A flexible DDoS detection System using IPFIX

Thomas Hirsch, **Tanja Zseby**
Flocon Workshop 2008
January 07-10, 2008
Fraunhofer Institute FOKUS

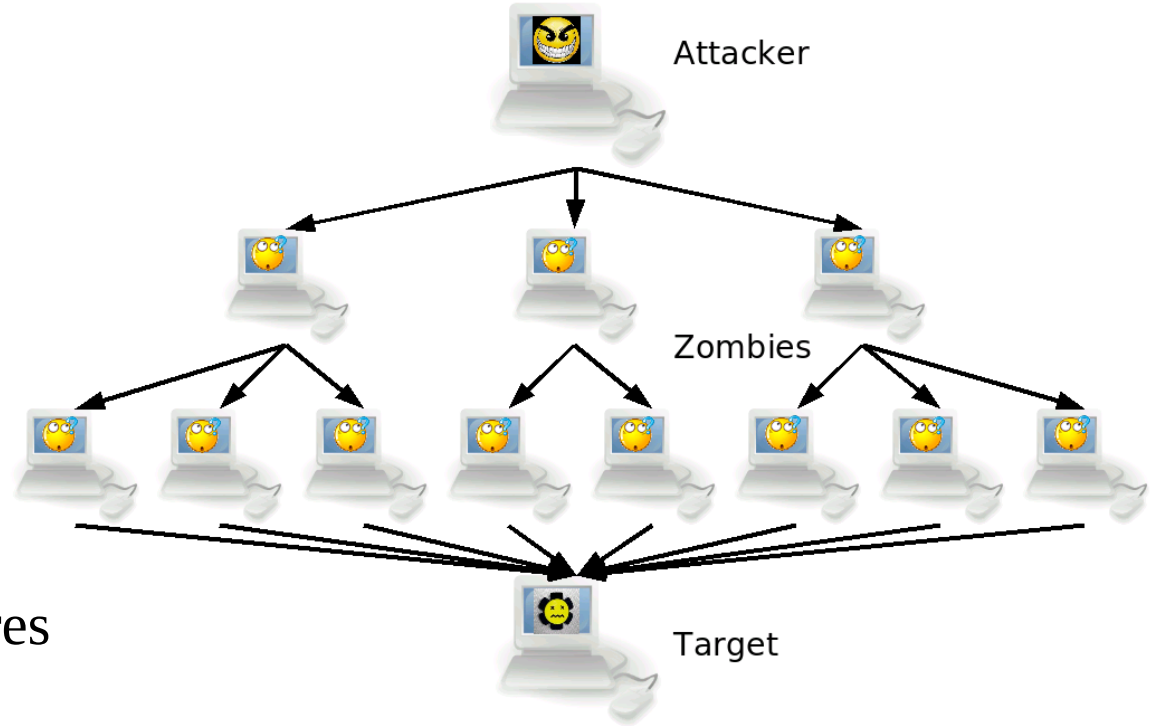
This work was done in the context of the NetCentric Security project. NetCentric Security is a project of Deutsche Telekom Laboratories supported by the Fraunhofer Institute for Open Communication Systems (FOKUS).

Outline

- Introduction:
  - Denial of Service – The Internet Bottleneck problem
- The Architecture
  - System Architecture
  - OpenIMP platform
  - DDos Detection Metrics
  - Detection using Latent Semantic Indexing and Clustering
- Conclusion:
  - How does IPFIX support the integration of new metrics

