IPFIX Mediation: Problem Statement

IPFIX IETF-77 March 23, 2010

draft-ietf-ipfix-mediators-problem-statement-08

Editor: Atsushi Kobayashi, Benoit Claise

Haruhiko Nishida, Christoph Sommer

Falko Dressler, Stephan Emile

History

- **-07 version went to IESG in January.**
- **AD Review started in February.**
  - Received technical and editorial comments from Dan.
- **IETF Last Call for -08 version started on March 1st.**
  - Received comments about security consideration section from SecDir: Yaron Sheffer.

Comments in AD Review

- **A few sections need further explanation.**
  - One-way delay in correlation function
  - Spatial composition in aggregation function
  - Data retention
- **Section 6.7. title "Exporting the Function Item" should be changed.**
  - ➔ Changed title "IPFIX Mediation Interpretation".
- **The protection of privacy and confidentiality should be added.**
  - ➔ Added bullet "Confidentiality protection and data integrity via IPFIX Mediation" in security consideration section.

Current -08 version already solved all comments.

Comments in IETF Last Call

Received 4 comments in security consideration.

All improvement will be included in next version -09.

- **Privacy concerns may be amplified when streams from multiple sources.**
  - ➔ New bullet "Privacy concerns on an IPFIX Mediator".

```
o  Privacy concerns on an IPFIX Mediator

      The probability to get specific end user's traffic generally
      increases by increasing the number of Observation Points.  An
      IPFIX Mediator collecting Flow Records from multiple Observation
      Points potentially raises the risk to privacy.  The IPFIX
      Mediator needs to apply appropriately anonymization or aggregation
      function to Data Records to avoid  violating privacy, when the
      purpose of traffic measurement is not to monitor specific end
      user's traffic trend.
```

Comments in IETF Last Call

- **In the case of multi-tenancy, each customer traffic data should be protected from one another.**
  - ➔ New bullet "Multiple tenant policy on an IPFIX Mediator".

o Multiple-tenancy policy on an IPFIX Mediator

An IPFIX Mediator handling traffic data from multiple tenants or customers needs to protect from one another traffic data. For example, an IPFIX Mediator needs to identify the customer's identifier, e.g., ingress interface index, network address range, VLAN ID, MAC address, and etc., when feeding customer's traffic data to a customer own dedicated IPFIX Collector. If the IPFIX Mediator can not identify each customer's traffic data, it may need to drop the Data Records. In addition, another technique to keep track of customer's identifier may be required when customer site are movable, e.g., in the case of virtual machine moving to another physical machine.

Comments in IETF Last Call

- **Confidentiality protection could be improved to more clearly.**
  - ➔ I will improve bullet "Confidentiality protection via an IPFIX Mediator".

> o Confidentiality protection via an IPFIX Mediator
>
> To ensure security of Data Records in transit, transport of Data Records should be confidentiality and integrity-protected, e.g. by using Transport Layer Security (TLS) [RFC4346] or Datagram Transport Layer Security (DTLS) [RFC4347]. However, an IPFIX Collector can not know whether received Data Records are transported as encrypted data between an Original Exporter and an IPFIX Mediator. If this information is required on the IPFIX Collector, it must be encoded in the IPFIX Mediator.

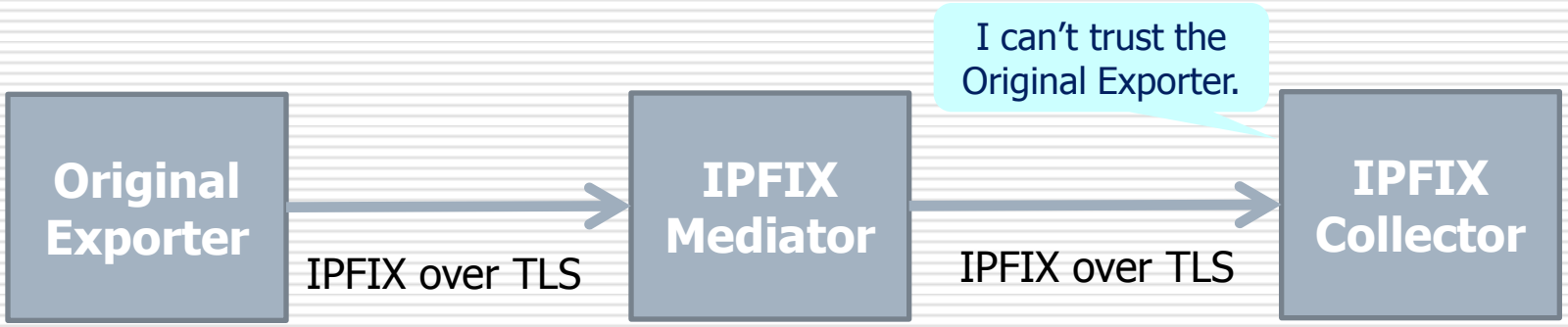
To be continued later to discuss about its solution in framework draft.

Comments in IETF Last Call

- **The trust model should be clarified.**
  - ➔ New bullet "Certification for an Original Exporter".

```
o  Certification for an Original Exporter

      An IPFIX Collector communicating via an IPFIX Mediator can not
      verify the identity of an Original Exporter directly.  If an
      Original Exporter and an IPFIX Collector are located in different
      administrative domains, an IPFIX Collector can not trust its Data
      Records.  If this information is required on the IPFIX Collector,
      it must be encoded in the IPFIX Mediator.
```



To be continued later to discuss about its solution in framework draft.

Next Step

- **IETF Last Call almost finished.**
  - I got go-ahead from SecDir.
- **Already prepared next version -09.**
  - http://www.nttv6.net/~akoba/wdiff-ps08-ps09-02.htm
- **Next Step: IESG review**