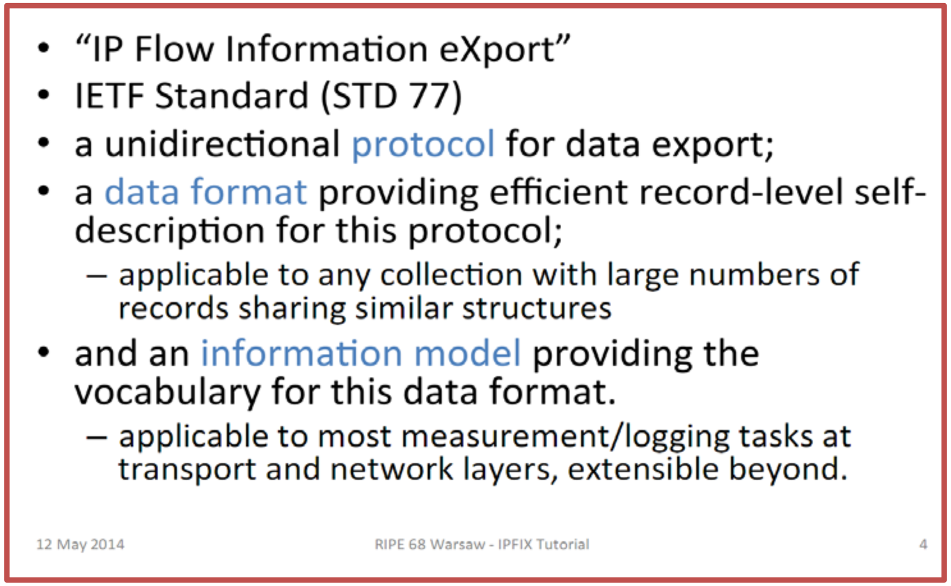
IPFIX IE Extensions for DDoS Attack Detection draft-fu-dots-ipfix-extension-01

Tianfu Fu	futianfu@huawei.com
Dacheng Zhang	dacheng.zdc@alibaba-inc.com
Liang Xia (Frank)	frank.xialiang@huawei.com
Min Li	l.min@huawei.com

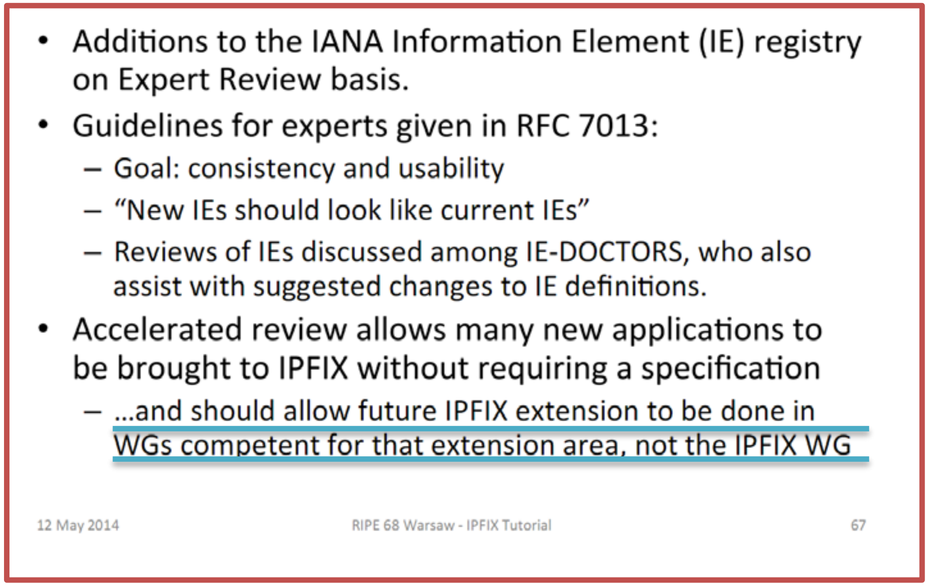
What is IPFIX

- **Refers to *“Applying IPFIX to Network Measurement and Management”* by *Brian Trammell***
  - ***What is IPFIX***
  - ***Introducing the IPFIX IE-DOCTORS***



