Individual Submission
Internet-Draft
Intended status: Standards Track
Expires: March 25, 2012

K. Goodier
L-3 Com
D. Rajnovic
Cisco

September 22, 2011

# Guidelines for Extensions to IODEF for Managed Incident Lightweight Exchange
## draft-goodier-mile-data-markers-00.txt

Abstract

This document provides extensions to Managed Incident Lightweight Exchange (MILE). MILE describes a subset of Incident Object Description Exchange Format (IODEF) defined in RFC 5070. The Data Markers extension is aimed at exchanging data tags or markers that label categories of information that have significance in the exchange of incident information. These data marker extension is aimed at exchanging data tags or markers that label information exchanged during incident handling. Data markers include sensitivity and data handling requirements that can prevent possible criminal errors in mismarking data. Both network and information security incidents typically result in the loss of service, data, and resources both human and system. Existing extensions to the IODEF-Document Class for Reporting Phishing [RFC 5901] have already been introduced for network security incidents. Data markers introduce extensions for information security incidents so that network providers and Computer Security Incident Response Teams (CSIRT) are equipped and ready to assist in communicating and tracing security incidents with tools and procedures in place before the occurrence of an attack. Data Markers also support Real-time Inter-network Defense (RID) [RFC 6045] that outlines a proactive inter-network communication method to facilitate sharing incident handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident handling solution. Combining these capabilities in a communication system provides a way to achieve higher security levels on networks. Policy guidelines for handling incidents are recommended and can be agreed upon by a consortium using the security recommendations and considerations.

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 March 25, 2012.

Table of Contents

## 1. Introduction

Guidance has improved for the handling of privacy and other data markers to ensure the consistent application of security controls in profiled implementations. Organizations require help from data marking parties to digitally define the related context and semantics. Rapid incident detection and coordination requires automation. Increases in internet engineering outsourcing via cloud services requires tighter security and knowledge on how data is protected and incidents that could affect that data. It is critical to have automated means to both detect and mitigate/stop attack traffic while augmenting the governance of any internet-based enterprise. Enterprise data marking standards that secure cyberspace particularly within private and hybrid networks require governance methodologies that enable a workforce who has a responsibility to locate and retrieve data in support of Lines of Businesses (LoBs) and specific missions. Data markers provide additional semantic or metadata labeling of IODEF Documents (e.g., for handling or disposition instructions, or compliance with data protection and data retention regulations).

### 1.1. Terminology

Data marker attributes containing enumerated values within IODEF elements may be further extended. For a data marker attribute named "foo", this is achieved by giving the value of "foo" as "ext-marker-value", and adding a new attribute named "ext-marker-foo" containing the extended value. The attributes which can be extended in this way are defined in [RFC5070], and limited by these values.

## 2. Applicability of Data Marker 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 answers to this question for data markers:

1. Data markers are critical to the reporting or sharing of information about an incident.

2. Without a data makers extension, IODEF can not adequately represent information about an incident.

### 2.1. Applicability

The five standard use cases that apply to the data markers extension follow:





1. Use Case 1:Information Sharing

2. Use Case 2:Incident Query

3. Use Case 3:Investigation Request-Results Sent

4. Use Case 4:Investigation Request-Request Sent

5. Use Case 5:Trace Back Request

Use Case 1: Information Sharing: An incident type is identified and marked and CSIRTs would like to share that information with other CSIRTs. The incident information may be a list of IP addresses known to be malicious or a type of an attack described (for example) in MAEC and embedded in an IODEF document. In this use case, a central authority, US CERT, may have knowledge of several instances of an attack type for which the supported community should be notified to increase awareness and detection capabilities for the attack type or sources. Information Sharing Flow: US CERT generates an IODEF document, using the relevant SCAP and marked data information sources, and sends a RID Report message out to all Agency CSIRTs with one or more attack type descriptions or information about malicious

entities. No response is required for this communication type.

Use Case 2: Incident Query: An incident query communication is used when one CSIRT would like to know if a type of attack has been detected by other CSIRTs. The information provided back can be limited to descriptions of the attack without providing source and destination information if that data is marked as controlled or classified. This use case is sending the request to US CERT because they may have a broad knowledge set of attack types within the government sector to share with Agency CSIRTs. Incident Query Flow: An Agency CSIRT sends an appropriately marked IncidentQuery to US CERT. US CERT responds with an appropriately marked Report message.

