

IP Flow Anonymisation Support

draft-boschi-ipfix-anon-04

Elisa Boschi, Brian Trammell – Hitachi Europe

Background: Anonymisation and IPFIX

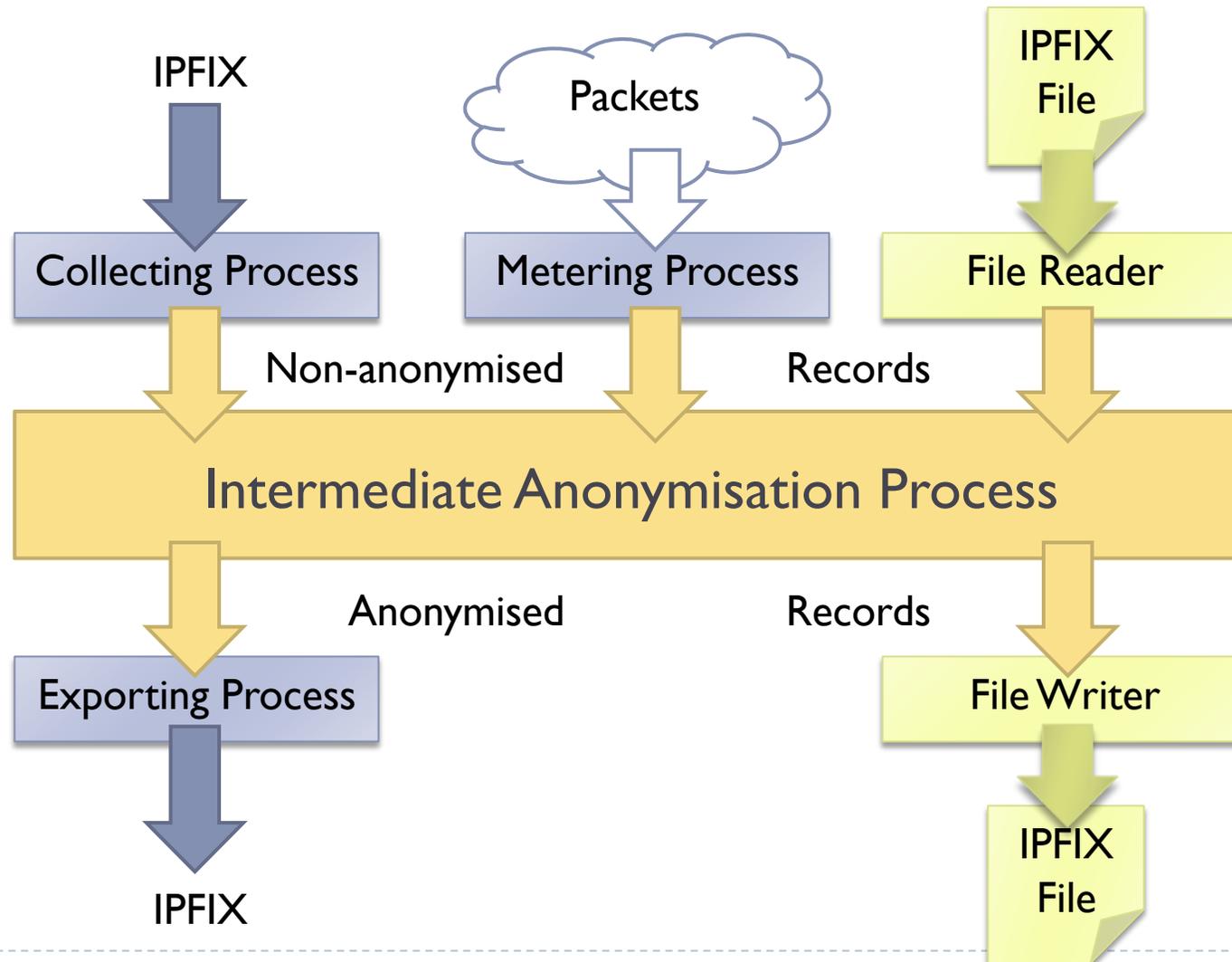
- ▶ **Anonymisation support long-standing IPFIX requirement**
 - ▶ IPFIX requirements (§6.7 RFC 3917)
 - ▶ Mediation function (§5.6 draft-ietf-ipfix-mediators-problem-statement)
 - ▶ Anonymous storage (§5.7 RFC 5655)

- ▶ **Adopted as WG item after Stockholm**

- ▶ **Published draft-ietf-ipfix-anon-00 for Hiroshima**
 - ▶ added Security Considerations section



Anonymisation Data Paths



-anon-00 contents (§§1-4)

▶ 1. Introduction

- ▶ the usual front matter

▶ 2. Terminology

- ▶ incorporates IPFIX terminology by reference
- ▶ may need additional anonymisation-specific terms [TODO]

▶ 3. Categorization

- ▶ defines broad categories (countability, reversibility) for anonymisation techniques in terms of *properties of the resulting information*.

▶ 4. Anonymisation

- ▶ defines general anonymisation techniques for flow data by type of IE: IP/Hardware address, timestamp, counter, etc.



-anon-00 contents (§§5-6)

- ▶ 5. Parameters for the Description of Anonymisation Techniques
 - ▶ defines parameters for configuring anonymisation
- ▶ 6. Anonymisation Export Support in IPFIX
 - ▶ defines anonymisation metadata export based on Options, three IEs:
 - **anonymisationTechnique** describes techniques in terms of properties of resulting information, as defined in Categorization, section 3.
 - **anonymisationStability** describes temporal comparability of values of a given field
 - **informationElementIndex** allows binding to specific instances of IEs within a template



-anon-00 contents (§§7-10)

▶ 7. Applying Anonymisation Techniques to IPFIX Export and Storage

- ▶ defines how processes are arranged for anonymisation
- ▶ defines guidelines for exporting anonymised data using IPFIX
 - i.e., avoidance of header and options data information leakage

▶ 8. Examples

- ▶ [TODO]

▶ 9. Security Considerations



- ▶ Clarify role of anonymisation.
- ▶ Discuss mapping lifetime tradeoffs.
- ▶ Reference guidelines in §7.2 for non-export of anonymisation-compromising information

▶ 10. IANA Considerations

- ▶ Enumerate information elements to be created.
-



Next steps

- ▶ Incorporate received commentary on additional anonymisation techniques.
 - ▶ Reverse truncation, leaving low-order bits intact.
 - ▶ Prefix-preserving mappings with identity map for low order bits.
- ▶ Incorporate received commentary on additional guidelines.
 - ▶ Elimination of special-use address space [RFC 3330] in data before anonymisation.
- ▶ Solicit additional commentary on both.
- ▶ Submission to IESG before Maastricht meeting
 - ▶ (June 2010, according to charter)

