DEMONE IPFIX Interoperability Event - Final Report

CESNET, Prague, CZ
25-26 March 2011
Test Setup

• Testing over two days at CESNET in Prague
• 1Gbit/s test traffic for MPs to observe
  – First IPFIX interop with realistic loads
• Tests of SCTP, TCP, UDP
  – connectivity from EP to CP
  – Template Record export and interpretation
  – Data Record export according to templates
Participants

- CESNET
- INVEA-TECH
- TU Munich (VERMONT)
- TU Kosice
- CERT/NetSA (YAF, SiLK)
- nTop.org (nProbe, nTop)
- ETH Zurich (ripfix)
- Cisco Systems* (PSAMP only)
  - *via replayed pcap
SCTP Issues

• Simple export works, as long as SCTP itself works
• Supporting kernel modules and libraries still somewhat temperamental
  – Much SCTP testing done virtualized
  – Some libraries/kernel modules have an apparent max SEQPACKET size of 62420
  – Some tests cancelled due to connection problems
• No implementation of multiple-stream export or exotic template handling
TCP matrix

- YAF
- INVEA
- nProbe
- SiLK
- VERMONT CP
- ripfix CP
- CESNET CP
TCP status

- Continued implementation-level faults need more debugging
  - Some prerelease implementations failed and were only partially tested, or completely removed from testing
  - One implementation corrupted export after large data volumes on TCP only.

- TCP not very widely implemented
UDP issues

• UDP support most mature
  – reflects migration from NetFlow v9

• Serious packet loss on test network
  – up to 90% for slow collectors
  – emphasis on using a well-provisioned, dedicated, separated measurement network for UDP still a good idea

• Otherwise, few issues
General issues

• Enterprise-specific Information Elements and Reduced Length Encoding
• 64-bit IEs on 32-bit machines: implementation issues with 64-bit cleanliness
• Timestamp encoding (especially NTP)
• Synchronization of template retransmit and expiry on UDP caused confusion
  – suggest simplification of the rules
Partially tested

- **IPFIX Files**
  - supported for debugging by certain implementations

- **IPFIX Structured Data**
  - Verified that noncompliant collectors can successfully ignore structured data, as designed (YAF → ripfix)

- **Export over IPv6**
  - Some implementations dual-stack, but many still v4-only
  - Transport session management changes may be required for larger addresses, especially for UDP

- **PSAMP**
  - replayed UDP packets from a prerelease Cisco implementation were partially decoded by VERMONT and ripfix
  - discovered issues with template export, now fixed.
Not tested

• DTLS
  – Very limited support, even five years later
  – FreeBSD only, OpenSSL patches...

• Multiple stream export or SCTP-PR
  – SCTP is basically a direct port from UDP for most

• Template withdrawal, stream separation, reuse
  – Is template handling needlessly complicated?
Acknowledgments

• FP7-DEMONS, sponsor
  – http://fp7-demons.org
• CESNET, facility and network
  – http://www.ces.net
• IPFIX implementors who brought code and devices to test