IP Flow Information eXport (IPFIX)

elisa.boschi@hitachi-eu.com

{boschi, zseby, mark, hirsch}@fokus.fraunhofer.de

HITACHI Inspire the Next FOKUS

Outline

- IPFIX
- Terminology
- Applicability
- Initial Goals
- Current Status
  - *Rough consensus (Internet-Drafts and RFCs)*
  - *Running code (Implementations)*
- Conclusions

HITACHI Inspire the Next FOKUS

IP Flow Information eXport

- General data transport protocol
- Flexible flow key (selection)
- Flexible flow export - TEMPLATE BASED
  - New fields can be added to flow records without changing the structure of the record format
  - The collecor can always interpret flow records
  - external data format description → compact encoding
- Efficient data representation
  - Extensible (future attributes to be added)
  - Flexible (customisable)
  - Independent (of the Transport protocol)

HITACHI Inspire the Next FOKUS

Terminology

- A TEMPLATE is an ordered sequence of <type,length> pairs
  - specify the structure and semantics of a particular set of information (**Information Elements**)
- DATA RECORDS contain values of parameters specified in a template record
- OPTION RECORDS define the
  - structure and interpretation of a data record
  - how to scope the applicability

HITACHI Inspire the Next FOKUS

The protocol

- Unidirectional (push mode)
- The exporter sends data (and option) templates
  - Information Elements descriptions
- Information Elements are sent in network byte order

Applicability

- Target applications requiring flow-based IP traffic measurements (RFC 3917)
  - Usage-based accounting
  - Traffic profiling
  - Attack/intrusion detection
  - QoS monitoring
  - Traffic engineering
- Other applications (AS):
  - Network planning
  - Peering agreements

HITACHI Inspire the Next FOKUS

Attack / intrusion detection

- IPFIX provides input to attack / intrusion detection functions:
  - Unusually high loads
  - Number of flows
  - Number of packets of a specific type
  - Flow volume
  - Source and destination address
  - Start time of flows
  - TCP flags
  - Application ports

HITACHI Inspire the Next FOKUS

Initial Goals 1/4

- *Define the notion of a "standard IP flow"*

*A **Flow** is a set of IP packets passing an Observation Point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties defined as the result of applying a function to the values of:*

- *One or more packet header field (e.g. dest. IP address), transport header field (e.g. dest. port number), or application header field (e.g. RTP header fields RTP-HDRF)*
- *One or more characteristics of the packet itself (e.g. # of MPLS labels)*
- *One or more fields derived from packet treatment (e.g. next hop IP address)*

HITACHI Inspire the Next FOKUS

Initial Goals 2/4

- *Devise data encodings that support analysis of IPv4 and IPv6 unicast and multicast flows…*
  - IPFIX Information Model
    - formal description of IPFIX information elements (fields), their name, type and additional semantic information
- *Consider the notion of IP flow information export based upon packet sampling*
  - The **flow definition** includes packets selected by a sampling mechanism
  - Through **option templates**, the configuration sampling parameters can be reported

HITACHI Inspire the Next FOKUS

Initial Goals 3/4

- *Identify and address any security concerns affecting flow data.*
  - Disclosure of flow info data
  - Confidentiality → IPSec and TLS
  - Forgery of flow records
  - Authentication and integrity → IPSec and TLS

- *Specify the transport mapping for carrying IP flow information* → SCTP / SCTP-PR
  - Reliable (or partially reliable)
  - Congestion aware
  - Simpler state machine than TCP

HITACHI Inspire the Next FOKUS

Initial Goals 4/4

- *Ensure that the flow export system is reliable (minimize the likelihood of flow data being lost and to accurately report such loss if it occurs).*
  - SCTP, TCP
  - UDP
    - Templates are resent at a regular time interval
  - Sequence numbers

HITACHI Inspire the Next FOKUS

Current status

- Internet-Drafts (~ sent to the IESG):
  - Architecture for IP Flow Information Export
  - Information Model for IP Flow Information Export
  - IPFIX Protocol Specification
  - IPFIX Applicability

- Request For Comments:
  - Requirements for IP Flow Information Export (RFC 3917)
  - Evaluation of Candidate Protocols for IP Flow Information Export (IPFIX) (RFC 3955)

HITACHI Inspire the Next FOKUS

Other related drafts

- Export of per packet information with IPFIX
  - E.Boschi, L.Mark draft-boschi-export-perpktinfo-00.txt
- IPFIX aggregation
  - F.Dressler, C.Sommer, G.Munz draft-dressler-ipfix-aggregation-01.txt
- Simple IPFIX Files for Persistent Storage
  - B.Trammell draft-trammell-ipfix-file-00.txt
- IPFIX templates for common ISP usage
  - E.Stephan, E. Moureau draft-stephan-isp-templates-00.txt
- IPFIX Protocol Specifications for Billing
  - B.Claise, P.Aitken, R.Stewart draft-bclaise-ipfix-reliability-00.txt
- IPFIX Implementation Guidelines

HITACHI Inspire the Next FOKUS

„Running code“

- At least 6 different IPFIX implementations
  - Ours is open source: http://www.6qm.org/downloads.php
- Implementers mailing list
- Interoperability events
  - July 2005, Paris (http://www.ist-mome.org)
  - Further tests planned
- Implementation guidelines in preparation

HITACHI Inspire the Next FOKUS

Conclusions

- IPFIX is the upcoming standard for (IP) flow information export
- Allows common analysis tools
- Data exchange

... questions?

HITACHI Inspire the Next FOKUS

IPFIX message format

- IPFIX message
  - message header
  - 1 or more {template, option template, data} sets

- A TEMPLATE is an ordered sequence of <type, length> pairs used to completely specify the structure and semantics of a particular set of information
  - (unique by means of a template ID)
  - DATA RECORDS contain values of parameters specified in a template record
  - Field values are encoded according to their data type specified in IPFIX-INFO
  - OPTION RECORDS define the structure and interpretation of a data record including how to scope the applicability

HITACHI Inspire the Next FOKUS

INFORMATION ELEMENTS

- INFORMATION ELEMENTS are descriptions of attributes which may appear in an IPFIX record
  - IANA assigned
  - Defined in the Information Model
  - Enterprise specific (proprietary I.E.)
- Variable Length I.E.
  - The length is carried in the information element content itself
- The type associated with an IE
  - indicates constraints on what it may contains
  - determines the valid encoding mechanisms for use in IPFIX
- I.E.s must be sent in network byte order (big endian)

HITACHI Inspire the Next FOKUS

INFORMATION ELEMENTS

- The elements are grouped into 9 groups according to their semantics and their applicability:

1. Identifiers
2. Metering and Exporting Process Properties
3. IP Header Fields
4. Transport Header Fields
5. Sub-IP Header Fields
6. Derived Packet Properties
7. Min/Max Flow Properties
8. Flow Time Stamps
9. Per-Flow Counters
10. Miscellaneous Flow Properties

} can serve as Flow Keys

(used for mapping packets to Flows)

HITACHI Inspire the Next FOKUS

Requirements for the data model

- IPFIX is intended to be deployed in high speed routers and to be used for exporting at high flow rates

- → Efficiency of data representation
- How data is represented = data model

- EXTENSIBLE
  - For future attributes to be added

- FLEXIBLE
  - Concerning the attributes (customisable)

- INDEPENDENT
  - Of the transport protocol

HITACHI Inspire the Next FOKUS