          Guidelines and Template for Defining Extensions to the
           Incident Object Description Exchange Format (IODEF)

Abstract

   This document provides guidelines for extensions to the Incident
   Object Description Exchange Format (IODEF) described in RFC 5070 for
   exchange of incident management data, and it contains a template for
   Internet-Drafts describing those extensions, in order to ease the
   work and improve the quality of extension descriptions.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Not all documents
   approved by the IESG are a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6684.

Table of Contents

1. Introduction

   In the five years since the specification of IODEF [RFC5070], the
   threat environment has evolved, as has the practice of cooperative
   network defense. These trends, along with experience gained through
   implementation and deployment, have indicated the need to extend
   IODEF. This document provides guidelines for defining these
   extensions. It starts by describing the applicability of IODEF
   extensions, and the IODEF extension mechanisms, before providing a
   section (Appendix A) that contains a template to be the starting
   point for any future Internet-Draft about an IODEF extension.

   This document is designed to give guidance on the extension of IODEF,
   especially for those extension authors who may be new to the IETF
   process. Nothing in this document should be construed as defining
   policies for the definition of these extensions.

   At publication time, the Managed Incident Lightweight Exchange (MILE)
   working group of the IETF provides a home for work on IODEF
   extensions that do not otherwise have a natural home. IODEF
   extensions that require the expertise of other IETF working groups or
   other standards development organizations may be done within those
   groups with consultation of IODEF experts, such as those appointed
   for review as in [RFC6685].

2. Applicability of Extensions to IODEF

   Before deciding to extend IODEF, the first step is to determine
   whether an IODEF extension is a good fit for a given problem. There
   are two sides to this question:

   1. Does the problem involve the reporting or sharing of
       observations, indications, or other information about an
       incident, whether in progress or completed, hypothetical or real?
       "Incident" is defined in the terminology for the original IODEF
       requirements [RFC3067]: an event that involves a security
       violation, whether a single attack of a group thereof. If the
       answer to this question is unequivocally "No", then IODEF is
       probably not a good choice as a base technology for the
       application area.

   2. Can IODEF adequately represent information about the incident
       without extension? IODEF has a rich set of incident-relevant
       classes. If, after detailed examination of the problem area and
       the IODEF specification, and consultation with IODEF experts, the
       answer to this question is "Yes", then extension is not
       necessary.

   Examples of such extensions to IODEF might include the following:

   o Leveraging existing work in describing aspects of incidents to
      make IODEF more expressive, by standardized reference to external
      information bases about incidents and incident-related information

   o Allowing the description of new types of entities (e.g., related
      actors) or new types of characteristics of entities (e.g.,
      information related to financial services) involved in an IODEF
      incident report

   o Allowing the representation of new types of indicators,
      observables, or incidents in an IODEF incident report

   o Allowing additional semantic or metadata labeling of IODEF
      Documents (e.g., for handling or disposition instructions, or
      compliance with data protection and data retention regulations)

3. Selecting a Mechanism for IODEF Extension

   IODEF was designed to be extended through any combination of the
   following:

   1. extending the enumerated values of Attributes, per Section 5.1 of
       [RFC5070];

2.   class extension through AdditionalData or RecordItem elements,
     per Section 5.2 of [RFC5070]; and/or

3.   containment of the IODEF Document element within an external XML
     Document, itself containing extension data, as done by Real-time
     Inter-network Defense (RID) [RFC6545].

Note that in this final case, the extension will not be directly
interoperable with IODEF implementations, and it must "unwrap" the
IODEF document from its container; nevertheless, this may be
appropriate for certain use cases involving integration of IODEF
within external schemas. Extensions using containment of an IODEF
Document are not further treated in this document, though the
document template in Appendix A may be of some use in defining them.

