Biflow implementation support in IPFIX

draft-trammell-ipfix-biflow-00

(was: draft-boschi-ipfix-biflow-01)

http://www.ietf.org/internet-drafts/draft-trammell-ipfix-biflow-00.txt

Brian Trammell <bht@cert.org>

Elisa Boschi <elisa.boschi@hitachi-eu.com>

Wednesday, March 22, 2006

IETF 65 - Dallas, TX, USA

The Problem

- Bidirectional flow information useful for a variety of use cases
  - e.g. security monitoring
    - analyzing response to scanning activity
    - separating likely compromise from compromise attempt.
- Biflow matching often most convenient at Metering Process
  - symmetric routing situations
  - “white-box” Metering Processes attached at Layer 2
- Most obvious present method of biflow export is inefficient and supports no explicit association between biflow halves.

Terminology

- "IP Traffic Flow" [IPFIX-PROTO] definition applies to biflows as well as uniflows.
- "Uniflow" and "Biflow" are special cases of Flow (from -01):
  - *A Uniflow is a Flow … restricted such that the Flow must be composed only of packets sent from a single endpoint to another single endpoint.*
  - *A Biflow is a Flow composed of packets sent in both directions between two endpoints.*
  - *A Biflow may also be defined as composed from two Uniflows such that:*
    - *each Non-directional Key Field of each Uniflow is identical to its counterpart in the other, and*
    - *each Directional Key Field of each Uniflow is identical to its reverse direction counterpart in the other*

Existing: Record Adjacency

- First export the initiating flow, then export the respondent flow, if any.
- Simple to implement, requires no protocol changes at all.
- But…
  - Duplicates all Flow Key information.
  - No actual association between biflow halves.
  - Informal agreement not enforced by protocol, so Collecting Processes cannot rely on this method and need large biflow match buffers anyway.

Common Properties? (in -01)

- draft-boschi-ipfix-reducing-redundancy may provide another method.
- Key data in common properties, counter data in specific properties.
- May require extension to differentiate directions in specific data records.
- Still requires multiple records per biflow.

Multiple IEs?

- Use multiple identical counter IEs for biflow records.
- First instance of each counter record for forward direction, second instance for reverse direction.
- Semantics are troublesome:
  - Not compatible with measurement process treatment sequence as IE order.
  - Interactions with other usages of multiple IE counters are unclear.

Proposed: Single Record Biflows

- Define “forward” direction to be flow initiator, as determined by Metering Process; “reverse” direction to be flow responder.
- Define new reverse counter information elements.
- Efficient and unambiguous.
- Requires new information elements.
  - “reverse” is another IE-space dimension
  - may need to mitigate continued explosion of IEs

Changes since boschi-ipfix-biflow-01

- Removed directionDomain IE
  - reverse counters now have single set of semantics, always apply to packets sent by biflow responder.
- Extended biflow semantics discussion.
- Editorial changes from “hallway meetings” in Vancouver.
- Change of primary authorship.

Next Steps

- trammell-ipfix-biflow-01: by 31 March
  - terminology rework
  - expand treatment of reverse IEs
  - expand treatment of corner cases
  - add common properties section
  - other comments from Dallas
- trammell-ipfix-biflow-02: for Montreal
  - incorporate continued list discussion on issues raised here