- “IP Flow Information eXport”
- IETF Standard (STD 77)
- a unidirectional protocol for data export;
- a data format providing efficient record-level self-description for this protocol;
  - applicable to any collection with large numbers of records sharing similar structures
- and an information model providing the vocabulary for this data format.
  - applicable to most measurement/logging tasks at transport and network layers, extensible beyond.

12 May 2014 RIPE 68 Warsaw - IPFIX Tutorial 4



- Additions to the IANA Information Element (IE) registry on Expert Review basis.
- Guidelines for experts given in RFC 7013:
  - Goal: consistency and usability
  - “New IEs should look like current IEs”
  - Reviews of IEs discussed among IE-DOCTORS, who also assist with suggested changes to IE definitions.
- Accelerated review allows many new applications to be brought to IPFIX without requiring a specification
  - …and should allow future IPFIX extension to be done in WGs competent for that extension area, not the IPFIX WG

12 May 2014 RIPE 68 Warsaw - IPFIX Tutorial 67

How IPFIX Fits into DOTS

From DOTS charter:

"The aim of DDoS Open Threat Signaling (DOTS) is to develop a standards based approach for the realtime signaling of DDoS related telemetry and threat handling requests and data between elements concerned with DDoS attack detection, classification, traceback, and mitigation. "

From draft-ietf-dots-requirements:

"Attack telemetry: Collected network traffic characteristics enabling the detection, classification, and in many cases traceback of a DDoS attack.

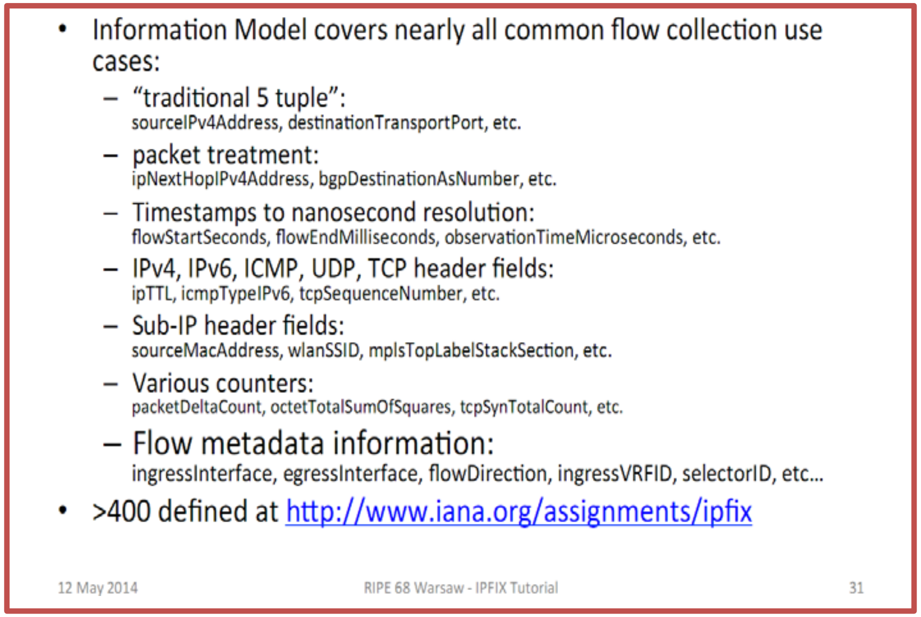
...

To achieve this aim, the protocol must permit the DOTS client to request or withdraw a request for coordinated mitigation; ... and to supply summarized attack information and additional hints the DOTS server elements can use to increase the accuracy and speed of the attack response."

