platforms, an XMPP-Grid Controller MAY establish a limit to the
amount of data it is willing to return in search or subscription
results. This mitigates the threat of an XMPP-Grid Platform causing
resource exhaustion by issuing a search or subscription that leads to
an enormous result.
8.3.6. Securing the Certification Authority

As noted above, compromise of a Certification Authority (CA) trusted to issue certificates for the XMPP-Grid Controller and/or XMPP-Grid Platforms is a major security breach. Many guidelines for proper CA security have been developed: the CA/Browser Forum's Baseline Requirements, the AICPA/CICA Trust Service Principles, etc. The CA operator and relying parties should agree on an appropriately rigorous security practices to be used.

Even with the most rigorous security practices, a CA can be compromised. If this compromise is detected quickly, relying parties can remove the CA from their list of trusted CAs, and other CAs can revoke any certificates issued to the CA. However, CA compromise may go undetected for some time, and there’s always the possibility that a CA is being operated improperly or in a manner that is not in the interests of the relying parties. For this reason, relying parties may wish to "pin" a small number of particularly critical certificates (such as the certificate for the XMPP-Grid Controller). Once a certificate has been pinned, the relying party will not accept another certificate in its place unless the Administrator explicitly commands it to do so. This does not mean that the relying party will not check the revocation status of pinned certificates. However, the Administrator can still be consulted if a pinned certificate is revoked, since the CA and revocation process are not completely trusted.

8.4. Summary

XMPP-Grid’s considerable value as a broker for security-sensitive data exchange distribution also makes the protocol and the network security elements that implement it a target for attack. Therefore, strong security has been included as a basic design principle within the XMPP-Grid design process.

The XMPP-Grid data transfer protocol provides strong protection against a variety of different attacks. In the event that an XMPP-Grid Platform or XMPP-Grid Controller is compromised, the effects of this compromise have been reduced and limited with the recommended role-based authorization model and other provisions, and best practices for managing and protecting XMPP-Grid systems have been described. Taken together, these measures should provide protection commensurate with the threat to XMPP-Grid systems, thus ensuring that they fulfill their promise as a network security clearing-house.
9. Privacy Considerations

XMPP-Grid Platforms can publish information about endpoint health, network access, events (which can include information about what services an endpoint is accessing), roles and capabilities, and the identity of the end user operating the endpoint. Any of this published information can be queried by other XMPP-Grid Platforms and could potentially be used to correlate network activity to a particular end user.

Dynamic and static information brokered by an XMPP-Grid Controller, ostensibly for purposes of correlation by XMPP-Grid Platforms for intrusion detection, could be misused by a broader set of XMPP-Grid Platforms which hitherto have been performing specific roles with strict well-defined separation of duties.

Care needs to be taken by deployers of XMPP-Grid to ensure that the information published by XMPP-Grid Platforms does not violate agreements with end users or local and regional laws and regulations. This can be accomplished either by configuring XMPP-Grid Platforms to not publish certain information or by restricting access to sensitive data to trusted XMPP-Grid Platforms. That is, the easiest means to ensure privacy or protect sensitive data, is to omit or not share it at all.

Another consideration for deployers is to enable end-to-end encryption to ensure the data is protected from the data layer to data layer and thus protect it from the transport layer.

10. Acknowledgements

The authors would like to acknowledge the contributions, authoring and/or editing of the following people: Joseph Salowey, Lisa Lorenzin, Clifford Kahn, Henk Birkholz, Jessica Fitzgerald-McKay, Steve Hanna, and Steve Venema. In addition, we want to thank Takeshi Takahashi, Panos Kampanakis, Adam Montville, Chris Inacio, and Dave Cridland for reviewing and providing valuable comments.

11. References

11.1. Normative References

[I-D.ietf-sacm-terminology]


11.2. Informative References


Cam-Winget, et al. Expires August 12, 2018

Authors’ Addresses

Nancy Cam-Winget (editor)
Cisco Systems
3550 Cisco Way
San Jose, CA  95134
USA

Email: ncamwing@cisco.com

Syam Appala
Cisco Systems
3550 Cisco Way
San Jose, CA  95134
USA

Email: syam1@cisco.com

Scott Pope
Cisco Systems
5400 Meadows Road
Suite 300
Lake Oswego, OR  97035
USA

Email: scottp@cisco.com

Peter Saint-Andre
Mozilla

Email: stpeter@mozilla.com
Abstract

This document describes how to use the Extensible Messaging and Presence Protocol (XMPP) to collect and distribute security-relevant information between network-connected devices. To illustrate the principles involved, this document describes such a usage for the Incident Object Description Exchange Format (IODEF).

