IPFIX Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 29, 2007

E. Boschi
Hitachi Europe
B. Trammell
CERT/NetSA
L. Mark
T. Zseby
Fraunhofer FOKUS
June 27, 2007

Extended Type Information for IPFIX Enterprise-Specific Information Elements
draft-boschi-ipfix-extended-type-00.txt

Abstract

This document describes an extension to IPFIX to provide type information for enterprise-specific Information Elements. This format is designed to facilitate interoperability and reusability

among a wide variety of applications and tools.

Table of Contents

1. Introduction

The IPFIX protocol specification allows the creation of enterprise-specific Information Elements to easily extend the protocol to meet requirements which aren't covered by the existing Information Model. However, there is no current mechanism to provide the data type for a given Information Element (e.g. enterprise-specific ones).

In this situation, it will not be possible to use any existing analysis tool on IPFIX records containing enterprise-specific Information Elements, since the tools will not be able to decode these Information Elements. Having to do some sort of tool-specific configuration (or code modification) on every tool just to tell which type each used Information Element has is a huge amount of work for users and implementors of enterprise-specific Information Eelements. Many tools in fact only need to know the field's data type to work on them. This memo specifies a mechanism for users to provide the data type of an Information Elements in a standardized, automatable way.

This memo specifies a mechanism for exporters to provide the data type and semantic information of enterprise-specific Information Elements within the exported data stream in a standardized and automatable way. We propose a mechanism, which makes use of IPFIX Options Records to allow the mapping from (enterpriseID,Information Element) pairs to corresponding data type and semantic information. Including the information inline allows more rapid processing of the data, and allows the flow stream (or file) to be partially self-describing.

2. Terminology

Terms used in this document that are defined in the Terminology section of the IPFIX Protocol [I-D.ietf-ipfix-protocol] document are to be interpreted as defined there.

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].

3. Type Information Extension

IPFIX Templates contain ID and length values but lack type and semantic information. There is no standard method to get this information for enterprise-specific Information Elements. A Collecting Process receiving data described by a Template containing unknown enterprise-specific Information Elements can only treat those

data as octet arrays. To be fully self-describing, enterprise-specific Information Elements must be additionally described via IPFIX Options according to the Information Element Semantics Options Template defined below.

In this section we first specify the necessary Information Elements for describing type information, and then the Information Element Semantics Options Template.

3.1. informationElementId

Description: An information element ID, as would appear in an IPFIX Template Record. This element can be used to scope properties to a specific information element within a Template. This IE should be encoded with the Enterprise ID bit set to 0, regardless of whether the Enterprise ID bit is set in the template to which this IE refers. See the definition of privateEnterpriseNumber below for more on the use of this IE to describe vendor-specific IEs.

Abstract Data Type: unsigned16

Data Type Semantics: identifier

ElementId: TBD1

Status: Proposed

Reference: Section 3.4.1 of the IPFIX Protocol draft

3.2. informationElementSemanticType

Description: A description of the semantics of an IPFIX information element within a template. These correspond to the data type semantics defined in section 3.2 of the IPFIX Information Model [I-D.ietf-ipfix-info]; see that section for more information on the types described below. This field may take the following values; the special value 0x00 (none) is used to note that no semantics apply to the field; it cannot be manipulated by a Collecting Process or File Reader that does not understand it a priori.

Value	Description
0x00	none
0x01	quantity
0x02	totalCounter
0x03	deltaCounter
0x04	identifier
0x05	flags

Abstract Data Type: unsigned8

ElementId: TBD2

Status: Proposed

3.3. informationElementStorageType

Description: A description of the storage type of an IPFIX information element within a template. These correspond to the abstract data types defined in section 3.1 of the IPFIX Information Model [I-D.ietf-ipfix-info]; see that section for more information on the types described below. This field may take the following values:

Value	Description
0x00	octetArray
0x01	unsigned8
0x02	unsigned16
0x03	unsigned32
0x04	unsigned64
0x05	signed8
0x06	signed16
0x07	signed32
0x08	signed64
0x09	float32
0x0A	float64
0x0B	boolean
0x0C	macAddress
0x0D	string
0x0E	dateTimeSeconds
0x0F	dateTimeMilliseconds
0x10	dateTimeMicroseconds
0x11	dateTimeNanoseconds
0x12	ipv4Address
0x13	ipv6Address

Abstract Data Type: unsigned8

ElementId: TBD3

Status: Proposed

Reference: Section 3.1 of the IPFIX Information Model

3.4. privateEnterpriseNumber

Description: A private enterprise number used to scope an information element ID, as would appear in an IPFIX Template Record. This element can be used to scope properties to a specific information element within a Template. If the Enterprise ID bit of the corresponding Information Element is cleared (has the value 0), this IE should be set to 0. The presence of a non-zero value in this IE implies that the Enterprise ID bit of the corresponding Information Element is set (has the value 1).

