Definition of ROLIE CSIRT Extension
draft-ietf-mile-rolie-csirt-05

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 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 March 8, 2020.

Copyright Notice

Table of Contents

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. Information-type Extensions

3.1. The "incident" information type

When an "atom:category" element has a "scheme" attribute equal to
"urn:ietf:params:rolie:category:information-type", the "term"
attribute defines the information type of the associated resource. A
new valid "term" value for this "scheme": "incident", is described in
this section, and registered in Section 7.1.1.

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.

o Timing information: start and end times for the incident and/or
   the response.

o 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 in
is the abstract realm of an incident should be classified under this
information-type.

3.2. The "indicator" information type

When an "atom:category" element has a "scheme" attribute equal to
"urn:ietf:params:rolie:category:information-type", the "term"
attribute defines the information type of the associated resource. A
new valid "term" value for this "scheme": "indicator", is described
in this section, and registered in Section 7.1.2.

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.

4. Data format requirements

This section defines usage guidance and additional requirements
related to data formats above and beyond those specified in
[RFC8322]. The following formats are expected to be commonly used to
express software descriptor information. For this reason, this
document specifies additional requirements to ensure
interoperability.

4.1. Incident Object Description Exchange Format

4.1.1. Description

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 [RFC7970] provides further high-level
discussion and technical details.

4.1.2. Requirements

   For an Entry to be considered as a "IODEF Entry", it MUST fulfill the
   following conditions:

   o The information-type of the Entry is "indicator" or "incident".
      For a typical Entry, this is derived from the information type of
      the Feed it is contained in. For a standalone Entry, this is
      provided by an "atom:category" element.

   o The document linked to by the "href" attribute of the
      "atom:content" element is an IODEF document as per [RFC7970]

   A "IODEF Entry" MUST conform to the following requirements:

   o The value of the "type" attribute of the "atom:content" element
      MUST be "application/xml".

   o There MUST be at least one "rolie:property" with the "name"
      attribute equal to "urn:ietf:params:rolie:property:content-id" and
      the "value" attribute exactly equal to the "<Indicator-ID>" or the
      "<Incident-ID>" element in the attached IODEF document. This
      allows for ROLIE consumers to more easily search for IODEF
      documents without needing to download the document itself.

4.2. Structured Threat Information eXpression (STIX) Format

4.2.1. Description

   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 full STIX specification [stix2] provides further high-level
   discussion and technical details.

4.2.2. Requirements

   For an Entry to be considered as a "STIX Entry", it MUST fulfill the
   following conditions:

   o The information-type of the Entry is "indicator" or "incident".
      For a typical Entry, this is derived from the information type of
      the Feed it is contained in. For a standalone Entry, this is
      provided by an "atom:category" element.

   o The document linked to by the "href" attribute of the
      "atom:content" element is a STIX object as per [stix2]

A "STIX Entry" MUST conform to the following requirements:

o The value of the "type" attribute of the "atom:content" element
   MUST be "application/xml" or "application/json".

o There MUST be at least one "rolie:property" with the "name"
   attribute equal to "urn:ietf:params:rolie:property:content-id" and
   the "value" attribute exactly equal to the "<id>" element in the
   attached STIX object . This allows for ROLIE consumers to more
   easily search for STIX objects without needing to download the
   document itself.

4.3. Malware Information Sharing Platform (MISP) Format

MISP involves documentation, utilities, and formats designed to
facilitate the day-to=day duties of security operators. MISP
includes it's own data format that is used to share between MISP
features. While MISP has Feed features that can share and distribute
events, it has support for linking to other sharing methods like
ROLIE.

MISP is defined by a family of internet drafts and are actively being
worked on. With that in mind, this extension will provide non-
normative guidance on using MISP format data in ROLIE. In the
future, when the MISP format is formally published, this document
will be updated to normative requirements around MISP content.

4.3.1. Creating MISP Event Entries

MISP content should be syndicated in ROLIE using the following
guidance:

o The information-type of the Entry is "indicator". For a typical
   Entry, this is derived from the information type of the Feed it is
   contained in. For a standalone Entry, this is provided by an
   "atom:category" element.

o The document linked to by the "href" attribute of the
   "atom:content" element is a MISP Event object as per
   [I-D.dulaunoy-misp-core-format]

o The value of the "type" attribute of the "atom:content" element
   should be "application/xml".

o There should be at least one "rolie:property" with the "name"
   attribute equal to "urn:ietf:params:rolie:property:content-id" and
   the "value" attribute exactly equal to the "<uuid>" element in the
   attached MISP Event . This allows for ROLIE consumers to more

easily search for MISP Events without needing to download the
document itself.

o It is also recommended to expose information in the ROLIE Entry
   that is required and recommended to expose in the MISP Manifest
   format. This ensures better compatibility between a ROLIE Feed
   and a MISP Manifest

   * The following fields are required by the MISP draft: info,
      Orgc, timestamp, date

   * The following fields are recommended by the MISP draft:
      analysis, threat_level_id

4.3.2. MISP Feeds and Manifests

   MISP Feeds are hosted lists of MISP events, each event represented by
   its UUID. Users request Events on a one-by-one basis and are served
   the full Event on each request.