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 https://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 December 28, 2018.

Copyright Notice

Copyright (c) 2018 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 (https://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
1. Introduction

This document describes "XMPP-Grid": a method for using the Extensible Messaging and Presence Protocol (XMPP) [RFC6120] to collect and distribute security-relevant information among network platforms, endpoints, and any other network-connected device. Among other things, XMPP provides a publish-subscribe service [XEP-0060] that acts as a broker, enabling control-plane functions by which entities can discover available information to be published or consumed. Although such information can take the form of any structured data (XML, JSON, etc.), this document illustrates the principles of XMPP-Grid with examples that use the Incident Object Description Exchange Format (IODEF) [RFC7970].

2. Terminology

This document uses XMPP terminology defined in [RFC6120] and [XEP-0060] as well as Security Automation and Continuous Monitoring (SACM) terminology defined in [I-D.ietf-sacm-terminology]. Because the intended audience for this document is those who implement and deploy security reporting systems, in general the SACM terms are used...
Broker: In SACM, a specific type of controller containing control plane functions; as used here, the term refers to an XMPP publish-subscribe service.

Broker Flow: In SACM, a method by which security-related information is published and consumed in a mediated fashion through a Broker. In this flow, the Broker handles authorization of Consumers and Providers to Topics, receives messages from Providers, and delivers published messages to Consumers.

Consumer: In SACM, an entity that contains functions to receive information from other components; as used here, the term refers to an XMPP publish-subscribe Subscriber.

Controller: In SACM, a "component containing control plane functions that manage and facilitate information sharing or execute on security functions"; as used here, the term refers to an XMPP server, which provides core message delivery [RFC6120] used by publish-subscribe entities.

Node: The XMPP term for a Topic.

Platform: Any entity that connects to the XMPP-Grid in order to publish or consume security-related data.

Provider: In SACM, an entity that contains functions to provide information to other components; as used here, the term refers to an XMPP publish-subscribe Publisher.

Publisher: The XMPP term for a Provider.

Publish-Subscribe Service: The XMPP term for the kind Broker discussed here.

Subscriber: The XMPP term for a Consumer.

Topic: A contextual information channel created on a Broker at which messages generated by a Provider are propagated in real time to one or more Consumers. Each Topic is limited to a specific type and format of security data (e.g., IODEF) and provides an XMPP interface by which the data can be obtained.

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. Architecture

The following figure illustrates the architecture of XMPP-Grid:

Platforms connect to the Controller (XMPP server) to authenticate and then establish appropriate authorizations and relationships (e.g., Provider or Consumer) at the Broker. The control plane messaging is established through XMPP and shown as "A" (control plane interface) in Figure 1. Authorized nodes can then share data either thru the...
Broker (shown as "B" in Figure 1) or in some cases directly (shown as "C" in Figure 1). This document focuses primarily on the Broker Flow for information sharing ("direct flow" interactions can be used for specialized purposes such as bulk data transfer, but methods for doing so are outside the scope of this document).

4. Workflow

A typical XMPP-Grid workflow is as follows:

a. A Platform with a source of security data requests connection to the XMPP-Grid via a Controller (XMPP server).

b. The Controller authenticates the Platform.

c. The Platform establishes authorized privileges (e.g. privilege to publish and/or subscribe to security data Topics) with a Broker.

d. The Platform can publish security-related data to a Topic, subscribe to a Topic, query a Topic, or any combination of these operations.

e. A Provider unicasts its Topic updates to the Grid in real time through a Broker. The Broker handles replication and distribution of the Topic to Consumers. A Provider can publish the same or different data to multiple Topics.

f. Any Platform on the Grid can subscribe to any Topics published to the Grid (as permitted by authorization policy), and as Consumers will then receive a continual, real-time stream of updates from the Topics to which it is subscribed.