Abstract Data Type: unsigned32

Data Type Semantics: identifier

ElementId: TBD4

Status: Proposed

Reference: Section 3.4.1 of the IPFIX Protocol draft

3.5. Information Element Semantics Options Template

The Information Element Semantics Options Template specifies the structure of a Data Record for attaching semantic and storage type information to Enterprise Specific Information Elements in specified Template Records. Data Records described by this template are referred to as Information Element semantics records.

In deployments in which interoperability across vendor implementations of IPFIX is important, an Exporting Process exporting data using Templates containing enterprise-specific Information Elements SHOULD export an Information Element semantics record for each enterprise-specific Information Element it exports. Collecting Processes MAY use these semantics records to improve handling of unknown enterprise-specific Information Elements. Exporting Processes using enterprise-specific Information Elements to implement proprietary features MAY omit semantics records for those Information ELements.

Information Element semantics records MUST be handled by Collecting Processes as scoped to the Transport Session in which they are sent; this facility is not intended to provide a method for the permanent definition of Information Elements.

Similarly, for security reasons, storage and semantics types for a given Information Element MUST NOT be re-defined by Information Element semantics records. Once an Information Element semantics record has been exported for a given Information Element within a given Transport Session, all subsequent semantics records for that Information Element MUST be identical. If conflicting semantic or type information is received in multiple semantics records by a Collecting Process, the Collecting Process MUST reset the Transport Session.

Information Element semantics records MUST NOT be used to define semantics for IANA registered Information Elements (private enterprise number (PEN) 0) or for PENs with a special meaning within the IPFIX Protocol (e.g., the Reverse PEN from Bidirectional Flow Export using IPFIX [I-D.ietf-ipfix-biflow]).

The template SHOULD contain the following Information Elements as defined in the IPFIX Information Model [I-D.ietf-ipfix-info] and above:

IE	Description
informationElementID	The Information Element identifier of the Information Element within the specified Template this record describes. This Information Element MUST be defined as a Scope Field.
privateEnterpriseNumber	The Private Enterprise number of the Information Element within the specified Template this record describes. This Information Element MUST be defined as a Scope Field.
informationElementStorageType	The storage type of the specified Information Element.
informationElementSemanticType	The semantic type of the specified Information Element.

4. Security Considerations

The same security considerations as for the IPFIX Protocol [I-D.ietf-ipfix-protocol] apply.

5. IANA Considerations

This document specifies the creation of four new IPFIX Information Elements as described in sections 4.1 through 4.4. IANA has assigned the IPFIX Information Element number TBD1 in the IPFIX Information Element registry for the informationElementId Information Element; the IPFIX Information Element number TBD2 in the IPFIX Information Element registry for the informationElementSemanticType Information Element; the IPFIX Information Element number TBD3 in the IPFIX Information Element registry for the informationElementStorageType Information Element; and the IPFIX Information Element number TBD4 in the IPFIX Information Element registry for the privateEnterpriseNumber Information Element.

[NOTE for IANA: The text TBD1 should be replaced with the assigned informationElementId Information Element number where it appears in

this document. The text TBD2 should be replaced with the assigned informationElementSemanticType Information Element number where it appears in this document. The text TBD3 should be replaced with the assigned informationElementStorageType Information Element number where it appears in this document. The text TBD4 should be replaced with the assigned privateEnterpriseNumber Information Element number where it appears in this document.]

In addition, IANA has created an Information Element Semantic Type subregistry for the values defined for the informationElementSemanticType Information Element in section 4.2. A specification is required to add entries to this subregistry; new values and their meaning must be documented in an RFC or other permanent and readily available reference.

[NOTE for IANA: Please create a new Information Element Semantic Type subregistry as specified in the paragraph above, with initial values taken from section 4.2 of this document.]

6. Acknowledgements

Thanks to David Moore for first raising this issue to the IPFIX mailing list.

7. References

7.1. Normative References

[I-D.ietf-ipfix-protocol]
Claise, B., "Specification of the IPFIX Protocol for the Exchange", draft-ietf-ipfix-protocol-24 (work in progress), November 2006.

[I-D.ietf-ipfix-info]
Quittek, J., "Information Model for IP Flow Information Export", draft-ietf-ipfix-info-15 (work in progress), February 2007.