The DDoS Problem

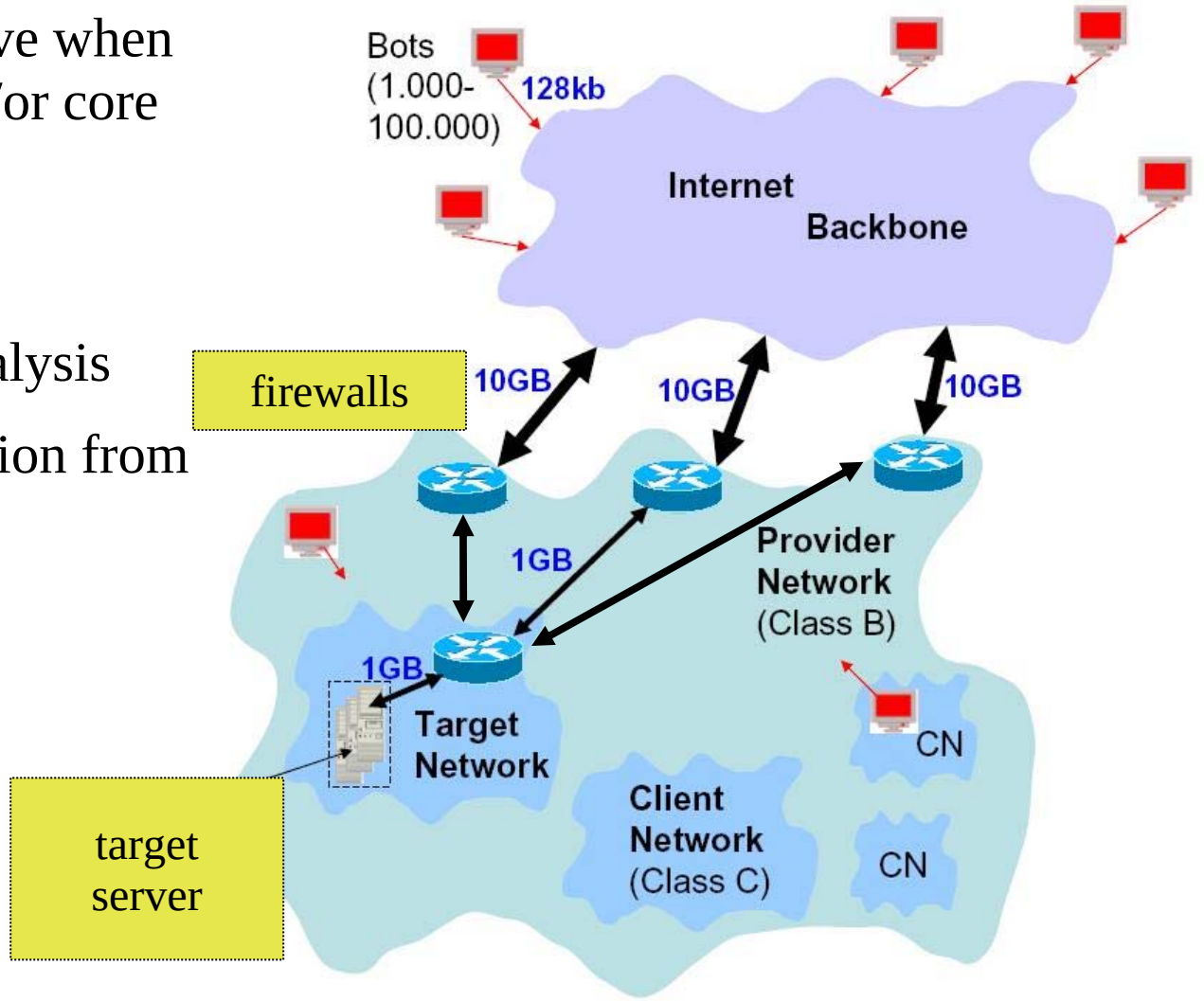
- DDoS Flooding attacks saturate the final link(s)
- Filters are only effective before the bandwidth becomes scarce
- Hence, the end user can hardly take effective measures