The general workflow is summarized in the figure below:
<table>
<thead>
<tr>
<th>IODEF Client</th>
<th>Controller &amp; Broker</th>
<th>IODEF Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Consumer)</td>
<td></td>
<td>(Provider)</td>
</tr>
</tbody>
</table>

Establish XMPP Client Session (RFC 6120)  

Establish XMPP Client Session (RFC 6120)  

Request Topic List (XEP-0030)  

Request Topic Creation (XEP-0060)  

Query Each Topic (XEP-0030)  

Return Topic List Including Topic Type (XEP-0030)  

Subscribe to IODEF Topic (XEP-0060)  

Subscription Success (XEP-0060)  

Receive IODEF Incident (XEP-0060)  

Figure 2: IODEF Example Workflow
XMPP-Grid implementations MUST adhere to the mandatory-to-implement and mandatory-to-negotiate features as defined in [RFC6120]. Similarly, implementations MUST implement [XEP-0060] to facilitate the asynchronous sharing for information. The Service Discovery per [XEP-0030] SHOULD be implemented to facilitate the means to dynamically discover the available information (Topics) to be published or consumes.

The following sections provide protocol examples for the service discovery and publish-subscribe parts of the workflow.

5. Service Discovery

Using the XMPP service discovery extension [XEP-0030], a Controller enables Platforms to discover what information can be consumed through the Broker, and at which Topics. As an example, the Controller at ‘security-grid.example’ might provide a Broker at ‘broker.security-grid.example’ hosting a number of Topics. A Platform at ‘xmpp-grid-client@mile-host.example’ would query the Broker about its available Topics by sending an XMPP "disco#items" request to the Broker:

```xml
<iq type='get'
   from='xmpp-grid-client@mile-host.example/2EBE702A97D6'
   to='broker.security-grid.example'
   id='B3C17F7B-B9EF-4ABA-B08D-805DA9F34626'>
   <query xmlns='http://jabber.org/protocol/disco#items'/>
</iq>
```

The Broker responds with the Topics it hosts:

```xml
<iq type='result'
   from='broker.security-grid.example'
   to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
   id='B3C17F7B-B9EF-4ABA-B08D-805DA9F34626'>
   <query xmlns='http://jabber.org/protocol/disco#items'>
     <item node='NEA1'
           name='Endpoint Posture Information'
           jid='broker.security-grid.example'/>
     <item node='MILEHost'
           name='MILE Host Data'
           jid='broker.security-grid.example'/>
   </query>
</iq>
```

In order to determine the exact nature of each Topic (i.e., in order to find topics that publish incidents in the IODEF format), a Platform would send an XMPP "disco#info" request to each Topic:
The Broker responds with the "disco#info" description, which SHOULD include an XMPP Data Form [XEP-0004] including a 'pubsub#type' field that specifies the supported namespace (in this example, the IODEF namespace defined in [RFC7970]):

6. Publish-Subscribe

Using the XMPP publish-subscribe extension [XEP-0030], a Consumer subscribes to a Topic and a Provider publishes information to that Topic, which the Broker then distributes to all subscribed Consumers.

First, a Provider would create a Topic as follows:

```xml
<iq type='set' from='datasource@provider.example/F12C2EFC9BB0' to='broker.security-grid.example'
  id='A67507DF-2F22-4937-8D30-88D2F7DBA279'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <create node='MILEHost'/>
  </pubsub>
</iq>
```
Note: The foregoing example is the minimal protocol needed to create a Topic with the default node configuration on the XMPP publish-subscribe service specified in the ‘to’ address of the creation request stanza. Depending on security requirements, the Provider might need to request a non-default configuration for the node; see [XEP-0060] for detailed examples.

Unless an error occurs (see [XEP-0060] for various error flows), the Broker responds with success:

```xml
<iq type='result'
    from='broker.security-grid.example'
    to='datasource@provider.example/F12C2EFC9BB0'
    id='A67507DF-2F22-4937-8D30-88D2F7DBA279'/>
```

Second, a Consumer would subscribe as follows:

```xml
<iq type='set'
    from='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    to='broker.security-grid.example'
    id='9C6EEE9E-F09A-4418-8D68-3BA6AF852522'>
    <pubsub xmlns='http://jabber.org/protocol/pubsub'>
        <subscribe node='MILEHost'
                  jid='xmpp-grid-client@mile-host.example'/>
    </pubsub>
</iq>
```

Unless an error occurs (see [XEP-0060] for various error flows), the Broker responds with success:

```xml
<iq type='result'
    from='broker.security-grid.example'
    to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    id='9C6EEE9E-F09A-4418-8D68-3BA6AF852522'>
    <pubsub xmlns='http://jabber.org/protocol/pubsub'>
        <subscription
            node='MILEHost'
            jid='xmpp-grid-client@mile-host.example'
            subscription='subscribed'/>
    </pubsub>
</iq>
```

