IPFIX – current trends and approaches for secured data transmission

Brussels, Belgium
28. September 2009

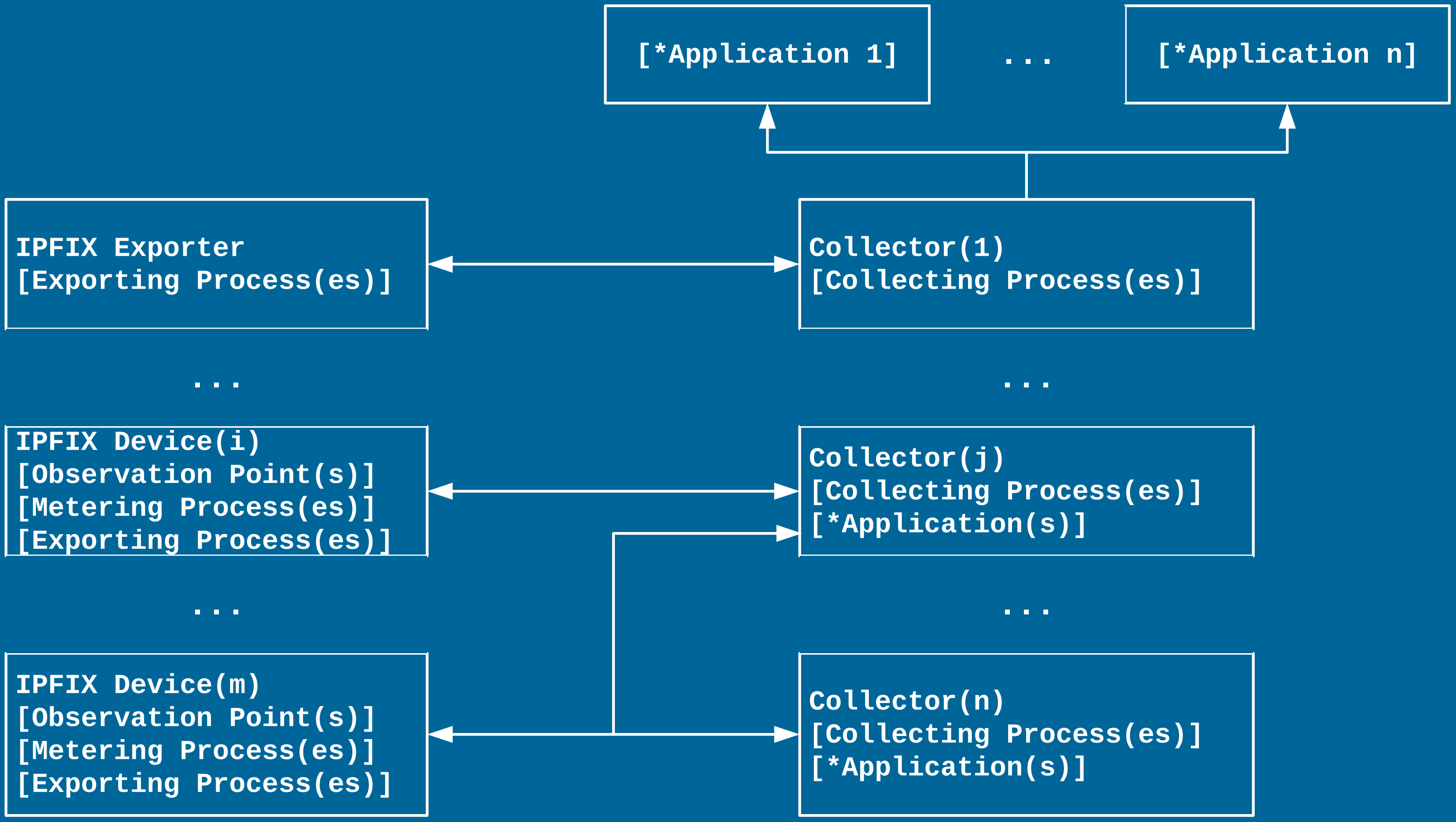
Oliver Jung, Carsten Schmoll
jung@ftw.at, carsten.schmoll@fokus.fraunhofer.de