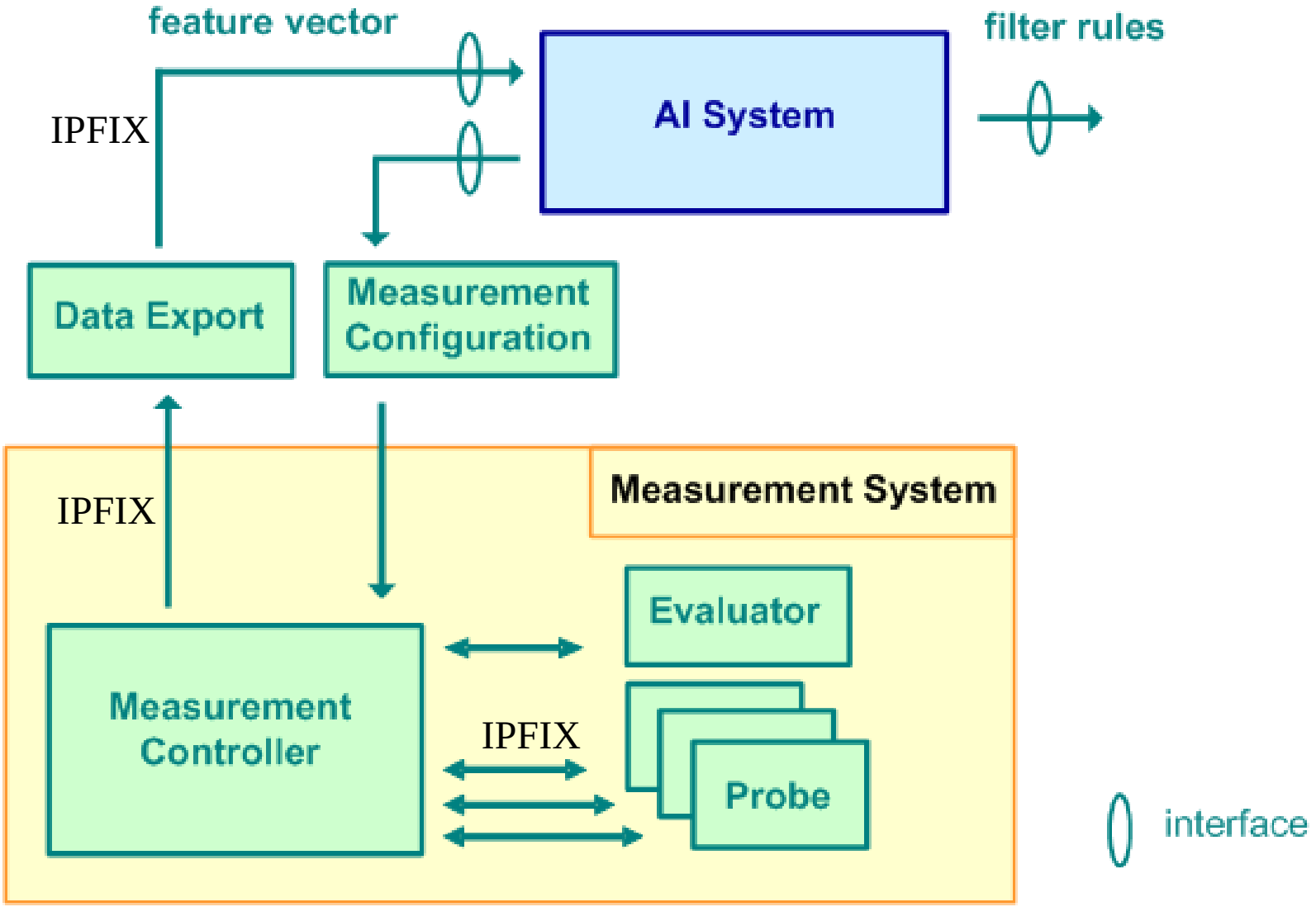
Fraunhofer Institute for Open Communication Systems

Mitigating DDoS at ISP level

- Mitigation can be effective when implemented on ISP and/or core routers
- This requires
  - high-speed traffic analysis
  - Information aggregation from various sources