Third, a Provider would publish an incident as follows:
<iq type='set' 
    from='datasource@provider.example/F12C2EFC9BB0' 
    to='broker.security-grid.example' 
    id='2A17D2B8-0DAE-4A6C-85A9-C10B1B40928C'>
    <pubsub xmlns='http://jabber.org/protocol/pubsub'>
        <publish node='MILEHost'>
            <item id='8bh1g27skbg47fh9wk7'>
                <IODEF-Document version="2.00" xml:lang="en"
                    xmlns="urn:ietf:params:xml:ns:iodef-2.0"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                    xsi:schemaLocation="http://www.iana.org/assignments/xml-registry/
                    schema/iodef-2.0.xsd">
                    <Incident purpose="reporting" restriction="private">
                        <IncidentID name="csirt.example.com">492382</IncidentID>
                        <GenerationTime>2015-07-18T09:00:00-05:00</GenerationTime>
                        <Contact type="organization" role="creator">
                            <Email>
                                <EmailTo>contact@csirt.example.com</EmailTo>
                            </Email>
                        </Contact>
                    </Incident>
                </IODEF-Document>
            </item>
        </publish>
    </pubsub>
</iq>

(The payload in the foregoing example is from [RFC7970]; payloads for additional use cases can be found in [RFC8274].)

The Broker would then deliver that incident report to all Consumers who are subscribe to the Topic:
<message
from='broker.security-grid.example'
to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
id='37B3921D-4F7F-450F-A589-56119A88BC2E'>
<event xmlns='http://jabber.org/protocol/pubsub#event'>
  <items node='MILEHost'>
    <item id='iah37s6ls964gguqy47aksbx9453ks77'>
      <IODEF-Document version="2.00" xml:lang="en"
xmlns="urn:ietf:params:xml:ns:iodef-2.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.iana.org/assignments/xml-registry/
  schema/iodef-2.0.xsd">
        <Incident purpose="reporting" restriction="private">
          <IncidentID name="csirt.example.com">492382</IncidentID>
          <GenerationTime>2015-07-18T09:00:00-05:00</GenerationTime>
          <Contact type="organization" role="creator">
            <Email>
              <EmailTo>contact@csirt.example.com</EmailTo>
            </Email>
          </Contact>
        </Incident>
      </IODEF-Document>
    </item>
  </items>
</event>
</message>

7. IANA Considerations

This document has no actions for IANA.

8. Security Considerations

An XMPP-Grid Controller serves as an controlling broker for XMPP-Grid Platforms such as Enforcement Points, Policy Servers, CMDBs, and Sensors, using a publish-subscribe-search model of information exchange and lookup. By increasing the ability of XMPP-Grid Platforms to learn about and respond to security-relevant events and data, XMPP-Grid can improve the timeliness and utility of the security system. However, this integrated security system can also be exploited by attackers if they can compromise it. Therefore, strong security protections for XMPP-Grid are essential.

This section provides a security analysis of the XMPP-Grid data transfer protocol and the architectural elements that employ it, specifically with respect to their use of this protocol. Three subsections define the trust model (which elements are trusted to do
what), the threat model (attacks that can be mounted on the system),
and the countermeasures (ways to address or mitigate the threats
previously identified).

8.1. Trust Model

The first step in analyzing the security of the XMPP-Grid transport
protocol is to describe the trust model, listing what each
architectural element is trusted to do. The items listed here are
assumptions, but provisions are made in the Threat Model and
Countermeasures sections for elements that fail to perform as they
were trusted to do.

8.1.1. Network

The network used to carry XMPP-Grid messages (i.e., the underlying
network transport layer over which XMPP runs) is trusted to:

- Perform best effort delivery of network traffic

The network used to carry XMPP-Grid messages is not expected
(trusted) to:

- Provide confidentiality or integrity protection for messages sent
  over it
- Provide timely or reliable service

8.1.2. XMPP-Grid Platforms

Authorized XMPP-Grid Platforms are trusted to:

- Preserve the confidentiality of sensitive data retrieved via the
  XMPP-Grid Controller

8.1.3. XMPP-Grid Controller

The XMPP-Grid Controller (including its associated Broker) is trusted
to:

- Broker requests for data and enforce authorization of access to
  this data throughout its lifecycle
- Perform service requests in a timely and accurate manner
- Create and maintain accurate operational attributes
o Only reveal data to and accept service requests from authorized parties

