

A flexible DDoS detection System using IPFIX

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



Fraunhofer Institute for Open
Communication Systems



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).

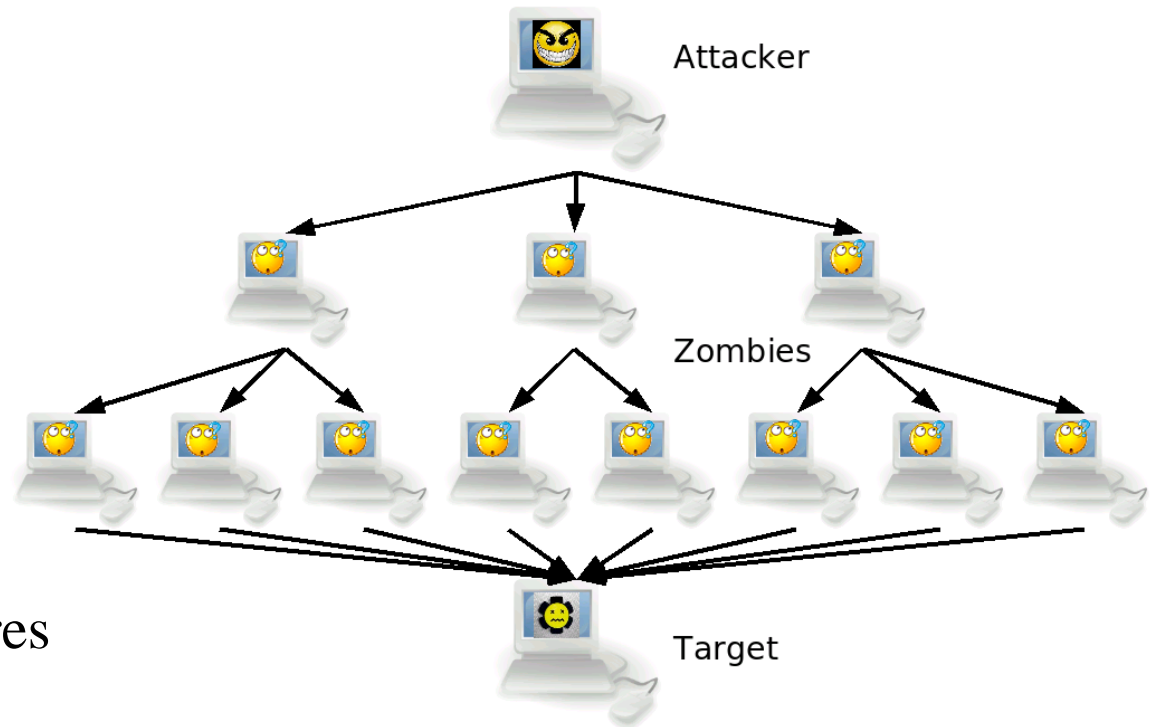
