Exporting Type Information for IPFIX Information Elements

draft-boschi-ipfix-exporting-type-00.txt

IETF 70 - Vancouver, BC, Canada - 4 Dec 2007

Elisa Boschi - Hitachi Europe
Brian Trammell - CERT/NetSA
Lutz Mark - Fraunhofer FOKUS
Tanja Zseby - Fraunhofer FOKUS

The problem, restated

- IPFIX provides no mechanism for representing information model properties within an IPFIX message stream.
- This requires an external reference for semantic and type information for information elements:
  - Only length is provided in IPFIX templates;
  - IANA provides external reference for registered IEs, but
  - No external reference for enterprise-specific IEs.
- Not possible to use generic analysis tools on IPFIX records containing enterprise-specific IEs, since the tools will not be able to decode these IEs.
- Potential interoperability issues with enterprise-specific IEs.

History

- FloCon, 2005 – Lack of type information identified as enterprise-specific IE interoperability issue, and added to open issues in guidelines.
- Prague, 2007 – Initial solution introduced in draft-trammell-ipfix-file to meet self-description requirement.
  - generally applicable to use cases other than file, e.g., data sharing across administrative domains.
- Chicago, 2007 – Refined solution in draft-boschi-ipfix-extended-type-00
  - suggests a complete inline representation of IPFIX information model.

Exporting Type

- Draft expanded to represent every dimension of an information element in the IPFIX Information Model inline within an IPFIX Message Stream.

- Provides a generalized mechanism for inline representation of Information Element type information using Options.
  - Backward-compatible – no (new) interoperability issues with collectors that don’t implement type export.
  - No changes to the IPFIX message format.

- Representing information inline allows for self-description (as required by the file format)

Supported IE Dimensions

- Every dimension provided for information elements in the IPFIX Information Model (and represented in the XML Schema defined there) is supported:
  - Data type (e.g., unsigned16, float32, dateTimeMilliseconds)
  - Semantics (e.g., counter, identifier, flags)
  - Units (e.g., packets, milliseconds)
  - Ranges
  - Name and description

Example

- Initial and Union TCP flags
  - Enterprise-specific IEs to allow export of initial TCP flags for flow completeness verification, continuation detection, etc.
- PEN 6871, IE numbers 14 and 15
- Without type export, generic collecting processes can treat these only as octet arrays of length 1.
- With type export, can display names and apply flag semantics.

Example (Template)

<table>
<tr><td colspan="2">Set ID 2</td><td>Length 40</td></tr>
<tr><td colspan="2">Template ID 256</td><td>Field Count 9</td></tr>
<tr><td>0</td><td>IE 8 (sourceIPv4Addr)</td><td>IE Length 4</td></tr>
<tr><td>0</td><td>IE 12 (destIPv4Addr)</td><td>IE Length 4</td></tr>
<tr><td>0</td><td>IE 7 (sourcePort)</td><td>IE Length 2</td></tr>
<tr><td>0</td><td>IE 11 (destPort)</td><td>IE Length 2</td></tr>
<tr><td>1</td><td>IE 14 (initialTCPFlags)</td><td>IE Length 1</td></tr>
<tr><td colspan="3">PEN 6871</td></tr>
<tr><td>1</td><td>IE 15 (unionTCPFlags)</td><td>IE Length 1</td></tr>
<tr><td colspan="3">PEN 6871</td></tr>
</table>

Example (Options Template)

Set ID 3		Length 26
Template ID 257		Field Count 5
Scope Field Count 2		
0	IE tbd (privateEntNbr)	IE Length 4
0	IE 303 (infoEltId)	IE Length 2
0	IE tbd (ieDataType)	IE Length 1
0	IE tbd (ieSemantics)	IE Length 1
0	IE tbd (ieName)	IE Length 65536 (var.)

Example (Options)

Set ID 257	Length 50	
6871 (PEN)		
14 (IE)	1 (type,u8)	5 (sem,flag)
“initialTCPFlags” (name)		
6871 (PEN)		
15 (IE)	1 (type,u8)	5 (sem,flag)
“unionTCPFlags” (name)		

Future Work

- Submission of ietf-00 revision after Vancouver IETF in December
- Submission of final draft to IESG after Philadelphia IETF, by June
- Questions?