An IPFIX-Based File Format

draft-trammell-ipfix-file-01

http://www.ietf.org/internet-drafts/draft-trammell-ipfix-file-01.txt

Brian Trammell, Elisa Boschi,
Lutz Mark, Tanja Zseby

Tuesday, July 11, 2006

IETF 66 - Montréal, Québec, Canada

The Idea

- File-based flow storage useful for archival applications as well as document-based workflows.
- Flat binary files ideal for flow storage
  - high record volume
  - low variety in record structure
- IPFIX message format ideal for flow records
  - templates provide extensible self-description without adding overhead to each record.
  - We consider “file” a fourth IPFIX transport.

The Document

- Motivation
- Requirements
  - Extensibility and Self-Description
  - Compression
  - Indexing and Searching Support
  - Data Integrity and Error Correction
  - Creator Authentication and Confidentiality
  - Anonymization and Obfuscation

The Document (continued)

- File Format Description
  - Base definition: any serialized stream of IPFIX Messages is a valid IPFIX File.
  - Additional extensions and capabilities deferred to -02 and beyond; we're working on requirements now.
- Customary IETF front- and back-matter

The Future

- Currently assessing WG interest for taking this on as it matures.
- Refine and come to agreement on requirements.
  - Planned completion by IETF 67, November 2006.
- Define IPFIX file format to meet these requirements.
  - Define message format extensions, or propose them for IPFIXv2.
  - Planned completion by IETF 68, March 2007.
- Gain implementation experience with IPFIX files.
  - At least one tool set (we know of) already uses "base definition" serialized IPFIX message streams as its native file format.

Questions and Discussion