An IPFIX-Based File Format
draft-trammell-ipfix-file-02

http://www.ietf.org/internet-drafts/draft-trammell-ipfix-file-02.txt

Brian Trammell, Elisa Boschi,
Lutz Mark, Tanja Zseby

Thursday, November 9, 2006

IETF 67 - San Diego, California, USA

The Idea In Review

- **Standard flow storage format useful for interoperability and implementation reuse.**
- **Flat binary files ideal for flow storage**
  - Wide variety of operations available on files.
  - Flow data not semantically complex.
    - Limits applicability of RDBMS.
  - Low variety in record structure relative to data volume.
    - Limits applicability of XML.
- **IPFIX message format ideal for flow records**
  - templates provide extensibility and self-description.

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
    - Implementation Performance (*new*)

The Document (continued)

- ## File Format Description

  - Any serialized stream of IPFIX Messages that would be valid over any transport is a valid IPFIX File.

  - Extensibility "free" with IPFIX Templates.

  - Propose use of IPFIX Options for self-description, limited error detection, anonymization notation.

  - Propose use of external standards and mechanisms for authentication, confidentiality, compression.

  - Propose to address compression error resilience issues at Exporting Process.

The Future

- Continue to assess WG interest for taking this on as it matures.

- Refine proposed methods for meeting requirements.
  - -02 revision's definition of IPFIX Options Templates incomplete.
  - Have deferred work on indexing and searching.

- Continue to gain implementation experience with IPFIX files.

Questions and Discussion