IPFIX Implementation
Guidelines

Elisa Boschi  (Hitachi Europe)
Lutz Mark  (Fraunhofer FOKUS)
Juergen Quittek  (NEC Europe)
Martin Stiemerling  (NEC Europe)
Paul Aitken  (Cisco)
Facts

- Submitted as IPFIX WG Item in August 2006

- **Milestone: November 2006**

- Recommendations and clarifications (for implementers)
  - E.g. IPFIX interoperability events, mailing list, implementers
  - Next event planned for 29,30 November 2006
  - Missing guidelines on security

- **New Document Structure since -00**
Changes from version -00

- Overall text improvement
- Clarifications have been added
- New concept of Transport Session

- Many sections improved
  - Middleboxes Changing the DSCP
  - Middleboxes Changing IP Addresses and Port Numbers
  - Order of Information Elements within the Template

- New guidelines:
  - Time issues
  - Devices without an absolute clock
  - Reduced-size Encoding of Information Elements
Document outline (1/3)

- Template Management Guidelines
  - Template Management
  - Template Records versus Option Template Records
  - Using Scopes
  - Multiple Information Elements of same type

- Exporting Process Guidelines
  - Sets
  - Order of Information Elements within the Template
  - Information Element Coding
  - Using counters
  - Padding
  - Time Issues
  - IPFIX Message Header Export Time and Data Record Time
  - Devices without an absolute clock
Document outline (2/3)

- Collecting Process Guidelines
  - Information Element (de)coding
  - Reduced-size Encoding of Information Elements
  - Template Management

- Transport-Specific Guidelines
  - SCTP
  - UDP
  - TCP

- Guidelines for implementation on Middleboxes
  - Traffic Flow Scenarios at Middleboxes
  - Location of the Observation Point
  - Reporting Flow-related Middlebox Internals
Document Outline (3/3)

- Extending the Information Model
  - Adding new IETF specified Information Elements
  - Adding enterprise-specific Information Elements

- Common Implementation Mistakes
  - IPFIX and NetFlow version 9
  - Padding of the Data Set
  - Field ID Numbers
  - Template ID Numbers

- Security Considerations

- Code Availability (open source)
Open Issues

- Enterprise specific Information Elements
  - how to obtain the type of the given IE
  - Do we want to address this and if yes, do we want to do it in this document?

- Security guidelines
  - At least 3 ongoing implementations
  - Delayed start

- The tunnelID mentioned in the middlebox section is not in IPFIX-INFO
  - many types of tunnels and identifiers
  - The section needs to be modified
Conclusions

- IPFIX Interoperability event
  - [http://ants.fokus.fraunhofer.de/ipfix/interop06/](http://ants.fokus.fraunhofer.de/ipfix/interop06/)
  - Focus on SCTP and security aspects

- Main goal for the next month(s): security guidelines

- Submission to IESG: November seems too early
  - Beginning 2007?

- Feedback welcome!