7.2. Informative References

[I-D.ietf-ipfix-biflow]
Trammell, B. and E. Boschi, "Bidirectional Flow Export using IPFIX", draft-ietf-ipfix-biflow-05 (work in progress), June 2007.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", BCP 14, RFC 2119, March 1997.

Appendix A. Examples

The following example illustrates how the type information extension mechanism defined in this document may be used to describe the semantics of enterprise-specific Information Elements. The Information Elements used in this example are as follows:

- initialTCPFlags, CERT (PEN 6871) private IE 14, 1 octet, the TCP flags on the first TCP packet in the flow.

- unionTCPFlags, CERT (PEN 6871) private IE 15, 1 octet, the union of the TCP flags on all packets after the first TCP packet in the flow.

An Exporting Process exporting flows containing these Information Elements might use a Template like the following:

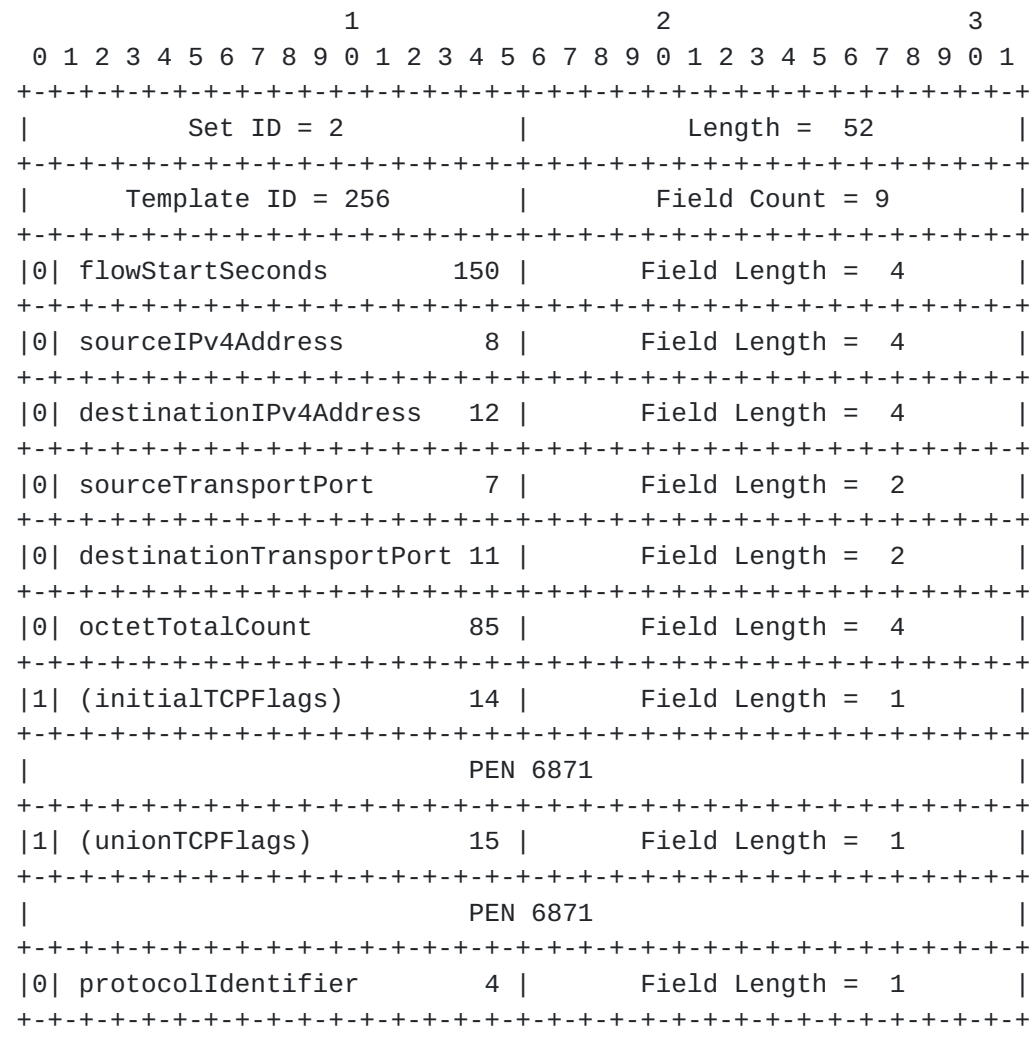

Figure 1: Template with Enterprise-Specific IEs

However, a Collecting Process receiving Data Sets described by this Template can only treat the enterprise-specific Information Elements as opaque octets; specifically, there is no hint to the collector that they contain flag informartion. To use the type information extension mechanism to address this problem, the Exporting Process would first export the Information Element Semantics Options Template described in section 4.5, above:

