draft-niccolini-sipclf-ipfix-03

Niccolini, Claise, Trammell, Kaplan

SIPCLF WG - IETF 78 Maastricht

26 July 2010

Changes since -00

- Movement toward a specification rather than a position statement
  - Alignment with draft-ietf-sipclf-problem-statement
  - Improved definition of Information Elements (IEs)
  - Improved recommended templates for request and response records
    - (currently only using mandatory fields)

- Improved examples (taken from RFC 3665)
  - At this point, examples are important for furthering discussion

Intro to IPFIX

- IP Flow Information Export
  - enables flexible export of network-related data with little variation in semantics
- Defines
  - a rich, easily extensible information model
    - RFC 5102, http://www.iana.org/assignments/ipfix
  - a template-driven data representation with a unidirectional protocol for transport
    - RFC 5101
  - and a file format for storing IPFIX data
    - RFC 5655

Extending IPFIX for SIP logging

- Fifteen SIP-specific information elements
  - Defined for fields specified in problem statement
  - Presently allocated as enterprise-specific under PEN 35566 (trammell.ch), to be proposed within IANA registry
- Recommended templates for request and response records
  - not technically required, as IPFIX is self-describing
  - simplifies generation of examples and comparisons with other representations
- Protocol and message formats completely IPFIX-interoperable

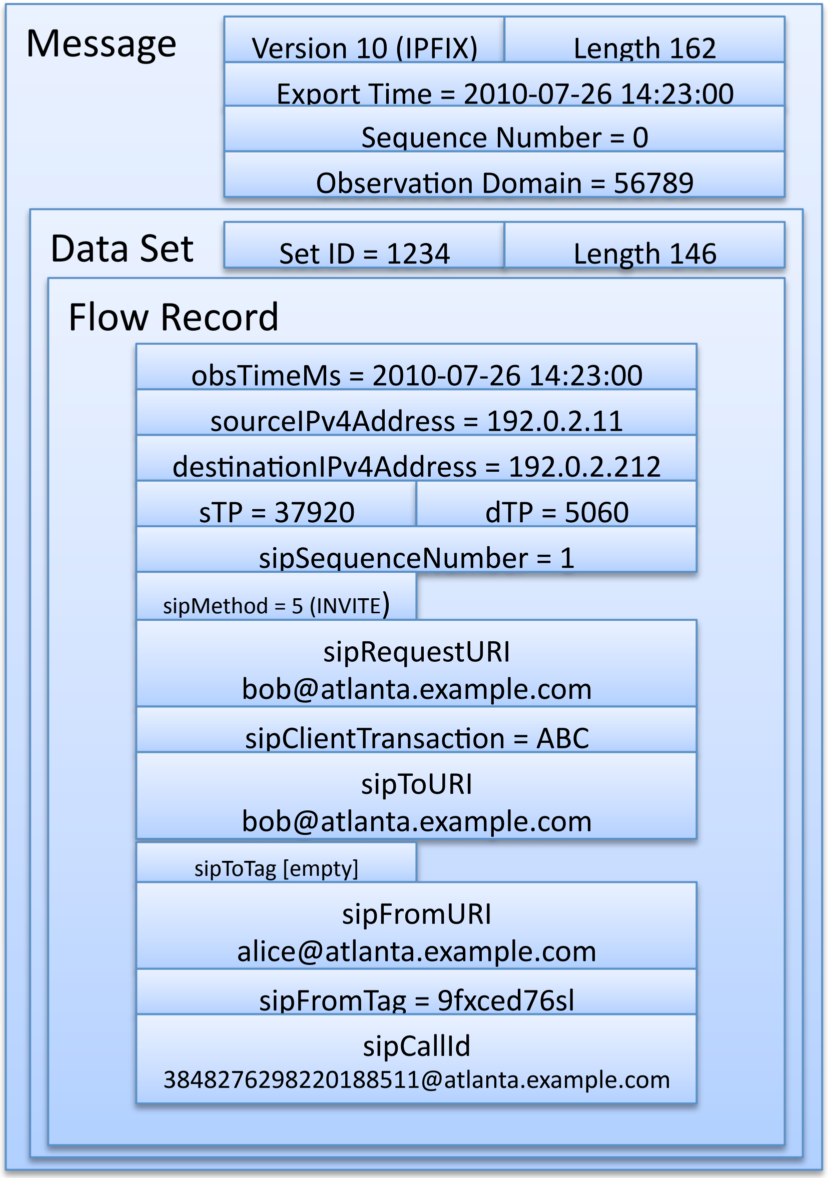
SIP information elements

Name	Number/Type	Description
sipAuthUsername	35566/401 string	The authenticated SIP username
sipMethod	35566/402 unsigned8	The SIP method from the CSeq: header, as per subregistry
sipRequestURI	35566/403 string	Request URI including parameters
sipFromURI	35566/404 string	From: URI
sipFromTag	35566/405 string	From: header field tag parameter, if present
sipToURI	35566/406 string	To: URI
sipToTag	35566/407 string	To: header field tag parameter, if present
sipCallId	35566/408 string	Call-ID: header field
sipSequenceNumber	35566/409 unsigned32	Sequence number from the CSeq: header field
sipContactURI	35566/410 string	Contact URI (possibly multiple per record)
sipPaiURI	35566/411 string	P-Asserted-Identity URI
sipResponseStatus	35566/412 unsigned16	SIP Response code
sipServerTransaction	35566/413 string	Server transaction identifier
sipClientTransaction	35566/414 string	Client transaction identifier
sipSessionId	35566/415 string *(octetArray, 16 octets)*	Session identifier, received in Session-ID: header or generated

Recommended Templates

Request Record (fixed 21, min 28 bytes)	Response Record (fixed 23, min 26 bytes)
observationTimeSeconds	observationTimeSeconds
sourceIPv4Address	sourceIPv4Address
destinationIPv4Address	destinationIPv4Address
sourceTransportPort	sourceTransportPort
destinationTransportPort	destinationTransportPort
sipSequenceNumber	sipSequenceNumber
	sipResponseStatus
sipMethod	sipMethod
sipRequestURI	
sipClientTransaction	
	sipServerTransaction
sipToURI	sipToURI
sipToTag	sipToTag
sipFromURI	
sipFromTag	
sipCallId	

Example Request Record Message



Message

Version 10 (IPFIX)

Length 162

Export Time = 2010-07-26 14:23:00

Sequence Number = 0

Observation Domain = 56789

Data Set

Set ID = 1234

Length 146

Flow Record

obsTimeMs = 2010-07-26 14:23:00

sourceIPv4Address = 192.0.2.11

destinationIPv4Address = 192.0.2.212

sTP = 37920

dTP = 5060

sipSequenceNumber = 1

sipMethod = 5 (INVITE)

sipRequestURI
bob@atlanta.example.com

sipClientTransaction = ABC

sipToURI
bob@atlanta.example.com

sipToTag [empty]

sipFromURI
alice@atlanta.example.com

sipFromTag = 9fxced76sl

sipCallId
3848276298220188511@atlanta.example.com

Advantages

- Leverages existing IPFIX work (storage, transmission, data model, mediation architecture)
  - SIP logging somewhat more complex than Apache CLF, the inspiration for this WG
  - IPFIX provides data model and architecture supporting larger-scale installations
- More efficient storage and processing than logging to a text file
  - Future work: cross conversion to text files
  - Future work: analysis of efficiency gain on realistic load

Next steps

- Complete definition of information model and recommended templates.
- Efficiency analysis, cross-conversion, more examples!
- Customary backmatter (security considerations, IANA)
- WG item adoption