IPFIX fundamentals

- IPFIX = IP Flow Information eXport
  - Standardized by IETF as a predecessor to NetFlow protocol
  - Push-based protocol for exporting IP flow related information
  - Very flexible due to use of data templates
  - Transport protocol can be SCTP,TCP,UDP
  - Data Model defines many std. fields; allows extension to own information elements too
  - http://www.ietf.org/html.charters/ipfix-charter.html

IPFIX reference model

- Various possible scenarios that can exist in an IPFIX system (EP:CP = 1:1, n:1, 1:n)



IPFIX working group standards

- IPFIX working group defined (among others):
  - Architecture for IP Flow Information Export (RFC 5470)
  - Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information (RFC 5101)
  - Information Model for IP Flow Information Export (RFC 5102)
  - Guidelines on implementation (RFC 5153), on testing (RFC 5471), reducing redundancy (RFC 5473), and exporting type information (RFC 5610)

IPFIX threats

- Disclosure of IP flow information data
  - IPFIX flow records can contain Personal Identifiable Information (PII)
  - PII should be kept confidential parties (exporting process and colleting process)
  - Observation of IPFIX flow records gives an attacker information about
    - active flows in the network,
    - communication endpoints and traffic patterns
  - IPFIX records can also reveal critical information about network infrastructure -> exploitable for future attacks

IPFIX threats

- Flooding attack against collecting process
  - CP is always listening for flow records to arrive data and thus can be flooded
- IPFIX state exhaustion: creation of too many observation domains, templates, etc.
- IPFIX parse/fuzzing attacks: sending malformed IPFIX messages