This document focuses on the DDoS related telemetry information part for DOTS, and proposes using a set of IPFIX IEs for the goal of DDoS attack inspection.

IPFIX Information Elements (IEs) for Security

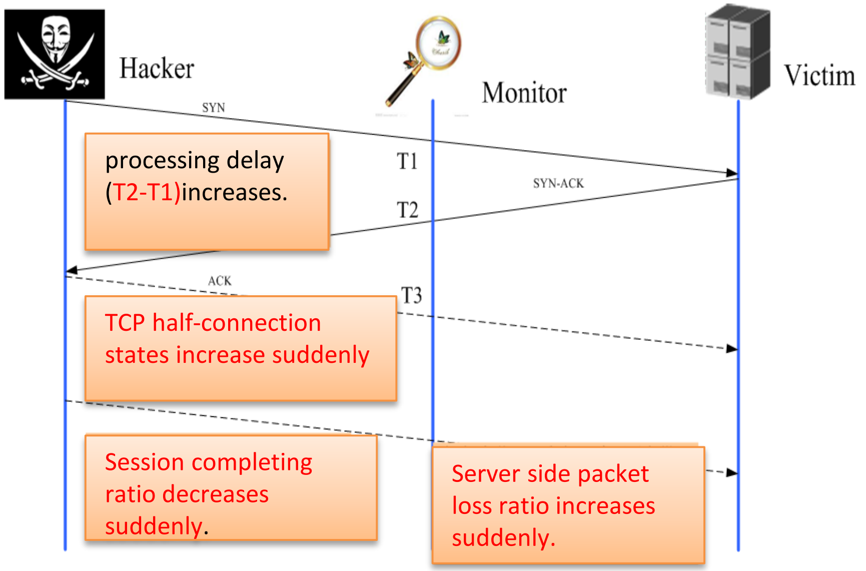
- Standard IEs
- An example of IEs for security



- Information Model covers nearly all common flow collection use cases:
  - "traditional 5 tuple": sourceIPv4Address, destinationTransportPort, etc.
  - packet treatment: ipNextHopIPv4Address, bgpDestinationAsNumber, etc.
  - Timestamps to nanosecond resolution: flowStartSeconds, flowEndMilliseconds, observationTimeMicroseconds, etc.
  - IPv4, IPv6, ICMP, UDP, TCP header fields: ipTTL, icmpTypeIPv6, tcpSequenceNumber, etc.
  - Sub-IP header fields: sourceMacAddress, wlanSSID, mplsTopLabelStackSection, etc.
  - Various counters: packetDeltaCount, octetTotalSumOfSquares, tcpSynTotalCount, etc.
  - Flow metadata information: ingressInterface, egressInterface, flowDirection, ingressVRFID, selectorID, etc...
- >400 defined at http://www.iana.org/assignments/ipfix

12 May 2014 RIPE 68 Warsaw - IPFIX Tutorial 31

A syn flood attack process



processing delay (T2-T1)increases.