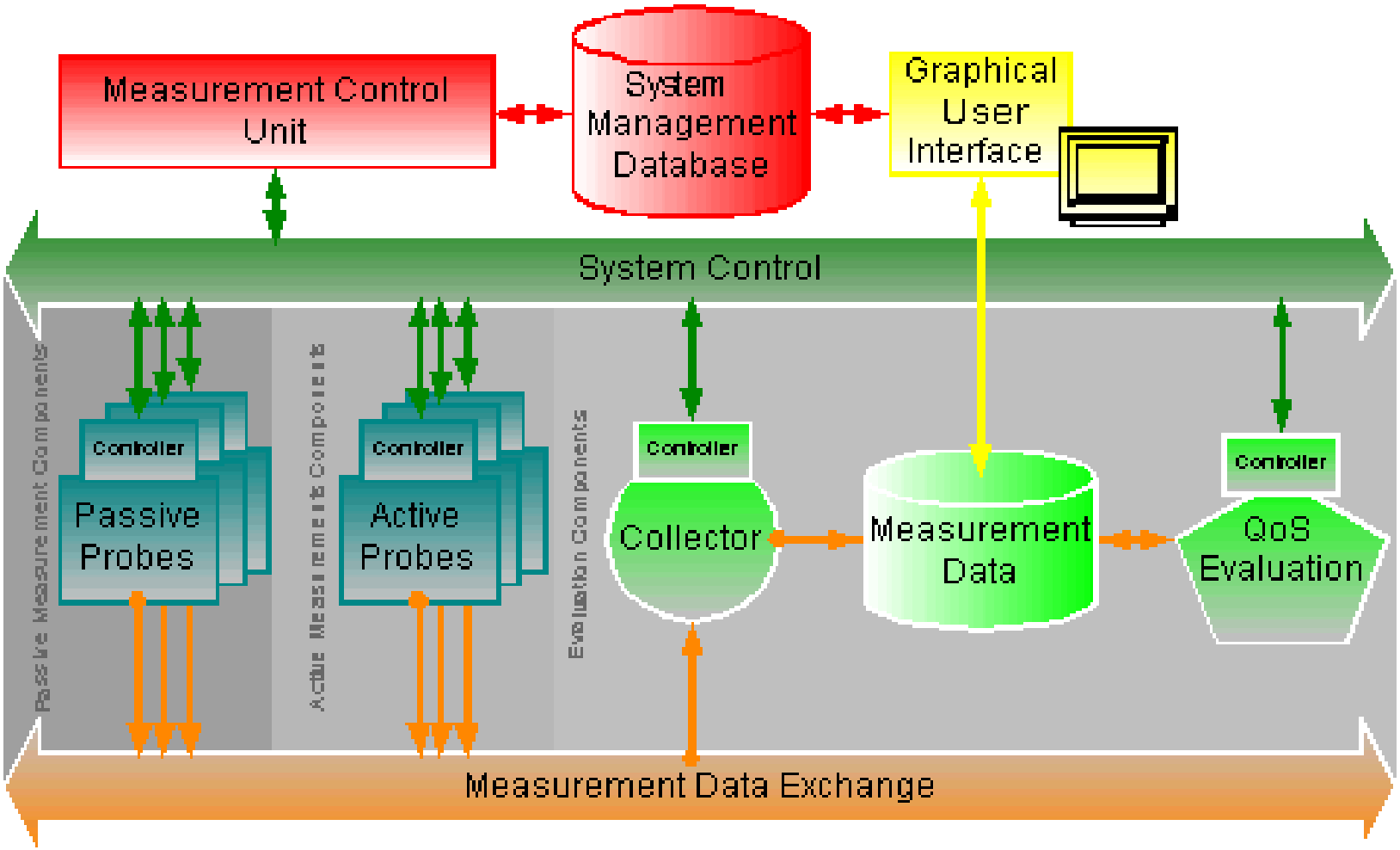


System Overview



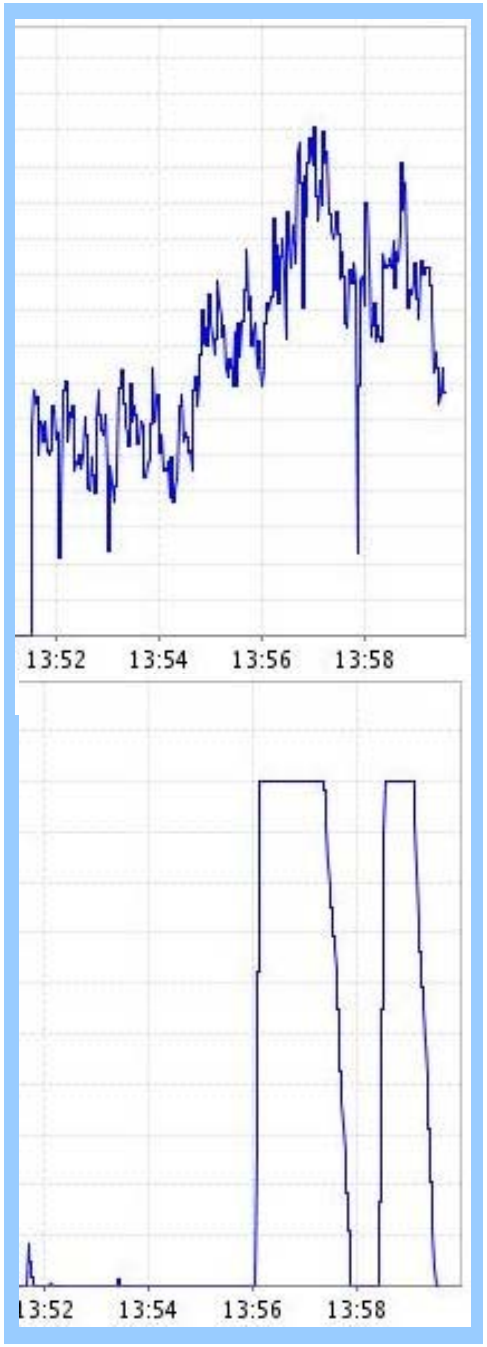
Fraunhofer Institute for Open Communication Systems

OpenIMP



DDoS Detection Metrics

- Some examples
  - Packet Count (above)
  - Byte Count
  - Packet count per flow / flag / message type
- Transformations
  - CUSUM (below)
  - Wavelet
  - Entropy

