# An IPFIX-Based File Format

## draft-trammell-ipfix-file-03

http://www.ietf.org/internet-drafts/draft-trammell-ipfix-file-03.txt

Brian Trammell, Elisa Boschi,
Lutz Mark, Tanja Zseby

Tuesday, March 19, 2007

IETF 68 - Prague, Czech Republic

# 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
- 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.
  - Use IPFIX Options for self-description, limited error detection, anonymization notation.
  - Use external standards and mechanisms for authentication, confidentiality, compression.
  - Guidelines for addressing compression and encryption error resilience issues at both EP and CP.

# IPFIX Options for Self-Description

- New information elements and recommended Options Templates for defining semantic and storage type information for vendor-specific IEs.
- Associates storage types and semantics defined for the Information Model with {template, enterprise, IE} tuples.
- Generally applicable on the wire, as well.

# Changes since -02

- Finished definition of IPFIX Options for Self-Description.
- Defined security rules for these options.
  - Need to restrict what changes an EP can make to a CP's data model.
- Identified a few new open issues.
  - Need a new section on IPFIX File Applicability to IPFIX collection infrastructures.

# The Future

- Continue to address open issues and address comments as received.
  - Expect an -04 before Chicago.
- Continue to gain implementation experience with IPFIX files.
  - At least two nearly complete, open source implementations.

# Questions and Discussion