The XMPP-Grid Controller is not expected (trusted) to:

o Verify the truth (correctness) of data

8.1.4. Certification Authority

The Certification Authority (CA) that issues certificates for the XMPP-Grid Controller and/or XMPP-Grid Platforms (or each CA, if there are several) is trusted to:

o Ensure that only proper certificates are issued and that all certificates are issued in accordance with the CA’s policies

o Revoke certificates previously issued when necessary

o Regularly and securely distribute certificate revocation information

o Promptly detect and report any violations of this trust so that they can be handled

The CA is not expected (trusted) to:

o Issue certificates that go beyond the XMPP-Grid needs or other constraints imposed by a relying party.

8.2. Threat Model

To secure the XMPP-Grid data transfer protocol and the architectural elements that implement it, this section identifies the attacks that can be mounted against the protocol and elements.

8.2.1. Network Attacks

A variety of attacks can be mounted using the network. For the purposes of this subsection the phrase "network traffic" can be taken to mean messages and/or parts of messages. Any of these attacks can be mounted by network elements, by parties who control network elements, and (in many cases) by parties who control network-attached devices.

o Network traffic can be passively monitored to glean information from any unencrypted traffic
Even if all traffic is encrypted, valuable information can be gained by traffic analysis (volume, timing, source and destination addresses, etc.)

- Network traffic can be modified in transit
- Previously transmitted network traffic can be replayed
- New network traffic can be added
- Network traffic can be blocked, perhaps selectively
- A "Man In The Middle" (MITM) attack can be mounted where an attacker interposes itself between two communicating parties and poses as the other end to either party or impersonates the other end to either or both parties
- Resist attacks (including denial of service and other attacks from XMPP-Grid Platforms)
- Undesired network traffic can be sent in an effort to overload an architectural component, thus mounting a denial of service attack

8.2.2. XMPP-Grid Platforms

An unauthorized XMPP-Grid Platform (one which is not recognized by the XMPP-Grid Controller or is recognized but not authorized to perform any actions) cannot mount any attacks other than those listed in the Network Attacks section above.

An authorized XMPP-Grid Platform, on the other hand, can mount many attacks. These attacks might occur because the XMPP-Grid Platform is controlled by a malicious, careless, or incompetent party (whether because its owner is malicious, careless, or incompetent or because the XMPP-Grid Platform has been compromised and is now controlled by a party other than its owner). They might also occur because the XMPP-Grid Platform is running malicious software; because the XMPP-Grid Platform is running buggy software (which can fail in a state that floods the network with traffic); or because the XMPP-Grid Platform has been configured improperly. From a security standpoint, it generally makes no difference why an attack is initiated. The same countermeasures can be employed in any case.

Here is a list of attacks that can be mounted by an authorized XMPP-Grid Platform:

- Cause many false alarms or otherwise overload the XMPP-Grid Controller or other elements in the network security system
(including human administrators) leading to a denial of service or disabling parts of the network security system

- Omit important actions (such as posting incriminating data), resulting in incorrect access

- Use confidential information obtained from the XMPP-Grid Controller to enable further attacks (such as using endpoint health check results to exploit vulnerable endpoints)

- Advertise data crafted to exploit vulnerabilities in the XMPP-Grid Controller or in other XMPP-Grid Platforms, with a goal of compromising those systems

- Issue a search request or set up a subscription that matches an enormous result, leading to resource exhaustion on the XMPP-Grid Controller, the publishing XMPP-Grid Platform, and/or the network

- Establish a communication channel using another XMPP-Grid Platform’s session-id

Dependencies of or vulnerabilities of authorized XMPP-Grid Platforms can be exploited to effect these attacks. Another way to effect these attacks is to gain the ability to impersonate an XMPP-Grid Platform (through theft of the XMPP-Grid Platform’s identity credentials or through other means). Even a clock skew between the XMPP-Grid Platform and XMPP-Grid Controller can cause problems if the XMPP-Grid Platform assumes that old XMPP-Grid Platform data deserves to be ignored.

### 8.2.3. XMPP-Grid Controllers

An unauthorized XMPP-Grid Controller (one which is not trusted by XMPP-Grid Platforms) cannot mount any attacks other than those listed in the Network Attacks section above.