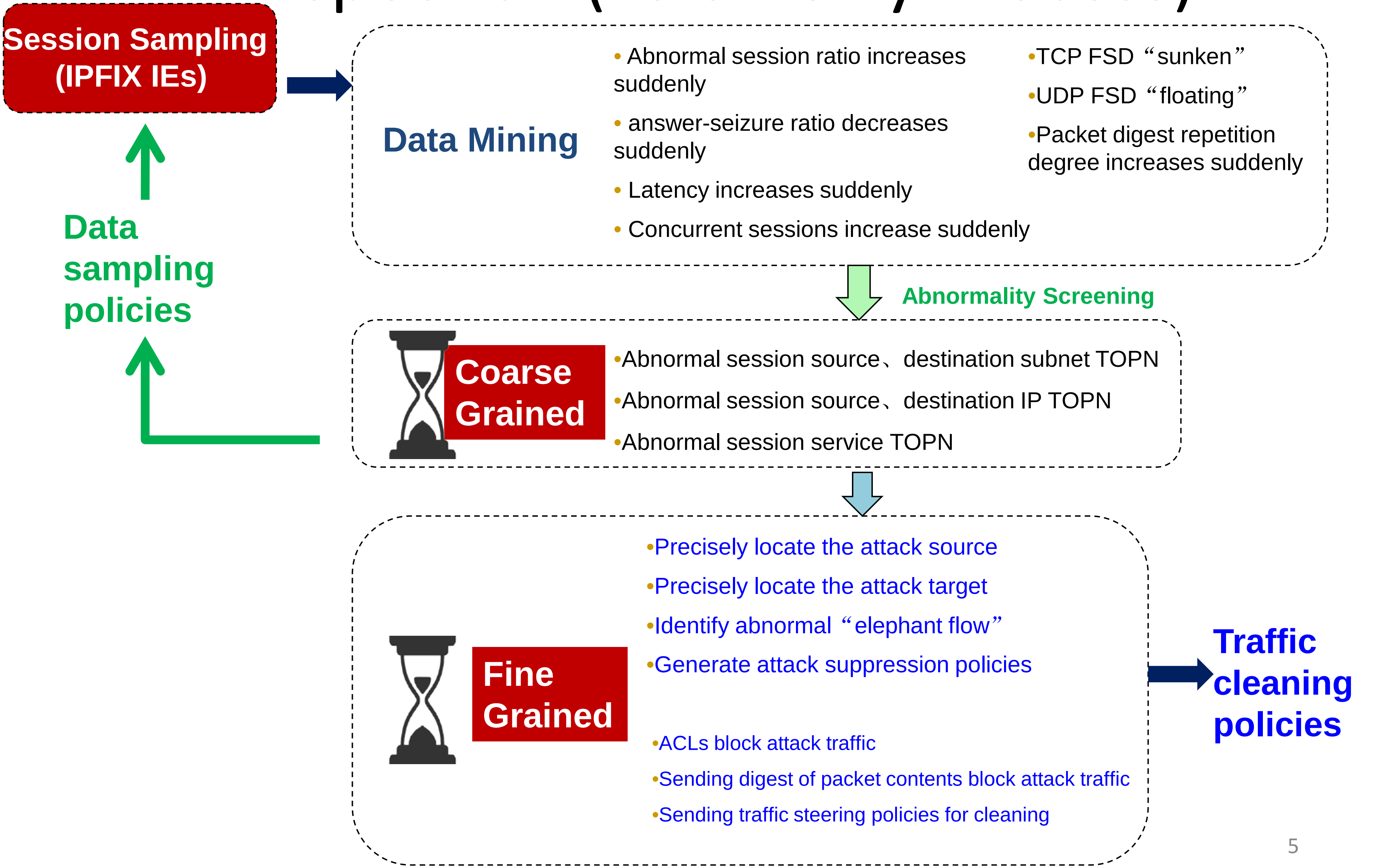
TCP half-connection states increase suddenly

Session completing ratio decreases suddenly.

Server side packet loss ratio increases suddenly.

Key Metrics for Attack Detection	**IP 5 tuple**	**Session delay(handshake time T2-T1）**	**Abnormal connection state(Terminate, half-connection, RST, ACK/SYN-ACK)**	Fragment packet statistics	DNS statistics (UDP Flood）
	Session completing ratio	Session packet loss ratio	Packet payload signature	Session packet statistics (FSD, Flow Size Distribution)	Others...