Certain attributes containing enumerated values within certain IODEF
elements may be extended. For an attribute named "foo", this is
achieved by giving the value of "foo" as "ext-value" and adding a new
attribute named "ext-foo" containing the extended value. The
attributes that can be extended this way are limited to the
following, denoted in 'Element@attribute' format, referencing the
section in which they are defined in [RFC5070]:

    Incident@purpose, Section 3.2
    AdditionalData@dtype, Section 3.6
    Contact@role, Section 3.7
    Contact@type, Section 3.7
    RegistryHandle@registry, Section 3.7.1
    Impact@type, Section 3.10.1
    TimeImpact@metric, Section 3.10.2
    TimeImpact@duration, Section 3.10.2
    HistoryItem@action, Section 3.11.1
    Expectation@action, Section 3.13
    System@category, Section 3.15
    Counter@type, Section 3.16.1
    Counter@duration, Section 3.16.1
    Address@category, Section 3.16.2
    NodeRole@category, Section 3.16.3
    RecordPattern@type, Section 3.19.2
    RecordPattern@offsetunit, Section 3.19.2
    RecordItem@dtype, Section 3.19.3

Note that this list is current as of publication time; the set of
IODEF data types may be extended by future specifications that update
[RFC5070].

An example definition of an attribute extension is given in
Appendix B.

   IODEF Documents can contain extended scalar or XML data using an
   AdditionalData element or a RecordItem element. Scalar data
   extensions must set the "dtype" attribute of the containing element
   to the data type to reference one of the IODEF data types as
   enumerated in Section 2 of [RFC5070], and it should use the "meaning"
   and "formatid" attributes to explain the content of the element.

   XML extensions within an AdditionalData or RecordItem element use a
   dtype of "xml", and they should define a schema for the topmost
   containing element within the AdditionalData or RecordItem element.
   An example definition of an element definition is given in
   Appendix C.

   When adding elements to the AdditionalData section of an IODEF
   document, an extension's namespace and schema should be registered
   with IANA; see Appendix A.6 for details.

4. Security Considerations

   This document raises no security issues itself. Extensions defined
   using the template in Appendix A need to provide an analysis of
   security issues they may raise. See Appendix A.5 for details.

5. Acknowledgments

   Thanks to David Black, Benoit Claise, Martin Duerst, Eran Hammer, Tom
   Millar, Kathleen Moriarty, Peter Saint-Andre, Robert Sparks, Takeshi
   Takahashi, Sean Turner, Samuel Weiler, and Peter Yee for their
   reviews and comments. This work is materially supported by the
   European Union Seventh Framework Program under grant agreement 257315
   (DEMONS).

6. References

6.1. Normative References

   [RFC5070]   Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident
               Object Description Exchange Format", RFC 5070,
               December 2007.

6.2. Informative References

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC3067]   Arvidsson, J., Cormack, A., Demchenko, Y., and J. Meijer,
               "TERENA'S Incident Object Description and Exchange Format
               Requirements", RFC 3067, February 2001.

   [RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC
              Text on Security Considerations", BCP 72, RFC 3552,
              July 2003.

   [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
              IANA Considerations Section in RFCs", BCP 26, RFC 5226,
              May 2008.

   [RFC5706] Harrington, D., "Guidelines for Considering Operations and
              Management of New Protocols and Protocol Extensions",
              RFC 5706, November 2009.

   [RFC6545] Moriarty, K., "Real-time Inter-network Defense (RID)",
              RFC 6545, April 2012.

   [RFC6685] Trammell, B., "Expert Review for Incident Object
              Description Exchange Format (IODEF) Extensions in IANA XML
              Registry", RFC 6685, July 2012.

Appendix A. Document Template

   The document template given in this section is provided as a starting
   point for writing an Internet-Draft describing an IODEF extension.
   RFCs are subject to additional formatting requirements and must
   contain additional sections not described in this template; consult
   the RFC Editor style guide
   (http://www.rfc-editor.org/styleguide.html) for more information.

