IPFIX/PSAMP: What Future Standards Can Offer to Network Security

Fraunhofer Institute for Open Communication Systems

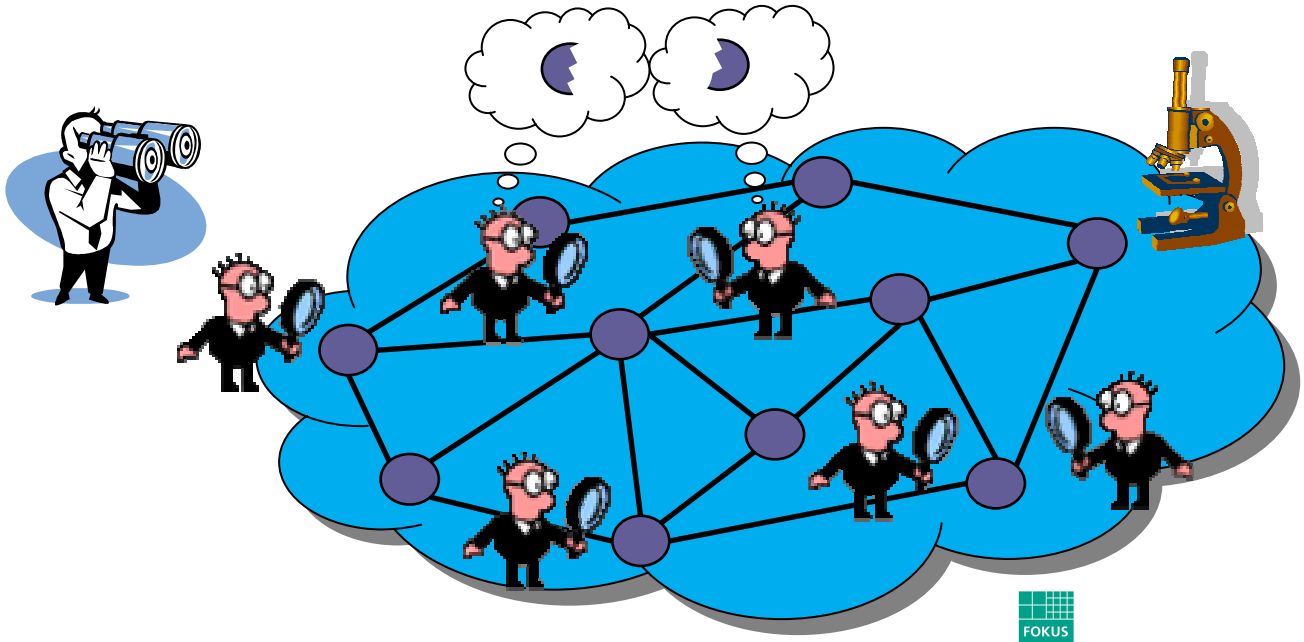
Tanja Zseby, Elisa Boschi, Thomas Hirsch, Lutz Mark

zseby@fokus.fhg.de

Measurement Requirements for Network Security

Goal: Detect deviations from normal traffic behavior

- Measurement requirements
  - **Network-wide**: get information from multiple observation points
  - **Flexible**: change viewpoints
  - **Shareable**: provide comparable and shareable results



Existing Solutions

- Specialized Hardware
  - + Extra resources to capture flow and packet data
  - + Detailed post-incident analysis possible
  - - Huge amount of measurement data ➔ high analysis effort
  - - Network installation required ➔ operators distrust new devices
  - - High costs ➔ prevent network-wide deployment
- SNMP
  - – Useful, but too coarse grained information
- Proprietary measurement tools
  - > 400 different tools (academia, research, operators, etc.) ➔ www.ist-mome.org
  - - Require additional devices ➔ prevent network-wide deployment
  - - Different input/output formats ➔ hard to share and compare
- Cisco NetFlow
  - + Integrated in routers ➔ network-wide deployment
  - - Fixed flow definition, no packet data ➔ limited flexibility
  - - High resource consumption ➔ Router performance degradation
  - - UDP transport ➔ potential data loss, no congestion control