Major Steps of Using IPFIX in DDoS Attack Inspection (Telemetry Process)



Session Sampling (IPFIX IEs)

Data Mining

- Abnormal session ratio increases suddenly
- answer-seizure ratio decreases suddenly
- Latency increases suddenly
- Concurrent sessions increase suddenly
- TCP FSD “sunken”
- UDP FSD “floating”
- Packet digest repetition degree increases suddenly

Abnormality Screening

Coarse Grained

- Abnormal session source、destination subnet TOPN
- Abnormal session source、destination IP TOPN
- Abnormal session service TOPN

Data sampling policies

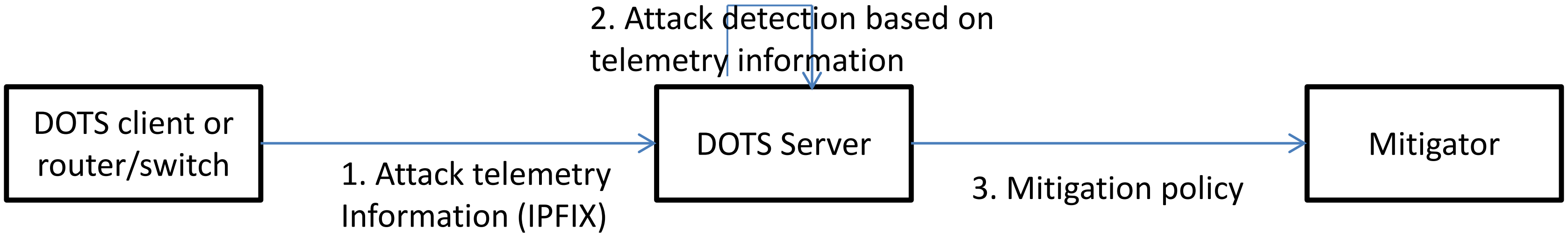
Fine Grained

- Precisely locate the attack source
- Precisely locate the attack target
- Identify abnormal “elephant flow”
- Generate attack suppression policies

- ACLs block attack traffic
- Sending digest of packet contents block attack traffic
- Sending traffic steering policies for cleaning

Traffic cleaning policies

Major Steps of Using IPFIX in DDoS Attack Inspection (DOTS Elements Interaction)



2. Attack detection based on telemetry information

DOTS client or router/switch

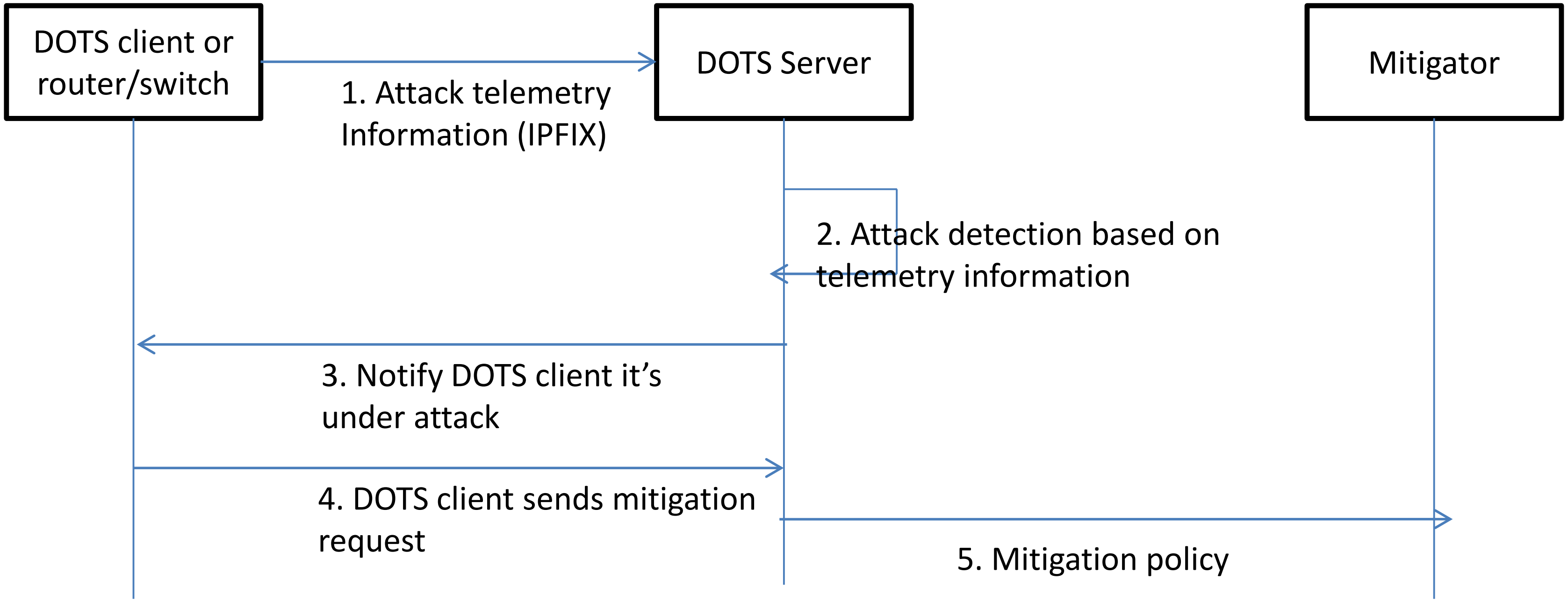
1. Attack telemetry Information (IPFIX)