An authorized XMPP-Grid Controller can mount many attacks. Similar to the XMPP-Grid Platform case described above, these attacks might occur because the XMPP-Grid Controller is controlled by a malicious, careless, or incompetent party (either an XMPP-Grid Controller administrator or an attacker who has seized control of the XMPP-Grid Controller). They might also occur because the XMPP-Grid Controller is running malicious software, because the XMPP-Grid Controller is running buggy software (which can fail in a state that corrupts data or floods the network with traffic), or because the XMPP-Grid Controller has been configured improperly.
All of the attacks listed for XMPP-Grid Platform above can be mounted by the XMPP-Grid Controller. Detection of these attacks will be more difficult since the XMPP-Grid Controller can create false operational attributes and/or logs that imply some other party created any bad data.

Additional XMPP-Grid Controller attacks can include:

- Expose different data to different XMPP-Grid Platforms to mislead investigators or cause inconsistent behavior
- Mount an even more effective denial of service attack than a single XMPP-Grid Platform could
- Obtain and cache XMPP-Grid Platform credentials so they can be used to impersonate XMPP-Grid Platforms even after a breach of the XMPP-Grid Controller is repaired
- Obtain and cache XMPP-Grid Controller administrator credentials so they can be used to regain control of the XMPP-Grid Controller after the breach of the XMPP-Grid Controller is repaired

Dependencies of or vulnerabilities of the XMPP-Grid Controller can be exploited to obtain control of the XMPP-Grid Controller and effect these attacks.

8.2.4. Certification Authority

A Certification Authority trusted to issue certificates for the XMPP-Grid Controller and/or XMPP-Grid Platforms can mount several attacks:

- Issue certificates for unauthorized parties, enabling them to impersonate authorized parties such as the XMPP-Grid Controller or an XMPP-Grid Platform. This can lead to all the threats that can be mounted by the certificate’s subject.
- Issue certificates without following all of the CA’s policies. Because this can result in issuing certificates that can be used to impersonate authorized parties, this can lead to all the threats that can be mounted by the certificate’s subject.
- Fail to revoke previously issued certificates that need to be revoked. This can lead to undetected impersonation of the certificate’s subject or failure to revoke authorization of the subject, and therefore can lead to all of the threats that can be mounted by that subject.
- Fail to regularly and securely distribute certificate revocation information. This can cause a relying party to accept a revoked certificate, leading to undetected impersonation of the certificate’s subject or failure to revoke authorization of the subject, and therefore can lead to all of the threats that can be mounted by that subject. It can also cause a relying party to refuse to proceed with a transaction because timely revocation information is not available, even though the transaction should be permitted to proceed.

- Allow the CA’s private key to be revealed to an unauthorized party. This can lead to all the threats above. Even worse, the actions taken with the private key will not be known to the CA.

- Fail to promptly detect and report errors and violations of trust so that relying parties can be promptly notified. This can cause the threats listed earlier in this section to persist longer than necessary, leading to many knock-on effects.

8.3. Countermeasures

Below are countermeasures for specific attack scenarios to the XMPP-Grid infrastructure.

8.3.1. Securing the XMPP-Grid Data Transfer Protocol

To address network attacks, the XMPP-Grid data transfer protocol described in this document requires that the XMPP-Grid messages MUST be carried over TLS (minimally TLS 1.2 [RFC5246]) as described in [RFC6120] and updated by [RFC7590]. The XMPP-Grid Platform MUST verify the XMPP-Grid Controller’s certificate and determine whether the XMPP-Grid Controller is trusted by this XMPP-Grid Platform before completing the TLS handshake. The XMPP-Grid Controller MUST authenticate the XMPP-Grid Platform either using the SASL EXTERNAL mechanism or using the SASL SCRAM mechanism (with the SCRAM-SHA-256-PLUS variant being preferred over the SCRAM-SHA-256 variant and SHA-256 variants [RFC7677] being preferred over SHA-1 variants [RFC5802]). XMPP-Grid Platforms and XMPP-Grid Controllers using mutual certificate-based authentication SHOULD each verify the revocation status of the other party’s certificate. All XMPP-Grid Controllers and XMPP-Grid Platforms MUST implement both SASL EXTERNAL and SASL SCRAM. The selection of which XMPP-Grid Platform authentication technique to use in any particular deployment is left to the administrator.

These protocol security measures provide protection against all the network attacks listed in the above document section except denial of service attacks. If protection against these denial of service
attacks is desired, ingress filtering, rate limiting per source IP address, and other denial of service mitigation measures can be employed. In addition, an XMPP-Grid Controller MAY automatically disable a misbehaving XMPP-Grid Platform.