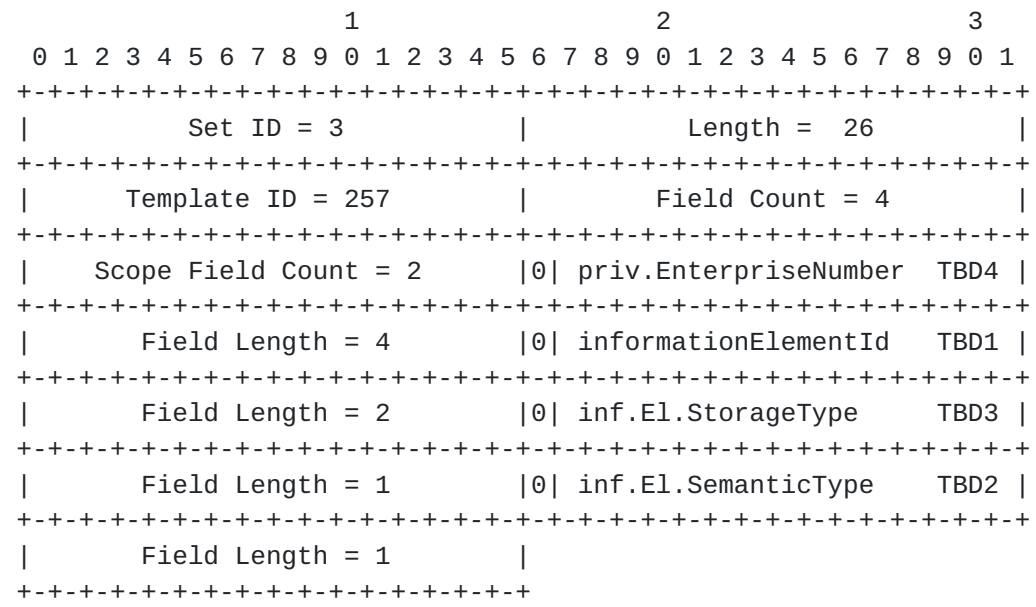

Figure 2: Example Information Element Semantics Options Template

Then, the Exporting Process would then export two records described by the Example Information Element Semantics Options Template to describe the enterprise-specific Information Elements:

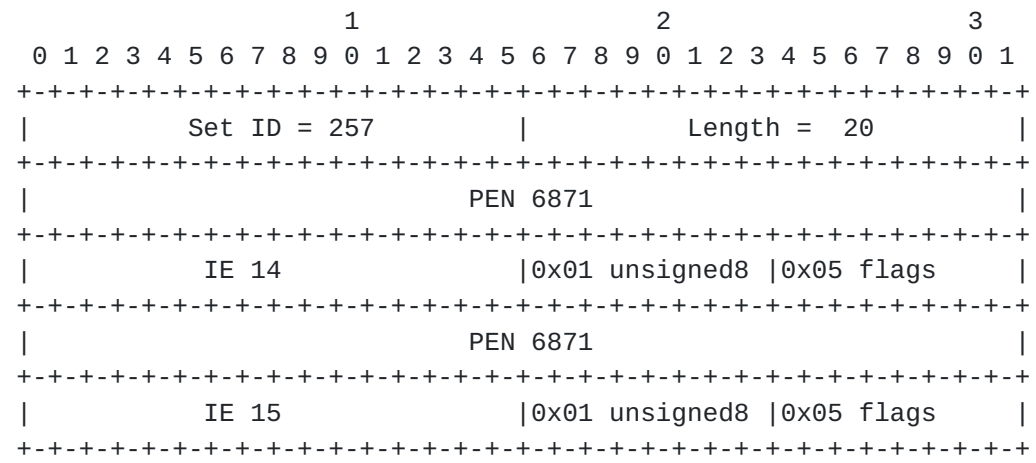

Figure 3: Type Information Extension Example

Appendix B. XML Specification of Extended Type Information Elements

This appendix contains a machine-readable description of the Information Elements defined in this document, coded in XML. Note that this appendix is of informational nature, while the text in section 3 is normative.