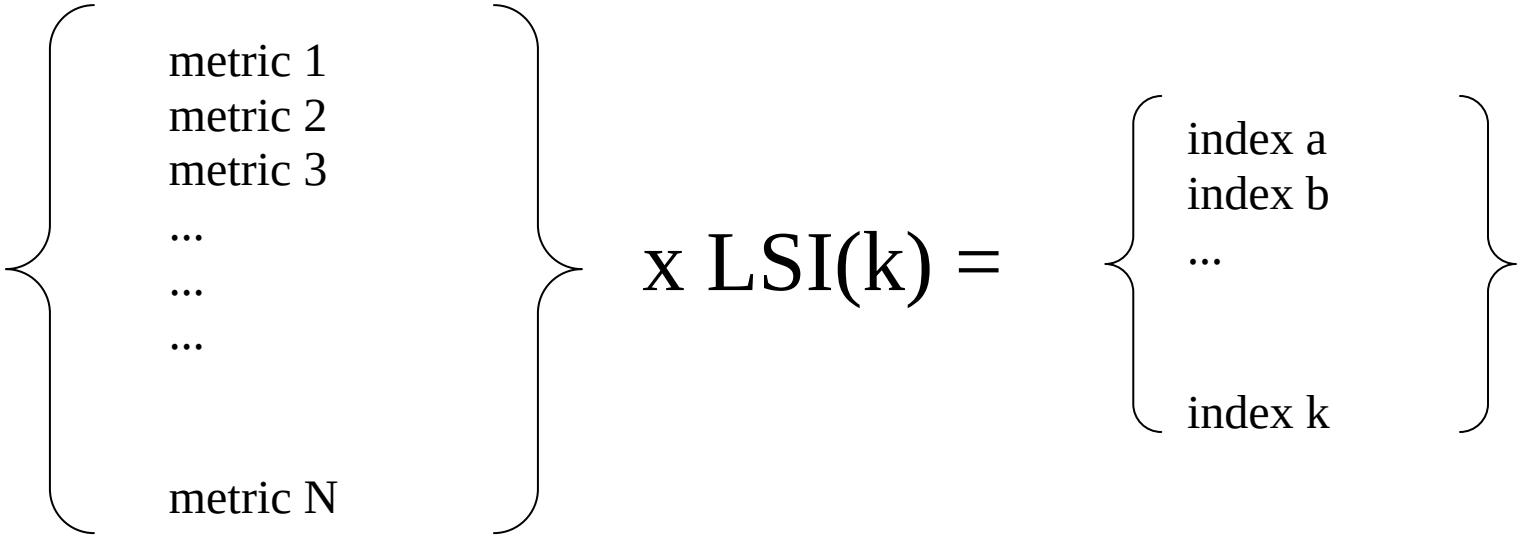


- A multitude of proposals in different papers!
- Which ones to implement?