   MISP Manifest files list MISP events by their UUIDs as well, but
   provide a variety of metadata for each Event inline. After examining
   the minimized and stripped Event in the manifest, a user could search
   for the Event UUID of interest in a locally located folder of Event
   files where the file name is the UUID of the Event.

   ROLIE hosting MISP data would operate as a combination of these
   approaches. Each ROLIE Feed would contain a list of Event Entries,
   each with metadata and identifying information about a given Event.
   Should the user be interested in the Event, the Event Entry provides
   a direct link to download the full Event. In short, a ROLIE MISP
   Feed is minimally mappable to a MISP Manifest file where a resolvable
   link to the MISP Event was injected into each Event described in the
   Manifest.

   With that in mind, a MISP Feed as well as a MISP Manifest with
   attached local file list could be fully converted and hosted as a
   ROLIE repository. As a lower overhead alternative, a ROLIE server
   could simply provide a view into MISP data.

5. atom:link Extensions

   This section defines additional link relationships that
   implementations MUST support. These relationships are not registered
   in the Link Relation IANA table as their use case is too narrow.
   Each relationship is named and described.

These relations come in related pairs. The first of each pair is
expected to be more common, as they can be determined at the time
that the Entry is created. The second of each pair will often need
to be added retroactively to an Entry.

5.1. Link relations for the 'incident' information-type

If a ROLIE server supports either the incident information-types,
then these link relations MUST be support

Name	Description
indicators	Provides a link to a collection of zero or more instances of cyber security indicators that are associated with the resource.
evidence	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.
attacker	Provides a link to a collection of zero or more resources that provides a representation of the attacker.
vector	Provides a link to a collection of zero or more resources that provides a representation of the method used by the attacker.

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

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

If a ROLIE server supports the indicator information-types, then
these link relations MUST be supported.

Name	Description
incidents	Provides a link to a collection of zero or more instances of incident representations associated with the resource.

Table 2: Link Relations for Resource-Oriented Lightweight Indicator
Exchange

5.3. Link relations for both information-types

   If a ROLIE server supports either the incident or the indicator
   information-types, then these link relations MUST be supported.

```
+----------------------+-------------------------------------------+
| Name                 | Description                               |
+----------------------+-------------------------------------------+
| assessments          | Provides a link to a collection of zero   |
|                      | or more resources that represent the      |
|                      | results of executing a benchmark.         |
| reports              | Provides a link to a collection of zero   |
|                      | or more resources that represent RID      |
|                      | reports.                                  |
| traceRequests        | Provides a link to a collection of zero   |
|                      | or more resources that represent RID      |
|                      | traceRequests.                            |
| investigationRequests | Provides a link to a collection of zero  |
|                      | or more resources that represent RID      |
|                      | investigationRequests.                    |
+----------------------+-------------------------------------------+
```

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

6. atom:category Extensions

6.1. Newly registered category values

   This document registers two additional registered atom:category
   names: 'urn:ietf:params:rolie:category:csirt:iodef:purpose' and
   'urn:ietf:params:rolie:category:csirt:iodef:restriction'. These
   categories expose important information from inside the attached
   IODEF document. The Purpose and Restriction elements are often used
   to sort or cateogrize IODEF documents, and in some use cases,
   determine the security and access permissions of the document.

   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.

6.2. 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.

7. IANA Considerations

7.1. 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> .

7.1.1. incident information-type

The entry is as follows:

    name: incident

    index: TBD

    reference: This document, Section 3.1

7.1.2. indicator information-type

The entry is as follows:

    name: indicator

    index: TBD

    reference: This document, Section 3.2

7.2. atom:category scheme registrations

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

7.2.1. category:csirt:iodef:purpose

   The entry is as follows:

      name: category:csirt:iodef:purpose

      Extension IRI: urn:ietf:params:rolie:category:csirt:iodef:purpose

      Reference: This document, Section 6.1

      Subregistry: None

7.2.2. category:csirt:iodef:restriction

   The entry is as follows:

      name: category:csirt:iodef:restriction

      Extension IRI:
      urn:ietf:params:rolie:category:csirt:iodef:restriction

      Reference: This document, Section 6.1

      Subregistry: None

8. 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.