   This template is informational in nature; in case of any future
   conflict with RFC Editor requirements for Internet-Drafts, those
   requirements take precedence.

A.1. Introduction

   The Introduction section lays out the problem being solved by the
   extension, and motivates the development and deployment of the
   extension.

A.2. Terminology

   The Terminology section introduces and defines terms specific to the
   document. Terminology from [RFC5070] or [RFC6545] should be
   referenced in this section, but not redefined or copied. If
   [RFC2119] terms are used in the document, this should be noted in the
   Terminology section.

A.3. Applicability

   The Applicability section defines the use cases to which the
   extension is applicable, and it details any requirements analysis
   done during the development of the extension. The primary goal of
   this section is to allow readers to see if an extension is indeed
   intended to solve a given problem. This section should also define
   and restrict the scope of the extension, as appropriate, by pointing
   out any non-obvious situations to which it is not intended to apply.

   In addition to defining the applicability, this section may also
   present example situations, which should then be detailed in the
   examples section, below.

A.4. Extension Definition

   This section defines the extension.

   Extensions to enumerated types are defined in one subsection for each
   attribute to be extended, enumerating the new values with an
   explanation of the meaning of each new value. An example enumeration
   extension is shown in Appendix B, below.

   Element extensions are defined in one subsection for each element, in
   top-down order, from the element contained within AdditionalData or
   RecordItem; an example element extension is shown in Appendix C,
   below. Each element should be described by a Unified Modeling
   Language (UML) diagram as in Figure 1, followed by a description of
   each of the attributes, and a short description of each of the child
   elements. Child elements should then be defined in a subsequent
   subsection, if not already defined in the IODEF Document itself, or
   in another referenced IODEF extension document.

```
   +--------------------+
   | Element            |
   +--------------------+
   | TYPE attribute0    |<>----------[ChildExactlyOne]
   | TYPE attribute1    |<>--{0..1}--[ChildZeroOrOne]
   |                    |<>--{0..*}--[ChildZeroOrMore]
   |                    |<>--{1..*}--[ChildOneOrMore]
   +--------------------+
```
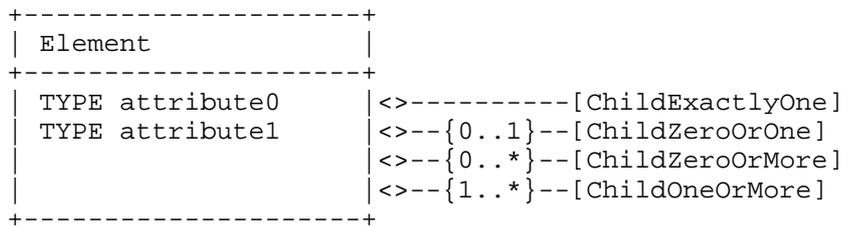
                   Figure 1: Example UML Element Diagram

   Elements containing child elements should indicate the multiplicity
   of those child elements, as shown in the figure above. Allowable
   TYPEs are enumerated in Section 2 of [RFC5070].

A.5. Security Considerations

   Any security considerations [RFC3552] raised by this extension or its
   deployment should be detailed in this section. Guidance should focus
   on ensuring the users of this extension do so in a secure fashion,
   with special attention to non-obvious implications of the
   transmission of the information represented by this extension.
   [RFC3552] may be a useful reference in determining what to cover in
   this section. This section is required by the RFC Editor.

   It should also be noted in this section that the security
   considerations for IODEF [RFC5070] apply to the extension as well.

A.6. IANA Considerations

   Any IANA considerations [RFC5226] for the document should be detailed
   in this section. Note that IODEF extension documents will generally
   register new namespaces and schemas. In addition, this section is
   required by the RFC Editor, so if there are no IANA considerations,
   the section should exist and contain the text "this document has no
   actions for IANA".

   IODEF Extensions that represent an enumeration should reference an
   existing IANA registry or subregistry for the values of that
   enumeration. If no such registry exists, this section should define
   a new registry to hold the enumeration's values and define the
   policies by which additions may be made to the registry.

