IPFIX evolution towards a more generic PUSH model

IPFIX IETF-74 March 22nd, 2009

<draft-claise-structured-data-in-ipfix-00>

Gowri Dhandapani, Stan Yates, Paul Aitken, <u>Benoit Claise</u>

Background info on the PUSH Model

- Which mechanism do we have to push data:
  - When there is a lot of data
  - When the data are non highly variable
- Solutions:
  - SNMP Notifications?
  - XML encoding?
  - Syslog?
  - IPFIX?
- One example: syslog replaced by NetFlow/IPFIX in a Firewall
- Some more references
  - IPFIX for VoIP Monitoring (Sven Anderson, NECLAB)
  - IEPG, Kobashi Atsushi (NTT) presented on IPFIX/PSAMP to export VoIP/IPTV metrics

draft-claise-structured-data-in-ipfix-00
Introduction

- IPFIX has always been about flat records

  Even if the Options Template could help

- A PUSH mechanism without structured data is not complete
- This draft is a extension to [RFC5101] and [RFC5102]

  Support hierarchical structured data and lists (sequences) of Information Elements in data records

Business Case for Structured Data

- One security-centric example in the draft
  - Although this is not a security draft!
- Other examples:
  - MPLS stack
  - Traceroute
  - Performance metrics
  - Access-list
- Where:
  - Export from a branch office (limited bandwidth)
  - Use of mediation functions

Examples

```
--------------------------------------------------------
 userId | sourceIPv4Address  |  applicationId list
--------------------------------------------------------
    1       192.0.2.201         1001, 1002, 1003
--------------------------------------------------------
```

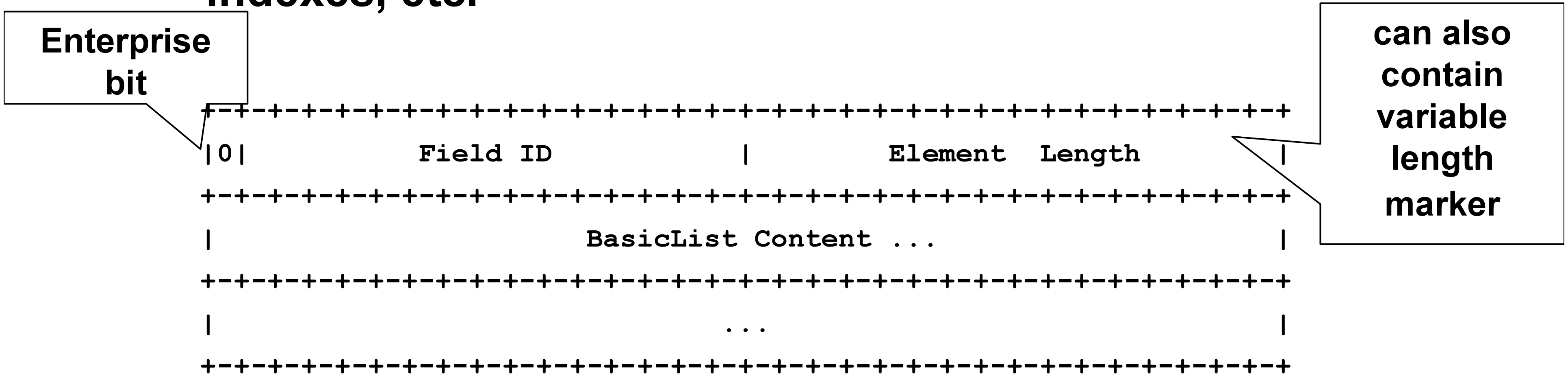
```
-----------------------------------------------------------------
      |        |        |             participant
sigId |protocol| risk   |     attacker     |        target
      |   Id   | Rating |  ip      | appId |    ip     | appId(s)
-----------------------------------------------------------------
1003     17       10     192.0.2.3    103
                         192.0.2.4    104   192.0.2.104  4001, 4002
                         192.0.2.5    105
-----------------------------------------------------------------
```

New Abstract Data Types and Information Element: basicList

basicList

represents a list of zero or more instances of any single Information Element. Primarily used for single-valued data types.

For example, a list of port numbers, list of interface indexes, etc.



Enterprise bit

can also contain variable length marker

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|          Field ID           |        Element  Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      BasicList Content ...                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure A: basicList Information Element Encoding

New Abstract Data Types and Information Element: subTemplateList

subTemplateList

represents a list of zero or more instances of structured data, where the data type of each list element is the same and corresponds with a single Template Record.

For example, structured data composed of multiple pairs of IP addresses

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Template ID          |    SubTemplateList Content    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure E: subTemplateList Encoding

New Abstract Data Types and Information Element: subTemplateMultiList

subTemplateMultiList

represents a list of of zero or more instances of structured data, where the data type of each list element can be different and correspond with different template definitions.

For example, structured data composed of multiple access-list entries, where entries can be composed of different criteria types

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Element 1 Length        |     Element 1 Template ID     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Element 1 Content ...                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Element 2 Length        |     Element 2 Template ID     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Element 2 content ...                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              ...                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Element N Length         |     Element N Template ID     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Element N content ...                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

What’s the Next Step for this Draft?

- Get some feedback
- To be addressed in the next version:
  - What about circular references
  - As scope: potentially useful
    - eg <this option> applies to <this list of items>
  - Usage Guidelines for Equivalent Data Representations

Observation & Conclusion

- IPFIX starts to be used as THE push mechanism when:
  - When there is a lot of data
  - When the data are non highly variable
- Feedback?