Fraunhofer FOKUS Institute for Open Communication Systems

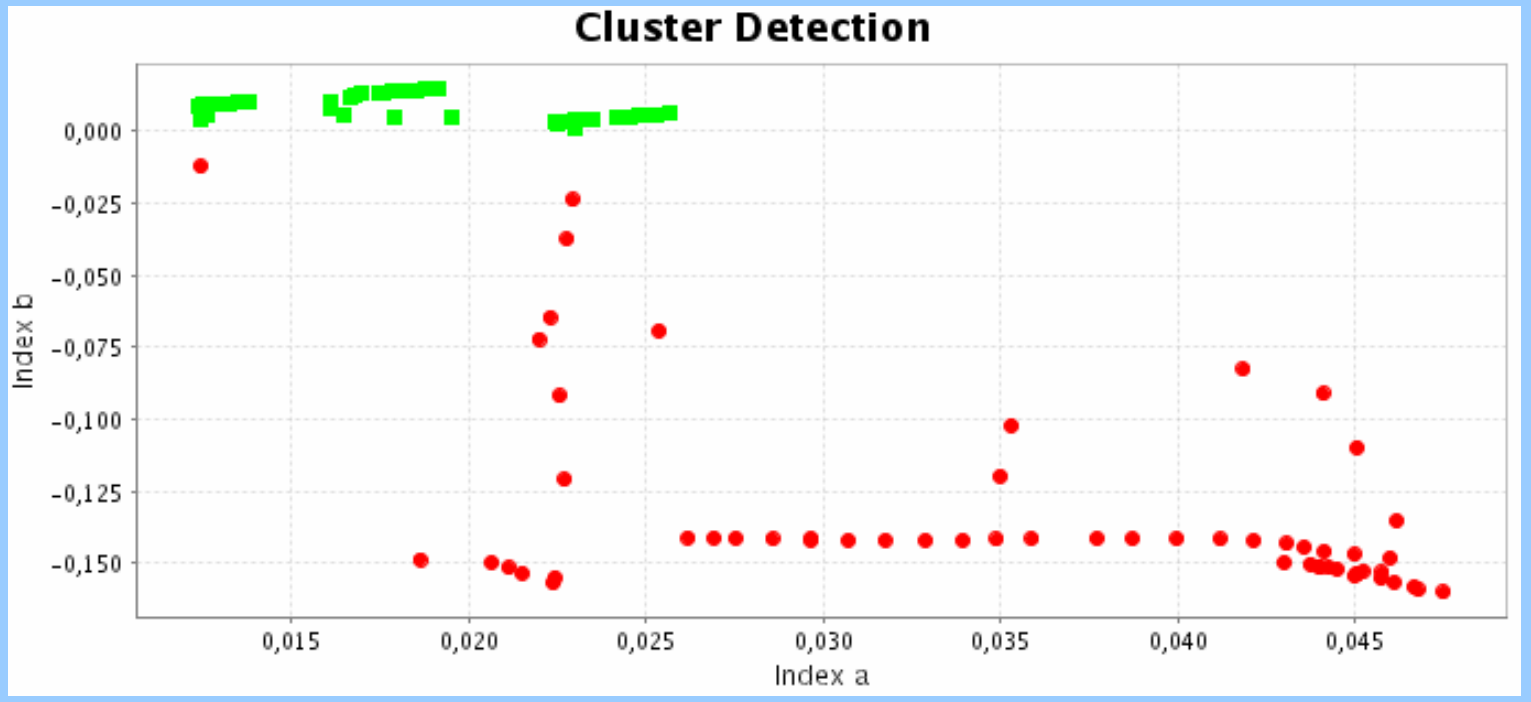
Latent Semantic Indexing

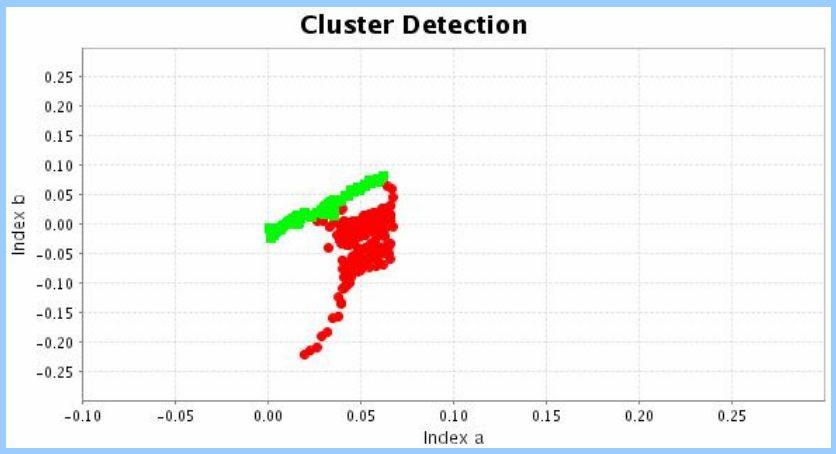
- allows to reduce a multi-dimensional feature vector
- into a lower-dimensional feature vector (easier to process)
- information preserving (principle components)
- maps all metrics into one uniformly sized *feature vector*