When sharing IODEF 2 documents using a ROLIE server, care should be
taken to seperate IODEF Entries into different workspaces based on
the "restriction" attribute of the IODEF Document (and therefore the
restriction property in ROLIE). Security and access controls are
most effectively deployed at the workspace level, as such, keeping
private and need-to-know IODEF documents in their own workspace helps
prevent unintended information leakage.

9. Normative References

[I-D.dulaunoy-misp-core-format]
          Dulaunoy, A. and A. Iklody, "MISP core format", draft-
          dulaunoy-misp-core-format-07 (work in progress), February
          2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
          Requirement Levels", BCP 14, RFC 2119,
          DOI 10.17487/RFC2119, March 1997,
          <https://www.rfc-editor.org/info/rfc2119>.

[RFC4287] Nottingham, M., Ed. and R. Sayre, Ed., "The Atom
          Syndication Format", RFC 4287, DOI 10.17487/RFC4287,
          December 2005, <https://www.rfc-editor.org/info/rfc4287>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2",
          FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007,
          <https://www.rfc-editor.org/info/rfc4949>.

[RFC5023] Gregorio, J., Ed. and B. de hOra, Ed., "The Atom
          Publishing Protocol", RFC 5023, DOI 10.17487/RFC5023,
          October 2007, <https://www.rfc-editor.org/info/rfc5023>.

[RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident
          Object Description Exchange Format", RFC 5070,
          DOI 10.17487/RFC5070, December 2007,
          <https://www.rfc-editor.org/info/rfc5070>.

[RFC7970] Danyliw, R., "The Incident Object Description Exchange
          Format Version 2", RFC 7970, DOI 10.17487/RFC7970,
          November 2016, <https://www.rfc-editor.org/info/rfc7970>.

[RFC8322] Field, J., Banghart, S., and D. Waltermire, "Resource-
          Oriented Lightweight Information Exchange (ROLIE)",
          RFC 8322, DOI 10.17487/RFC8322, February 2018,
          <https://www.rfc-editor.org/info/rfc8322>.

   [stix2]   Organization for the Advancement of Structured Information
               Standards (OASIS) Cyber Threat Intelligence (CTI)
               Technical Committee, "Structured Threat Information
               Expression 2.0", July 2017, <https://oasis-open.github.io/
               cti-documentation/resources#stix-20-specification>.

Appendix A. Examples of Use

   Use of this extension in a ROLIE repository will not typically change
   that repository's operation. As such, the general examples provided
   by the ROLIE core document would serve as examples. Provided below
   is a sample incident ROLIE entry containing an IODEF document:

```
<?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">
  <id>f762c77c-057d-45c9-b805-677ab89aaf7c</id>
  <title>Sample Incident</title>
  <published>2018-09-04T18:13:51.0Z</published>
  <updated>2019-08-05T18:13:51.0Z</updated>
  <summary>A document containing an indicator of comprimise. </summary>
  <link rel="self" href="http://www.example.org/rolie/CSIRT/123456"/>
  <link rel="feed" href="http://www.example.org/rolie/CSIRT/"/>
  <rolie:property name=urn:ietf:params:rolie:property:content-id
      value="id847201"/>
  <category
      scheme="urn:ietf:params:rolie:category:information-type"
      term="incident"/>
  <rolie:format
      ns="urn:ietf:params:xml:ns:iodef-2.0"/>
  <content type="application/xml"
      src="http://www.example.org/rolie/csirt/123456/data"/>
</entry>
```

   Below is a sample indicator ROLIE entry containing a STIX document:

```xml
<?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">
  <id>0c99df51-767f-4940-8a09-c4b607b6fe21</id>
  <title>Sample Indicator</title>
  <published>2018-09-04T18:13:51.0Z</published>
  <updated>2019-08-05T18:13:51.0Z</updated>
  <summary>A document containing an incident report. </summary>
  <link rel="self" href="http://www.example.org/rolie/CSIRT/654321"/>
  <link rel="feed" href="http://www.example.org/rolie/CSIRT/"/>
  <rolie:property name=urn:ietf:params:rolie:property:content-id
      value="exmaple:indicator:654321"/>
  <category
      scheme="urn:ietf:params:rolie:category:information-type"
      term="indicator"/>
  <rolie:format
      ns=http://stix.mitre.org/XMLSchema/core/1.2/stix_core.xsd"/>
  <content type="application/xml"
      src="http://www.example.org/rolie/csirt/654321/data"/>
</entry>
```

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