IETF Standardization Efforts: IPFIX

IPFIX - IP Flow Information EXport

- Protocol for flow information export
  - Exports flow data from routers and probes (IPv4, IPv6)
  - Works on top of UDP, TCP or SCTP
  - Similar to Cisco NetFlow but much more flexible
- Upcoming IETF Standard
  - Active IETF working group
  - Protocol draft in last call
  - First Implementations exist
- Target Applications [RFC3917]
  - Usage-based Accounting
  - Traffic Profiling
  - Traffic Engineering
  - **Attack/Intrusion Detection** ←
  - QoS Monitoring

IPFIX Details

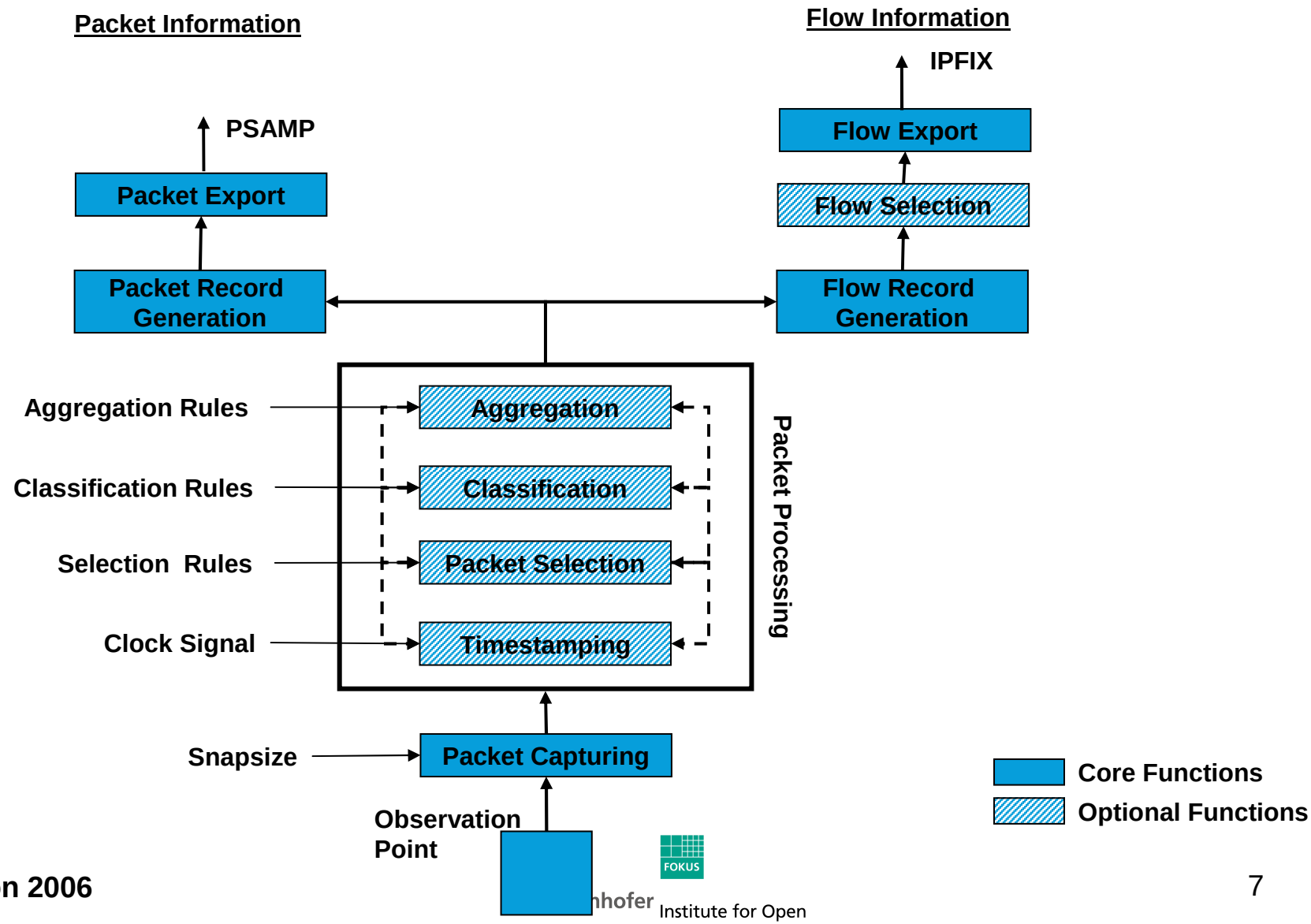
- Template-based approach
  - **Template Records**: define structure of Data Records
  - **Data Records**: contain parameter values
  - **Option Template Records**: provide additional information for Collectors
- Push-Model
  - Flow records pushed from exporter to collector
  - Trigger not defined in IPFIX
    - Measurement configuration out of scope
    - Flow termination criteria currently used, but others possible
- Information Elements (IEs)
  - Base sets of IEs defined in IPFIX-INFO, PSAMP-INFO
  - Attributes that can appear in IPFIX records
  - Vendor-specific IEs can be defined