8.3.2. Securing XMPP-Grid Platforms

XMPP-Grid Platforms can be deployed in locations that are susceptible to physical attacks. Physical security measures can be taken to avoid compromise of XMPP-Grid Platforms, but these are not always practical or completely effective. An alternative measure is to configure the XMPP-Grid Controller to provide read-only access for such systems. The XMPP-Grid Controller SHOULD also include a full authorization model so that individual XMPP-Grid Platforms can be configured to have only the privileges that they need. The XMPP-Grid Controller MAY provide functional templates so that the administrator can configure a specific XMPP-Grid Platform as a DHCP server and authorize only the operations and metadata types needed by a DHCP server to be permitted for that XMPP-Grid Platform. These techniques can reduce the negative impacts of a compromised XMPP-Grid Platform without diminishing the utility of the overall system.

To handle attacks within the bounds of this authorization model, the XMPP-Grid Controller MAY also include rate limits and alerts for unusual XMPP-Grid Platform behavior. XMPP-Grid Controllers SHOULD make it easy to revoke an XMPP-Grid Platform’s authorization when necessary. Another way to detect attacks from XMPP-Grid Platforms is to create fake entries in the available data (honeytokens) which normal XMPP-Grid Platforms will not attempt to access. The XMPP-Grid Controller SHOULD include auditable logs of XMPP-Grid Platform activities.

To avoid compromise of XMPP-Grid Platform, XMPP-Grid Platform SHOULD be hardened against attack and minimized to reduce their attack surface. They should be well managed to minimize vulnerabilities in the underlying platform and in systems upon which the XMPP-Grid Platform depends. Personnel with administrative access should be carefully screened and monitored to detect problems as soon as possible.

8.3.3. Securing XMPP-Grid Controllers

Because of the serious consequences of XMPP-Grid Controller compromise, XMPP-Grid Controllers need to be especially well hardened against attack and minimized to reduce their attack surface. They need to be well managed to minimize vulnerabilities in the underlying platform and in systems upon which the XMPP-Grid Controller depends. Network security measures such as firewalls or intrusion detection...
systems can be used to monitor and limit traffic to and from the
XMPP-Grid Controller. Personnel with administrative access ought to
be carefully screened and monitored to detect problems as soon as
possible. Administrators SHOULD NOT use password-based
authentication but should instead use non-reusable credentials and
multi-factor authentication (where available). Physical security
measures ought to be employed to prevent physical attacks on XMPP-
Grid Controllers.

To ease detection of XMPP-Grid Controller compromise should it occur,
XMPP-Grid Controller behavior should be monitored to detect unusual
behavior (such as a reboot, a large increase in traffic, or different
views of an information repository for similar XMPP-Grid Platforms).
XMPP-Grid Platforms should log and/or notify administrators when
peculiar XMPP-Grid Controller behavior is detected. To aid forensic
investigation, permanent read-only audit logs of security-relevant
information (especially administrative actions) should be maintained.
If XMPP-Grid Controller compromise is detected, a careful analysis
should be performed of the impact of this compromise. Any reusable
credentials that can have been compromised should be reissued.

8.3.4. Broker Access Models for Topics

The XMPP publish-subscribe specification [XEP-0060] defines five
access models for subscribing to Topics at a Broker: open, presence,
roster, authorize, and whitelist. The first model allows
uncontrolled access and the next two models are appropriate only in
instant-messaging applications. Therefore, a Broker SHOULD support
only the authorize model (under which the Topic owner needs to
approve all subscription requests and only subscribers can retrieve
data items) and the whitelist model (under which only preconfigured
Platforms can subscribe or retrieve data items). In order to ease
the deployment burden, subscription approvals and whitelist
management can be automated (e.g., the Topic "owner" can be a policy
server). The choice between "authorize" and "whitelist" as the
default access model is a matter for local service policy.

8.3.5. Limit on Search Result Size

While XMPP-Grid is designed for high scalability to 100,000s of
Platforms, an XMPP-Grid Controller MAY establish a limit to the
amount of data it is willing to return in search or subscription
results. This mitigates the threat of an XMPP-Grid Platform causing
resource exhaustion by issuing a search or subscription that leads to
an enormous result.
8.3.6.  Securing the Certification Authority

As noted above, compromise of a Certification Authority (CA) trusted to issue certificates for the XMPP-Grid Controller and/or XMPP-Grid Platforms is a major security breach. Many guidelines for proper CA security have been developed: the CA/Browser Forum’s Baseline Requirements, the AICPA/CICA Trust Service Principles, etc. The CA operator and relying parties should agree on an appropriately rigorous security practices to be used.