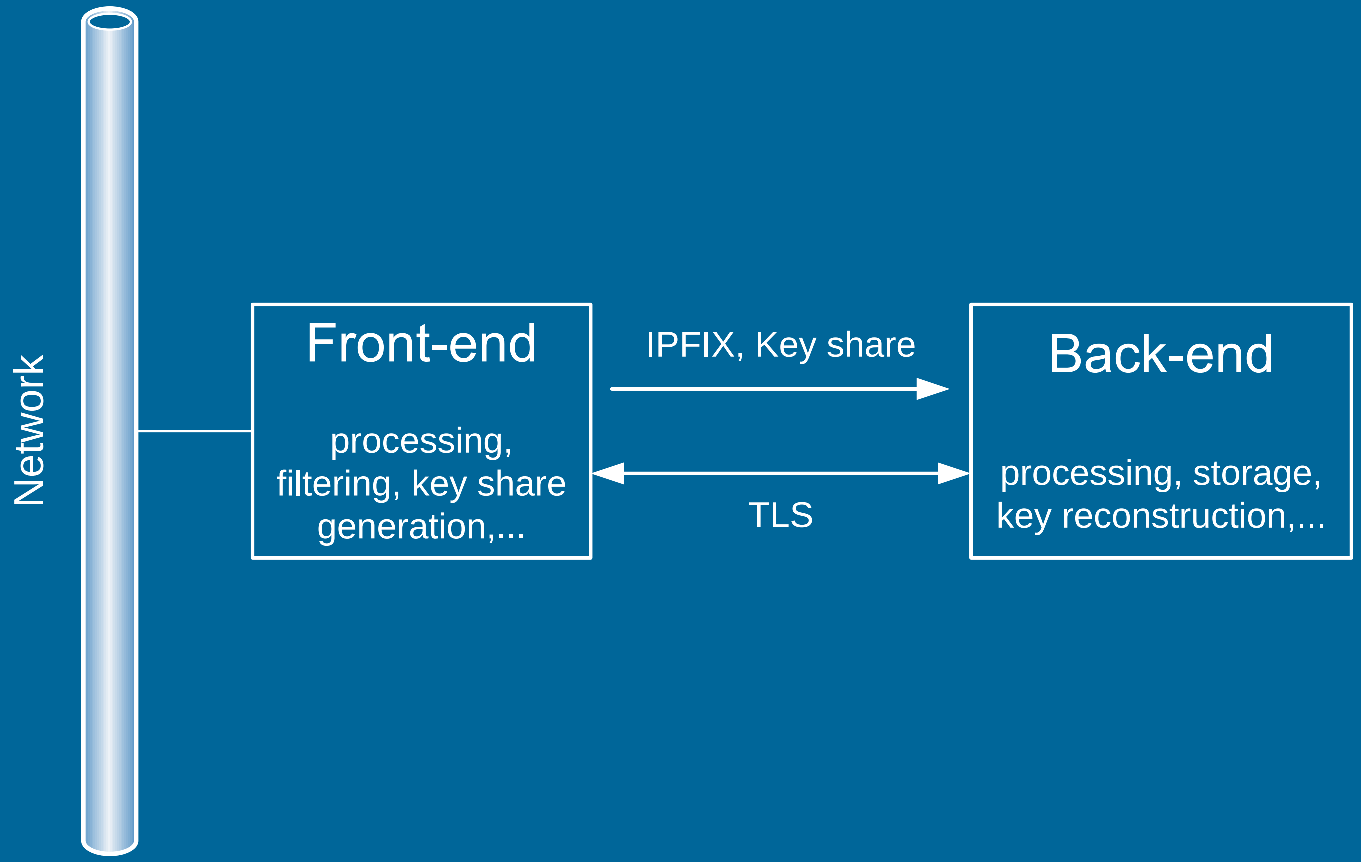
IPFIX security

- Secure data transmission:
  - – Handled on transport layer by IPSec or TLS
  - – Both support mutual authentication on Server/Client-level with host keys and assigned certificates
  - – This secures the data on the way between IPFIX Exporting Process and IPFIX Collecting Process – but not further
- What if collected data is to be stored and evaluated only later?

Security approaches

- Option 1:
  - Use encrypted database filled by IPFIX Collecting process (CP)
- Option 2:
  - Send already encrypted data over IPFIX and decrypt only later on real use of the data
- In the PRISM project we follow the second approach – advantages:
  - Easier to use different encryption keys per CP
  - The Exporting process can decide when to make the data decryptable at all by sending the key material

PRISM architecture



Network

Front-end

processing, filtering, key share generation,...

IPFIX, Key share

TLS

Back-end

processing, storage, key reconstruction,...

Technical realisation

- Send blobs of binary encrypted data via IPFIX to CP inside a new Information Element (IE) „encrypted data block„
  - – CP may store these blobs in a database or in a file (c.f. upcoming IPFIX file standard)
  - – If key material is available then decryption can take place
  - – Our recommendation is to format the data inside the encrypted blobs as IPFIX records!
    - That way decrypted material can be handled also by an IPFIX CP

IPFIX encryption keys

- Transport of the key material can also be done inline via IPFIX with a separate IE „key share“
  - Key shares are protected by the TLS transport
  - The CP can reassemble key material by itself,
  - decrypt selected data blocks and decode them
- The PRISM project will implement, test and benchmark such a system
- Applications will involve use for
  - IDS, data retention, and others.

Key share threats and vulnerabilities

- Flow records are protected from unauthorized access on the backend
- Attacks against encrypted traces (key recovery, traffic analysis,…)
- Key shares are only provided in case of a suspicious event
- Insider attack on key share is possible:
  - Attacker injects bogus IP packets with suspicious event characteristics
  - Front end can not distinguish between bogus packets and “proper” attack packets

Securing the IPFIX environment

- For safeguarding the PRISM environment including the IPFIX exporting and collecting process it is
  - recommended to protect the whole domain by firewalls on the IP+port level,
  - secure the EP and CP by X.509-based certificates (mandated in RFC 5153),
  - and allow access to the involved machines only to authorized personnel (minimum: user/password, better certificate-based access only)

Next steps

- A comprehensive security assessment is currently performed for the PRISM system
- System improvements will be considered if necessary
- Results including the potential identification of vulnerabilities will be part of the upcoming deliverable D2.3.2

Finish

Thanks for your interest!

Questions?