Use Case 3: Investigation Request-Results Sent: An incident is detected by a CSIRT and further investigation is required to identify and mitigate or stop the attack. In this use case instance, the Agency CSIRT will detect and data mark the incident. It could be identified by any CSIRT including US CERT or the Provider CSIRT in other use cases. Investigation Request Flow: An Agency CSIRT detects an incident. The source of the incident is identified using SCAP and event information and an IODEF document with data markers with data markers is generated. The IODEF document is sent to the Provider CSIRT in a RID Investigation message using the appropriate transport protocol and data markers. The Provider CSIRT decides to work on the incident investigation, then sends the proper ly data marked Result message when the investigation is complete. Note: The Result message





can contain the information deemed appropriate for sharing with the Agency CSIRT. Data markers for policy and privacy considerations relative to the incident are required. In this use case, the Provider CSIRT sends the full investigation Report including the source of the attack and the action taken to stop the attack, traffic from the source address was blocked.

Use Case 4: Investigation Request-Request Sent: An incident is detected by a CSIRT and further investigation is required to identify and mitigate or stop the attack. In this use case instance, the Agency CSIRT will detect the incident. It could be identified by any CSIRT including US CERT or the Provider CSIRT in other use cases. Investigation Request Flow: An Agency CSIRT detects an incident. The source of the incident is identified using SCAP and event information and an IODEF document with data markers is generated. The IODEF

document is sent to the Provider CSIRT in a RID Investigation message using the appropriate transport protocol and data markers. The Provider CSIRT is unable to work on the Investigation request, a RequestAuthorization message is sent to the Agency CSIRT to notify them of the inability to respond at this time. The Agency CSIRT takes an action to block the source address from accessing the application that was targeted using the tools available to them from the Provider.

Use Case 5: Trace Back Request: In the case where the source of an incident is unknown (possibly spoofed), the ability to iteratively track an incident through providers or networks may be necessary. This communication flow is similar to the Investigation request, but could involve multiple CSIRTs until a source is found or a party does not have the resources to participate. The actions taken in this case may be close to the source of an attack or downstream Provider depending on who cooperates and marks data. This use case just describes one of the many possible flows that could occur in the trace back request. Trace Back Request Flow: An Agency CSIRT detects an incident using event information and the appropriate information for that event (application server is targeted in a DDoS attack). The Agency CSIRT generates an IODEF document and encapsulates it in a RID wrapper with data markers for a TraceRequest. The TraceRequest is sent to the upstream to their Provider's CSIRT. The Provider CSIRT confirms receipt with a RequestAuthorization message indicating that this can be looked at now by the Provider CSIRT. The investigation begins at the Provider CSIRT, and the next upstream provider has been found (where the traffic is originating), a TraceRequest message is sent to the next Provider CSIRT. The next Provider CSIRT sends a RequestAuthorization response to both the Agency CSIRT (originator of request) and the Provider CSIRT who sent the TraceRequest. The response provided in the AuthorizationRequest is yes and the incident will be investigated. The investigation has





completed and a Result message is sent to the Agency CSIRT. The information provided in the report must be marked according to the policy of the CSIRT that sends the report. In this use case, the information provided is limited to a description of the actions taken with appropriate data markers, the traffic has been rate limited with no information on the true source of the attack.

## 2.2. Extension Definition

This section defines the data markers 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 the new value. An example enumeration extension is shown in Section 2.2.2, 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 Section 2.2.3, below. Each element should be described by a 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 MILE extension document.

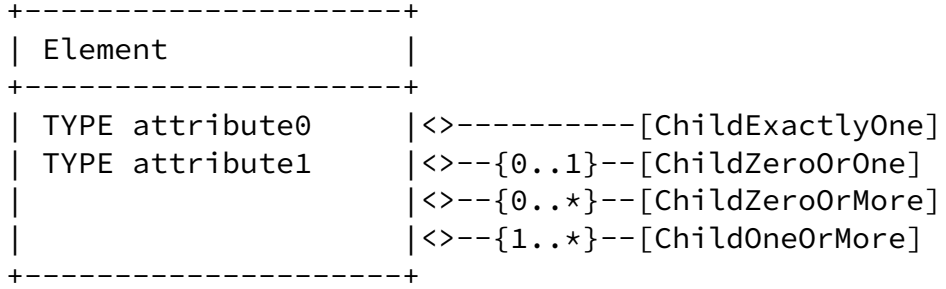


Figure 1: Example UML Element Diagram

Elements containing child elements should indicate the multiplicity of those child elements, as shown in the figure above. Allowable TYPEs are discussed in the following subsection.