DOTS Server

3. Mitigation policy

Mitigator

Mode 1 – DOTS Server Enabled Mitigation



DOTS client or router/switch

DOTS Server

Mitigator

1. Attack telemetry Information (IPFIX)

2. Attack detection based on telemetry information

3. Notify DOTS client it’s under attack

4. DOTS client sends mitigation request

5. Mitigation policy

Mode 2 – DOTS Client Enabled Mitigation

Challenges of Using IPFIX in DDoS Attack Inspection

- **Packet sampling can not be aware of the session related information:** statistics, status, duration, other metrics;
- **Low packet sampling probability for small session:** the smaller packet sampling probability leads to big difficulty to detect small session based attacks (SYN-Flood, ACK-Flood, etc)**;**
- **Lack of support for correlated bidirectional sampling:** today's packet sampling is independently applied in each direction and leads to the difficulty to correlate the statistic of both sides. Example: SNMP/DNS Reflected Amplification;
- **Current information is not sufficient:** without detailed information, it's impossible to distinguish some attacks, such as IP fragment attack and Slowloris HTTP attack, from the ordinary ones

Solution: Security Extension of IPFIX

IPFIX Security Extension IEs

- **Upstream/downstream counters for packets and octets**
  - pktUpstreamCount
  - pktDownstreamCount
  - octetUpstreamCount
  - octetDownstreamCount
- **ICMP echo/reply counters**
  - icmpEchoDeltaCount
  - icmpEchoReplyDeltaCount
- **TCP connection anomaly information**
  - A new values is added to FlowEndReason: 0x06 protocol exception timeout
  - tcpControlStateBits
  - tcpOutoforderTotalCount
  - tcpPayloadOctetTotalCount

- Network session related: completing ratio, abnormal session ratio, concurrent session ratio, half-connection, etc.
- Apply for DDoS flood attack inspection for syn, udp, icmp, dns, ntp, and so on.

IPFIX Security Extension IEs (Continue)

- **Fragment statistic**
  - fragmentPacketDeltaCount
  - fragmentFirstTooShortDeltaCount
  - fragmentFlagErrorDeltaCount

DDoS Fragment attack inspection

- **Flow Metric Distribution**
  - octetVariance
  - flowTimeIntervalVariance
  - flowSessionEndMilliseconds
  - flowTimeInterval
  - serverResponseTime
  - clientResponseTime
  - sessionResponseTime

- Session packet number/distribution, session size distribution, session running time and response time, session time distribution, etc.
- Apply for various DDoS flood attack inspection: syn, udp, dns, icmp, fragment, etc.

Next Steps

- Solicit comments;
- Keep on improving

Thanks!

Liang Xia (Frank)