Even with the most rigorous security practices, a CA can be compromised. If this compromise is detected quickly, relying parties can remove the CA from their list of trusted CAs, and other CAs can revoke any certificates issued to the CA. However, CA compromise may go undetected for some time, and there’s always the possibility that a CA is being operated improperly or in a manner that is not in the interests of the relying parties. For this reason, relying parties may wish to "pin" a small number of particularly critical certificates (such as the certificate for the XMPP-Grid Controller). Once a certificate has been pinned, the relying party will not accept another certificate in its place unless the Administrator explicitly commands it to do so. This does not mean that the relying party will not check the revocation status of pinned certificates. However, the Administrator can still be consulted if a pinned certificate is revoked, since the CA and revocation process are not completely trusted.

8.4.  Summary

XMPP-Grid’s considerable value as a broker for security-sensitive data exchange distribution also makes the protocol and the network security elements that implement it a target for attack. Therefore, strong security has been included as a basic design principle within the XMPP-Grid design process.

The XMPP-Grid data transfer protocol provides strong protection against a variety of different attacks. In the event that an XMPP-Grid Platform or XMPP-Grid Controller is compromised, the effects of this compromise have been reduced and limited with the recommended role-based authorization model and other provisions, and best practices for managing and protecting XMPP-Grid systems have been described. Taken together, these measures should provide protection commensurate with the threat to XMPP-Grid systems, thus ensuring that they fulfill their promise as a network security clearing-house.
9. Privacy Considerations

XMPP-Grid Platforms can publish information about endpoint health, network access, events (which can include information about what services an endpoint is accessing), roles and capabilities, and the identity of the end user operating the endpoint. Any of this published information can be queried by other XMPP-Grid Platforms and could potentially be used to correlate network activity to a particular end user.

Dynamic and static information brokered by an XMPP-Grid Controller, ostensibly for purposes of correlation by XMPP-Grid Platforms for intrusion detection, could be misused by a broader set of XMPP-Grid Platforms which hitherto have been performing specific roles with strict well-defined separation of duties.

Care needs to be taken by deployers of XMPP-Grid to ensure that the information published by XMPP-Grid Platforms does not violate agreements with end users or local and regional laws and regulations. This can be accomplished either by configuring XMPP-Grid Platforms to not publish certain information or by restricting access to sensitive data to trusted XMPP-Grid Platforms. That is, the easiest means to ensure privacy or protect sensitive data, is to omit or not share it at all.

Another consideration for deployers is to enable end-to-end encryption to ensure the data is protected from the data layer to data layer and thus protect it from the transport layer.

10. Operations and Management Considerations

In order to facilitate the management of Providers and the onboarding of Consumers, it is helpful to generate the following ahead of time:

- Agreement between the operators of Provider services and the implementers of Consumer software regarding identifiers for common Topics (e.g., these could be registered with the XMPP Software Foundation’s registry of well-known nodes for service discovery and publish-subscribe located at <https://xmpp.org/registrar/nodes.html>).

- Security certificates (including appropriate certificate chains) for Controllers, including identification of any Providers associated with the Controllers (which might be located at subdomains).

- Consistent and secure access control policies for publishing and subscribing to Topics.
These matters are out of scope for this document but ought to be addressed by the XMPP-Grid community.

11. Acknowledgements

The authors would like to acknowledge the contributions, authoring and/or editing of the following people: Joseph Salowey, Lisa Lorenzin, Clifford Kahn, Henk Birkholz, Jessica Fitzgerald-McKay, Steve Hanna, and Steve Venema. In addition, we want to thank Takeshi Takahashi, Panos Kampanakis, Adam Montville, Chris Inacio, and Dave Cridland for reviewing and providing valuable comments.

12. References

12.1. Normative References

[I-D.ietf-sacm-terminology]


12.2. Informative References


Authors’ Addresses

Nancy Cam-Winget (editor)
Cisco Systems
3550 Cisco Way
San Jose, CA  95134
USA

Email: ncamwing@cisco.com

Syam Appala
Cisco Systems
3550 Cisco Way
San Jose, CA  95134
USA

Email: syam1@cisco.com