### 2.2.1. IODEF Data Types

The allowable TYPEs for attributes within IODEF are enumerated in section 2 of [RFC5070], and consist of:

- INTEGER





- REAL

- CHARACTER
- STRING
- ML_STRING (for strings in encodings other than that of the enclosing document)
- BYTE for bytes or byte vectors in Base 64 encoding
- HEXBIN for bytes in ascii-hexadecimal encoding
- ENUM for enumerated types; allowable values of the enumeration must be defined in the attribute definition
- DATETIME for ISO 8601:2000 [RFC3339] encoded timestamps
- TIMEZONE for timezones as encoded in section 2.9 of [RFC5070].
- PORTLIST for port lists as encoded in section 2.10 of [RFC5070].
- POSTAL for postal addresses as defined in section 2.23 of [RFC4519].
- NAME for names of natural or legal persons as defined in section 2.3 of [RFC4519].
- PHONE for telephone numbers as defined in section 2.35 of [RFC4519].
- EMAIL for email addresses as defined in section 3.4.1. of [RFC2822].
- URL for URLs as in [RFC2396].

In addition to these simple data types, IODEF provides a compound data type for representing network address information. Addresses included within an extension element should be represented by containing an IODEF:Address element, which supports IPv4 and [RFC2373] IPv6 addresses, as well as MAC, ATM, and BGP autonomous system numbers. Application-layer addresses should be represented with the URL simple attribute type, instead.

### 2.2.2. Example Enumerated Type Extension Definition: E.164 Address

This example extends the IODEF Address element to support the encoding of ENUM-mapped telephone numbers [RFC6116].

Attribute: Address@category

Extended value(s): enum-e164

Content format: An E.164 telephone number encoded as a domain name in the e164.int space, e.g. "2.1.2.1.5.5.5.2.1.2.1.e164.int." for +1 212 555 1212, as per section 3.2 of [RFC6116].

Additional considerations: none.

### 2.2.3. 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 reference to a real incident.

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

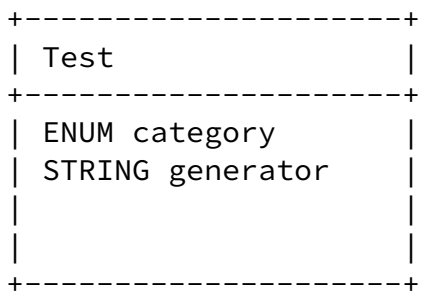


Figure 2: The Test class

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 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 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 may be freely shared to support this purpose.

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

## 2.3. 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 should be tested to validate against the schema given in the appendix.

## 2.4. Security Considerations

[SECDIR and RFC-EDITOR NOTE: Despite the title, this section is NOT a Security Considerations section, rather a template Security Considerations section for future extension documents to be built from this template. See Section 3 for Security Considerations for this document.]

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 or storage of the information represented by an extension.

## 2.5. IANA Considerations

[IANA and RFC-EDITOR NOTE: Despite the title, this section is NOT an IANA Considerations section, rather a template IANA Considerations section for future extension documents to be built from this template. See Section 4 for IANA Considerations for this document.]

Any IANA considerations [RFC5226] for the document should be detailed in this section; if none, the section should exist and contain the text "this document has no actions for IANA".

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 the appendix of the document, or to a well-known external reference in the case of an extension with an externally-defined schema.

## 2.6. Appendix: XML Schema Definition for Extension

The XML Schema describing the elements defined in the Extension Defintion section is given here. Each of the examples in section Section 2.3 should be verified to validate against this schema by automated tools.

# 3. Security Considerations

This document defines a template for MILE extensions to the IODEF and RID documents; as such, it has no security considerations on its own.

## 4. IANA Considerations

This section will be updated.

## 5. References

### 5.1. Normative References

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





[RFC6045] Moriarty, K., "Real-time Inter-network Defense (RID)", RFC 6045, November 2010.

### 5.2. Informative References

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

[RFC2373] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.

[RFC2396] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[RFC2822] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

[RFC3339] Klyne, G., Ed. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, July 2002.

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

[RFC4519] Sciberras, A., "Lightweight Directory Access Protocol (LDAP): Schema for User Applications", RFC 4519, June 2006.

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

[RFC6116] Bradner, S., Conroy, L., and K. Fujiwara, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 6116, March 2011.





Authors' Addresses

Dr. Katherine S. Goodier
L-3 Communications"
2720 Technology Drive
Annapolis Junction
USA

Phone: +01 301 547 7043
Email: katherine.goodier@l-3com.com

Damir Rajnovic
Cisco

Email: gaus@cisco.com