IETF Standardization Efforts: PSAMP

PSAMP - Packet Sampling

- Exporting packet information with IPFIX
  - IEs for reporting packet header and payload
  - PSAMP IEs defined in draft-ietf-psamp-info-04.txt
  - PSAMP Framework in draft-ietf-psamp-framework-10.txt
- Packet selection methods
  - Filtering: deterministic selection based on packet content
  - Sampling: random or deterministic selection
  - PSAMP Schemes in draft-ietf-psamp-sample-tech-07.txt

IPFIX/PSAMP Measurement Model



What IPFIX/PSAMP can offer to NW Security

- Network-wide measurements
  - Measurement results from routers
  - No extra devices required
  - Different transport protocols (e.g. for congestion control)
- Highly flexible measurement definition
  - Arbitrary packet and flow information, highly flexible flow definition
  - Data selection techniques
  - Extensible information model
- Comparable and shareable data
  - Standardized data format
  - Different aggregation levels and sampling to enhance privacy
  - Secure data exchange (e.g. among domains)

IPFIX applicability statement: draft-ietf-ipfix-as-10.txt

Reporting Flow Statistics with IPFIX

That's what IPFIX was designed for!

- Very flexible flow definition
  - Any set of packets with "common properties" defined by flow keys
    - Packet header fields (e.g. destination IP address)
    - Packet properties (e.g. number of MPLS labels)
    - Packet treatment (e.g. output IF)
  - Information elements usable as flow keys defined in IPFIX-INFO
    - All IPv4 header fields (except checksum)
    - Main IPv6 header fields (addresses, next header, flow label, etc.)
    - Main transport header fields (UDP, TCP ports, sequence num., ICMP types)
    - Some sub IP header fields (MAC addresses, MPLS labels, etc.)
  - Flow termination criteria (currently used)
    - Idle timeout (no activity)
    - Active timeout (active, but max lifetime expired)
    - End of Flow detected (e.g. TCP FIN observed)
    - Forced end (external event, e.g. shut down of the Metering Process)
    - Cache full (lack of resources)

Reporting Flow Statistics with IPFIX

- Variety of information elements to report flow characteristics
  - Counters (e.g. bytes, packets, delta and total counters)
  - Timestamps (flow start, end, duration)
  - Statistics (min/max pktlength, min/max TTL, TCP flags, options)
  - Others (e.g. flow end reason)
- Per-flow TCP Flag counters
  - Recently introduced in IPFIX-INFO
  - E.g. tcpSynTotalCount, tcpFinTotalCount
  - Useful for detection of claim&hold attacks (e.g. SYN flood)