Fraunhofer Institute for Open Communication Systems

Cluster Detection





FOKUS

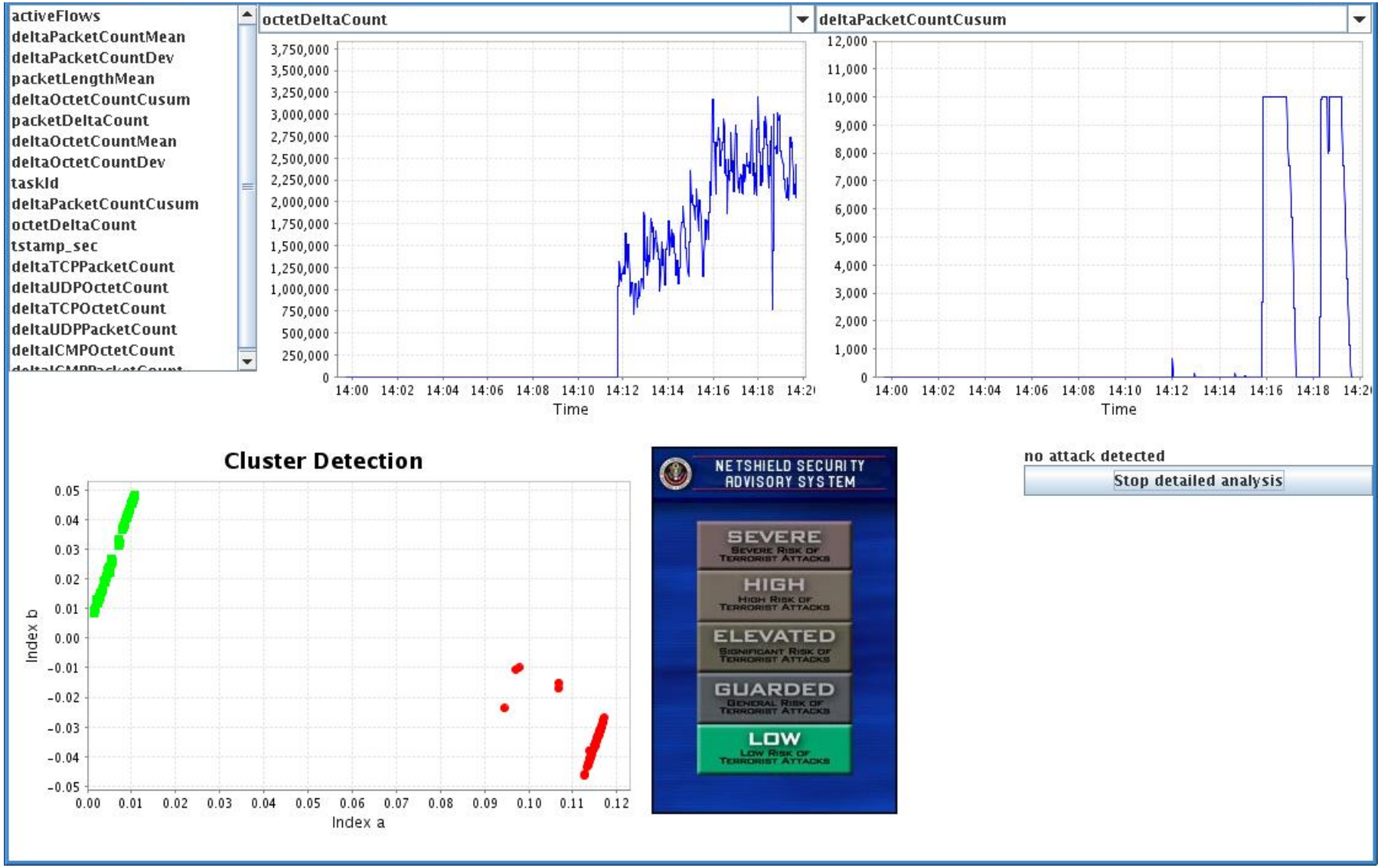
Fraunhofer Institute for Open Communication Systems

Cluster Detection

- Unknown Clusters are a possible threat
- Reactions include
  - Filtering, if bandwidth is scarce anyway
  - Detailed analysis of identified anomalies

Fraunhofer FOKUS Institute for Open Communication Systems

What it looks like...



FOKUS

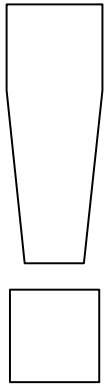
Fraunhofer Institute for Open Communication Systems

The advantage of using IPFIX

- Established standard for network metrics
- New probes/metrics can be added into the system
  - They immediately speak the language of the system
  - Standard components (routers) may provide the data
  - A training phase is needed for new information sources
- Latent Semantic Indexing reduces any number of metrics
- Cluster Detection operates on the same feature space size

- Detection seamlessly integrates new IPFIX information sources

Thank You!



Questions?