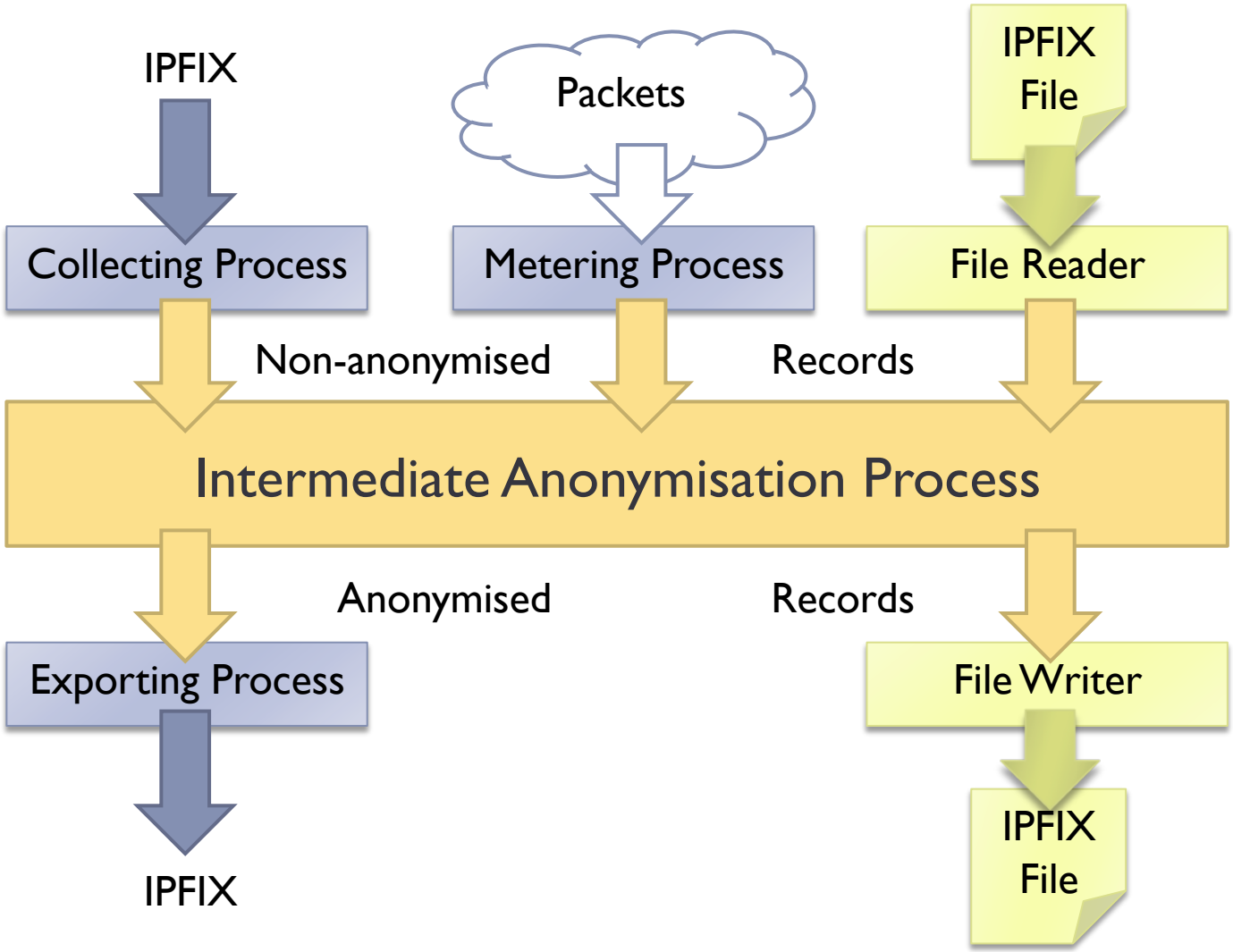
IP Flow Anonymisation Support
draft-ietf-ipfix-anon-02

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
- WGLC completed 20 March

Anonymisation Data Paths



-anon-02 contents (§§1-4)

- 1. Introduction
- 2. Terminology
- 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.
  - Add reverse truncation.
  - Discuss "low-order unchanged": protects against scanning attacks.
  - Clarify: permutation is not always random.

-anon-02 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.
    - **anonymisationFlags** describes temporal comparability of values of a given field, plus options such as perimeter anonymisation and low-order unchanged.
    - **informationElementIndex** allows binding to specific instances of IEs within a template
  - Add reverse truncation, noise and offset techniques to anonymisationTechnique.

-anon-02 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
  - Added special-use addressing guidelines.
  - Added perimeter anonymisation
    - different techniques for addresses inside and outside a given network
- 8. Examples
- 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

- WGLC elapsed, but we need more comments!
  - Open question: do we adequately address hash-based permutation?
- Submission to IESG before Maastricht meeting
  - (June 2010, according to charter)