Bi-directional Flows

- Reporting both directions of a communication is useful for NW security
  - Connection status: incomplete connections can indicate attacks
  - Check request/response pairs (DNS, etc.)
- BUT: IPFIX currently reports each direction as separate flows ➔ How to report bi-directional flows?
- With standard IPFIX (without extensions)
  - Approach 1: Two records with record adjacency
    - unidirectional flow records adjacent to each other, collector reassembles
    - + extremely simple
    - - maintaining right ord
    - set of properties
    - Flow records (for each direction) carry individual uniflow properties (references keys by commonPropertiesID)
    - + more efficient
    - - additional resources for managing commonPropertiesID (at exporting and collecting process)
    - - three records required (instead of two)
- With IPFIX extension
  - Definition of new IEs for reverse direction
  - Re-use existing IEs and use special vendor ID to separate forward and backward direction
- Approaches currently discussed in draft-trammell-ipfix-biflow-02.txt ➔ best method will be selected

SEE BI-FLOW TALK

Packet Captures

- IPFIX: only header information
  - Define each packet as separate flow
  - IP, transport header, and some sub IP information per packet
  - Flow keys reported for each packet ➔ inefficient
- IPFIX improved export
  - Sharing flow key information among data records
  - ➔ Methods discussed in reduced redundancy draft
- With PSAMP
  - Header: ipHeaderPacketSection
  - Payload: ipPayloadPacketSection
  - Sub IP: dataLinkFrameSection, mplsLabelStackSection, etc.
- Data reduction
  - Aggregation of flows
  - Packet selection methods ← **PSAMP**

PSAMP Packet Selection Schemes

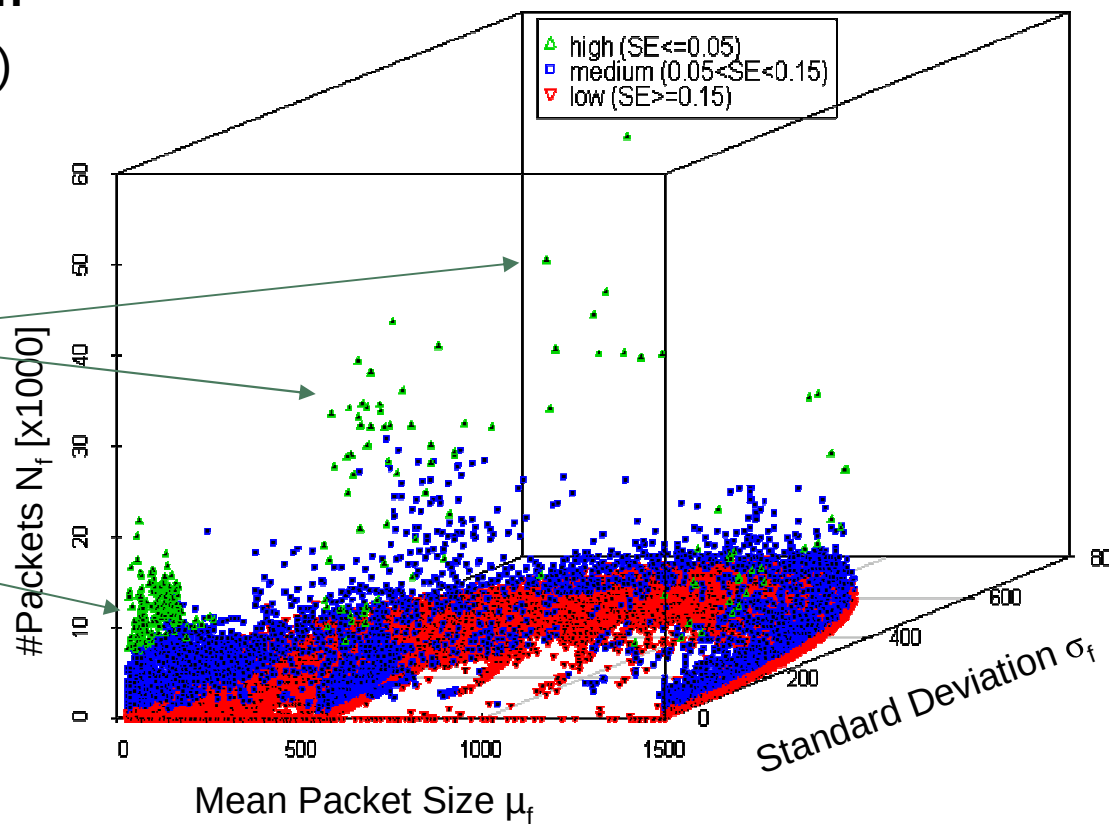
- PSAMP offers basic packet selection techniques
  - Filtering: deterministic selection based on packet content
    - Mask/match filter
    - Hash-based selection
    - Router state filter
  - Sampling: random or deterministic selection
    - Systematic count-based
    - Systematic time-based
    - Random n-out-of-N
    - Random uniform probabilistic
    - Random non-uniform probabilistic
    - Random non-uniform flow-state
- Packet selection possible at different points in measurement process
- Concatenation of selectors possible (e.g. for stratified sampling)
- Flow sampling
  - Allowed in IPFIX architecture
  - Currently not defined in PSAMP