The format in which this specification is given is described by the XML Schema in Appendix B of the IPFIX Information Model [I-D.ietf-ipfix-info].

```
<?xml version="1.0" encoding="UTF-8"?>

<fieldDefinitions xmlns="urn:ietf:params:xml:ns:ipfix-info"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                  xsi:schemaLocation="urn:ietf:params:xml:ns:ipfix-info
                  ipfix-info.xsd">

  <field name="informationElementId" dataType="unsigned16"
         dataTypeSemantics="identifier" group="misc"
         elementId="TBD1" applicability="all" status="current">
    <description>
      <paragraph>
        An information element ID, as would appear in an IPFIX Template
        Record. This element can be used to scope properties to a specific
        information element within a Template. This IE should be encoded with
        the Enterprise ID bit set to 0, regardless of whether the Enterprise
        ID bit is set in the template to which this IE refers. See the
        definition of privateEnterpriseNumber below for more on the use of
        this IE to describe vendor-specific IEs.
      </paragraph>
    </description>
  </field>

  <field name="informationElementSemanticType" dataType="unsigned8"
         dataTypeSemantics="identifier" group="misc"
         elementId="TBD2" applicability="all" status="current">
    <description>
      <paragraph>
        A description of the semantics of an IPFIX information element within
        a template. These correspond to the data type semantics defined in
        section 3.2 of the IPFIX Information Model; see that section for more
        information on the types described below. This field may take the
        following values; the special value 0x00 (none) is used to note that
        no semantics apply to the field; it cannot be manipulated by a
        Collecting Process or File Reader that does not understand it a
        priori.
      </paragraph>
      <artwork>
        +-------+--------------+
        | Value | Description  |
        +-------+--------------+
        | 0x00  | none         |
        | 0x01  | quantity     |
        | 0x02  | totalCounter |
```

```
        | 0x03  | deltaCounter |
        | 0x04  | identifier   |
        | 0x05  | flags        |
        +-------+--------------+
      </artwork>
    </description>
  </field>

  <field name="informationElementStorageType" dataType="unsigned8"
          dataTypeSemantics="identifier" group="misc"
          elementId="TBD3" applicability="all" status="current">
    <description>
      <paragraph>
        A description of the storage type of an IPFIX information element
        within a template. These correspond to the abstract data types defined
        in section 3.1 of the IPFIX Information Model; see that section for
        more information on the types described below. This field may take the
        following values:
      </paragraph>
      <artwork>
        +-------+----------------------+
        | Value | Description          |
        +-------+----------------------+
        | 0x00  | octetArray           |
        | 0x01  | unsigned8            |
        | 0x02  | unsigned16           |
        | 0x03  | unsigned32           |
        | 0x04  | unsigned64           |
        | 0x05  | signed8              |
        | 0x06  | signed16             |
        | 0x07  | signed32             |
        | 0x08  | signed64             |
        | 0x09  | float32              |
        | 0x0A  | float64              |
        | 0x0B  | boolean              |
        | 0x0C  | macAddress           |
        | 0x0D  | string               |
        | 0x0E  | dateTimeSeconds      |
        | 0x0F  | dateTimeMilliseconds |
        | 0x10  | dateTimeMicroseconds |
        | 0x11  | dateTimeNanoseconds  |
        | 0x12  | ipv4Address          |
        | 0x13  | ipv6Address          |
        +-------+----------------------+
      </artwork>
    </description>
  </field>
```

```
  <field name="privateEnterpriseNumber" dataType="unsigned32"
           dataTypeSemantics="identifier" group="misc"
           elementId="TBD4" applicability="all" status="current">
    <description>
      <paragraph>
        A private enterprise number used to scope an information element ID,
        as would appear in an IPFIX Template Record. This element can be used
        to scope properties to a specific information element within a
        Template. If the Enterprise ID bit of the corresponding Information
        Element is cleared (has the value 0), this IE should be set to 0. The
        presence of a non-zero value in this IE implies that the Enterprise ID
        bit of the corresponding Information Element is set (has the value 1).
      </paragraph>
    </description>
  </field>
</fieldDefinitions>
```

Authors' Addresses

Elisa Boschi
Hitachi Europe SAS
Immeuble Le Theleme
1503 Route les Dolines
06560 Valbonne
France

Phone: +33 4 89874100
Email: elisa.boschi@hitachi-eu.com

Brian H. Trammell
CERT Network Situational Awareness
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, Pennsylvania 15213
United States

Phone: +1 412 268 9748
Email: bht@cert.org

Lutz Mark
Fraunhofer Institute for Open Communication Systems
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany

Phone: +49 30 3463 7306
Email: lutz.mark@fokus.fraunhofer.de

Tanja Zseby
Fraunhofer Institute for Open Communication Systems
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany

Phone: +49 30 3463 7153
Email: tanja.zseby@fokus.fraunhofer.de

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).