   IODEF Extensions adding elements to the AdditionalData section of an
   IODEF Document should register their own namespaces and schemas for
   extensions with IANA; therefore, this section should contain at least
   a registration request for the namespace and the schema, as follows,
   modified as appropriate for the extension:

   Registration request for the IODEF My-Extension namespace:

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

     Registrant Contact: Refer here to the Authors' Addresses section of
   the document, or to an organizational contact in the case of an
   extension supported by an external organization.

     XML: None

   Registration request for the IODEF My-Extension XML schema:

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

     Registrant Contact: Refer here to the Authors' Addresses section of
   the document, or to an organizational contact in the case of an
   extension supported by an external organization.

     XML: Refer here to the XML Schema in Appendix A of the document, or
   to a well-known external reference in the case of an extension with
   an externally defined schema.

A.7. Manageability Considerations

   If any of the operational and/or management considerations listed in
   Appendix A of [RFC5706] apply to the extension, address them in this
   section. If no such considerations apply, this section can be
   omitted.

A.8. Appendix A: XML Schema Definition for Extension

   The XML Schema describing the elements defined in the Extension
   Definition section is given here. Each of the examples in
   Appendix A.9 will be verified to validate against this schema by
   automated tools.

A.9. Appendix B: Examples

   This section contains example IODEF Documents illustrating the
   extension. If example situations are outlined in the Applicability
   section, documents for those examples should be provided in the same
   order as in the Applicability section. Example documents will be
   tested to validate against the schema given in the appendix.

Appendix B. Example Enumerated Type Extension Definition: Presentation
             Action

   This example extends the IODEF Expectation element to represent the
   expectation that a slide deck be derived from the IODEF Incident, and
   that a presentation be given by the recipient's organization thereon.

   Attribute: Expectation@action

   Extended value(s): give-a-presentation

   Value meaning: generate a slide deck from the provided incident
   information and give a presentation thereon.

   Additional considerations: the format of the slide deck is left to
   the recipient to determine in accordance with its established
   practices for the presentation of incident reports.

Appendix C. Example Element Definition: Test

   This example defines the Test class for labeling IODEF test data.

   The Test class is intended to be included within an AdditionalData
   element in an IODEF Document. If a Test element is present, it
   indicates that an IODEF Document contains test data, not a
   information about a real incident.

The Test class contains information about how the test data was
generated.

```
                +--------------------+
                | Test               |
                +--------------------+
                | ENUM category      |
                | STRING generator   |
                |                    |
                |                    |
                |                    |
                +--------------------+
```
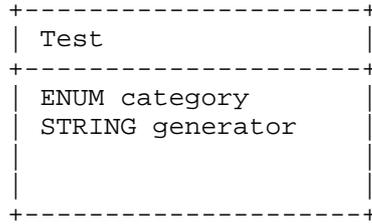
                 Figure 2: The Test Class

The Test class has two attributes:

category: Required. ENUM. The type of test data. The permitted
   values for this attribute are shown below. The default value is
   "unspecified".

   1. unspecified. The document contains test data, but no further
       information is available.

   2. internal. The test data is intended for the internal use of
       an implementor, and it should not be distributed or used
       outside the context in which it was generated.

   3. unit. The test data is intended for unit testing of an
       implementation, and it may be included with the implementation
       to support this as part of the build and deployment process.

   4. interoperability. The test data is intended for
       interoperability testing of an implementation, and it may be
       freely shared to support this purpose.

   generator: Optional. STRING. A free-form string identifying the
      person, entity, or program that generated the test data.

Author's Address

   Brian Trammell
   Swiss Federal Institute of Technology Zurich
   Gloriastrasse 35
   8092 Zurich
   Switzerland

   Phone: +41 44 632 70 13
   EMail: trammell@tik.ee.ethz.ch