Sampling Example: Achievable Accuracy

Example: Flow volume estimation

- PSAMP random n-out-of-N (5%)
- Sampling ***before*** classification

C/C/RN, Case B, f=5%, S24D24



High accuracy for large flows

High accuracy for flows with small variation

$$SE_{rel} = \frac{\sqrt{\frac{N \cdot N_f}{n} \cdot \left(\sigma_{x_f}^2 + \mu_{x_f}^2\right) - \frac{N_f^2}{N} \cdot \mu_{x_f}^2}}{N_f \cdot \mu_{x_f}}$$

➔ **Large flows detectable with very small effort**

➔ **MORE ON SAMPLING IN PANEL**

IPFIX Configuration

- Past: Configuration was out of scope for IPFIX
  - WG wanted to concentrate on protocol spec
  - Proprietary CLI configuration of IPFIX processes always possible
- Now: Several Proposals for IPFIX configuration
  - IPFIX MIB (draft-dietz-ipfix-mib-00.txt)
    - Monitoring IPFIX exporters and collectors (configuration, statistics)
    - Potentially configuration of IPFIX exporters and collectors
  - IPFIX XML configuration (draft-muenz-ipfix-configuration-00.txt)
    - Data model for configuration parameters of IPFIX devices
    - Configuration by Netconf, SOAP, etc.
  - NSIS proposal (draft-dressler-nsis-metering-nslp-04.txt)
    - Path-coupled dynamic configuration of Metering Entities
    - Metering NSIS Signaling Layer Protocol NSLP (M-NSLP),
    - Cooperation between NSIS and IPFIX required

Storage of Data

- Standardized format for storing IPFIX data
  - Post-incident analysis (forensics, research)
  - Sharing information (e.g. among providers)
  - Provide training data (traces with “normal” behavior)
- IPFIX file format draft (draft-trammell-ipfix-file-01.txt)
  - Collects Requirements
    - Extensibility (multiple record types, new fields, etc.)
    - Self-Description (interpretation without additional knowledge)
    - Data Integrity and Error Correction
    - Authentication and Confidentiality
    - Indexing and Searching
    - Anonymization
- Goal: propose an IPFIX file format
  - Evaluation of existing solutions (ARGUS, SiLK, etc.)
  - Collection of requirements

Support in Routers

- IPFIX (Flow Export)
  - First Implementations exist
  - Cisco plans IPFIX compliance
- Packet Export
  - Resource limitation on routers prevent full packet export
  - Packet export from sampled data possible
  - Tradeoff between reported amount of information (#packets, snapsize) and required resources
- Sampling Methods
  - Cisco: random 1-in-K, systematic sampling
  - Conformance to PSAMP if one PSAMP scheme is supported
  - No information about support for further schemes

Conclusion

- IPFIX/PSAMP
  - Protocol to export flow and packet information
  - Upcoming standard
  - Can integrate data selection methods
- Provides measurement results
  - Network-wide
  - Flexible
  - Shareable

➔Powerful standards for network security

FOKUS Open Source IPFIX library available at:

http://ants.fokus.fraunhofer.de/libipfix/

Thank you for your attention!

Fraunhofer Institute for Open Communication Systems