Content

- Background
- Changes from last iteration
- Ideas
- Issues
- Next step

The goal of this presentation is to summarize things up and solicit comments as much as possible.
Background

• draft-fu-dots-ipfix-tcp-tracking-00 is a new iteration of draft-fu-dots-ipfix-extension-01

• The original draft proposes a set of IPFIX Information Elements that can be used for DDoS detection.

• The new iteration cuts off some Information Elements that are deemed unnecessary.
Changes from last iteration

draft-fu-dots-ipfix-extension-01
  fragmentPacketCount
  fragmentFirstTooShortCount
  fragmentFlagErrorCount
  fragmentOffsetErrorCount
  icmpEchoCount
  icmpEchoReplyCount
  octetVariance
  serverResponseTime
  clientResponseTime
  sessionResponseTime
  tcpControlStateBits
  pktTimeInterval
  pktTimeIntervalVariance
  tcpOutOfOrderTotalCount

draft-fu-dots-ipfix-tcp-tracking-00
  tcpHandshakeSyn2SynAckTime
  tcpHandshakeSynAck2AckTime
  tcpHandshakeSyn2AckRttTime
  tcpConnectionTrackingBits
  tcpPacketIntervalAverage
  tcpPacketIntervalVariance
  tcpOutOfOrderDeltaCount
Ideas

• The focus of the new draft is to detect anomaly in TCP traffics
  • It’s easier to tell apart anomaly if information is collected from massive TCP connections.
  • Collected information will be processed using big data technologies, to monitor for behavioral changes.

• Why choose IPFIX?
  • We need a way to export this information.
  • IPFIX is standard and widely supported.
  • Need to define several new Information Elements on IPFIX.
TCP connections Tracking

Client

SYN-ACK

ACK

FIN

ACK

FIN

Server

SYN

tcpHandshakeSyn2SynAckTime

tcpHandshakeSynAck2AckTime

tcpConnectionTrackingBits

| 1 | 1 | 1 | 1 | 1 | 1 | 0 | ...
| 5 | 4 | 3 | 2 | 1 | 0 | 9 | ...

| S | S | A | F | A | F | A | ...
| Y | / | C | I | C | / | C | ...
| N | A | K | N | K | A | K | ...

+++++++

Some extra information:
- tcpPacketIntervalAverage
- tcpPacketIntervalVariance
- tcpOutOfOrderDeltaCount
Issues

• Asymmetric traffic
  • Asymmetric traffic reduces the applicability of the new IEs. The information can only be collected at convergent points.

• Performance concern
  • How well it scales depends on the power of the collecting device. It may limit the applicability of the new IEs.
Next step

• We appreciate the comments DOTS WG has given.

• Possible directions:
  • Direct submission to IANA IPFIX Registry?
  • Discussion in other WGs?
  • ...


Thanks