Outline

- 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



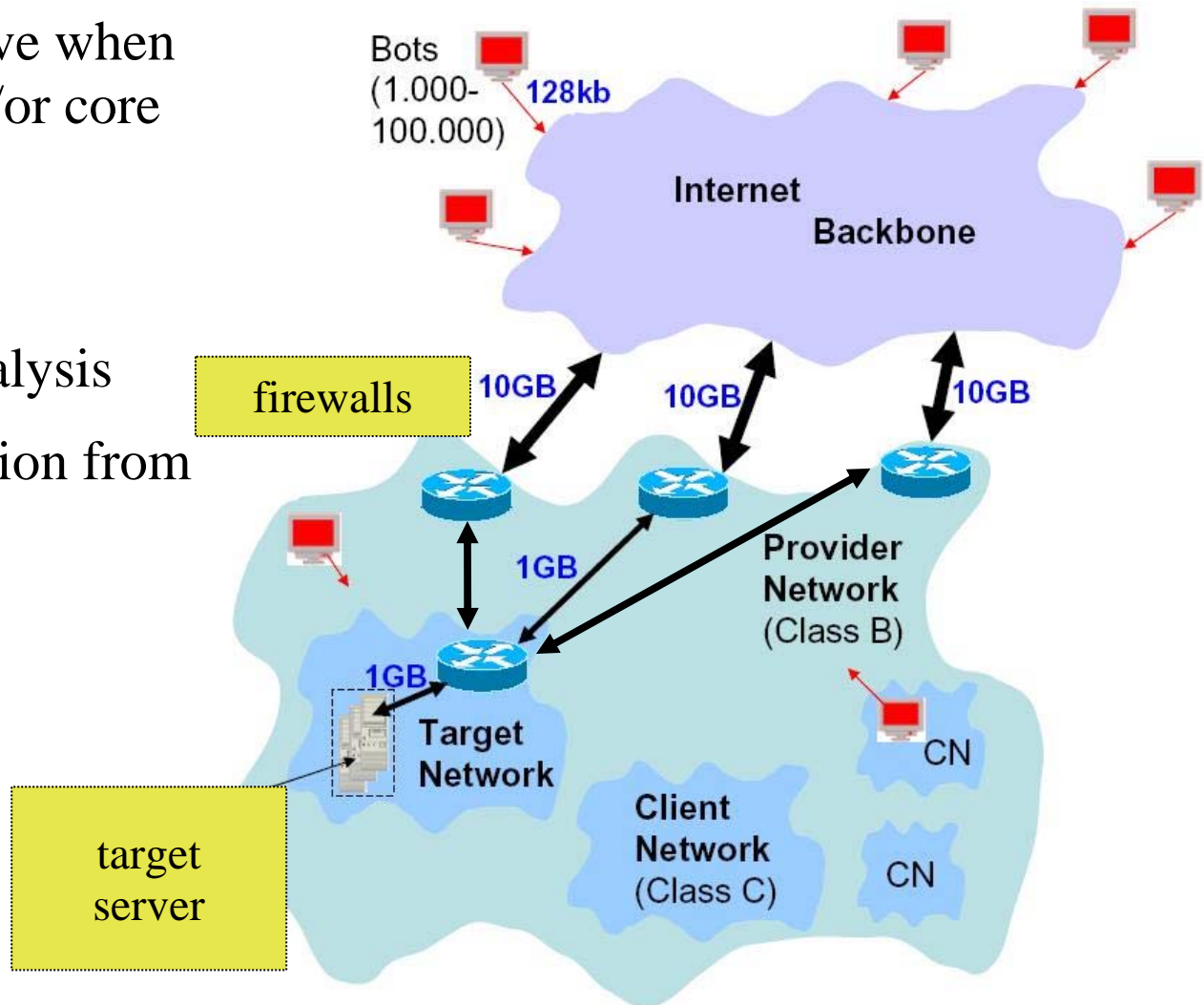
The DDoS Problem

- 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

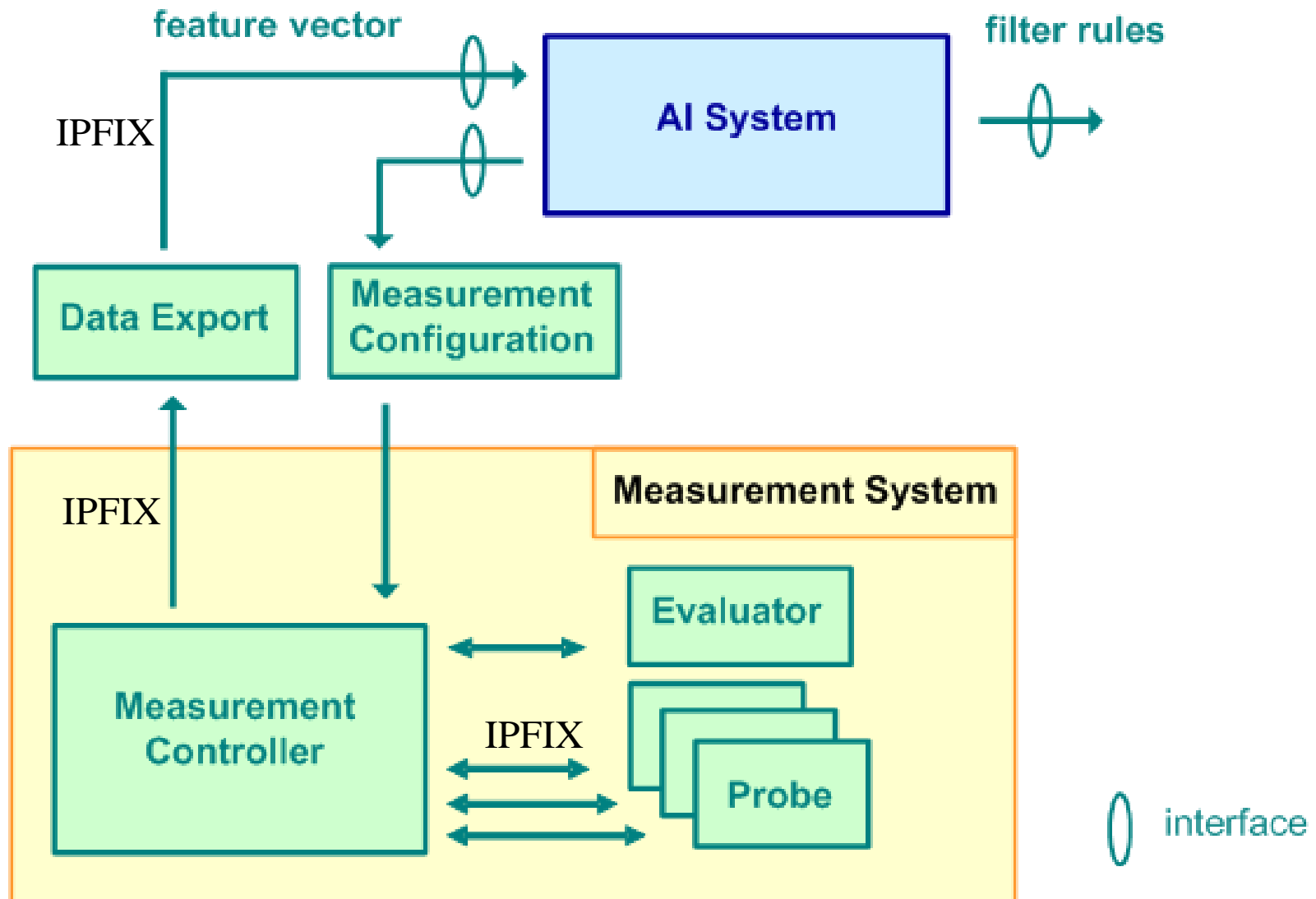


Mitigating DDoS at ISP level

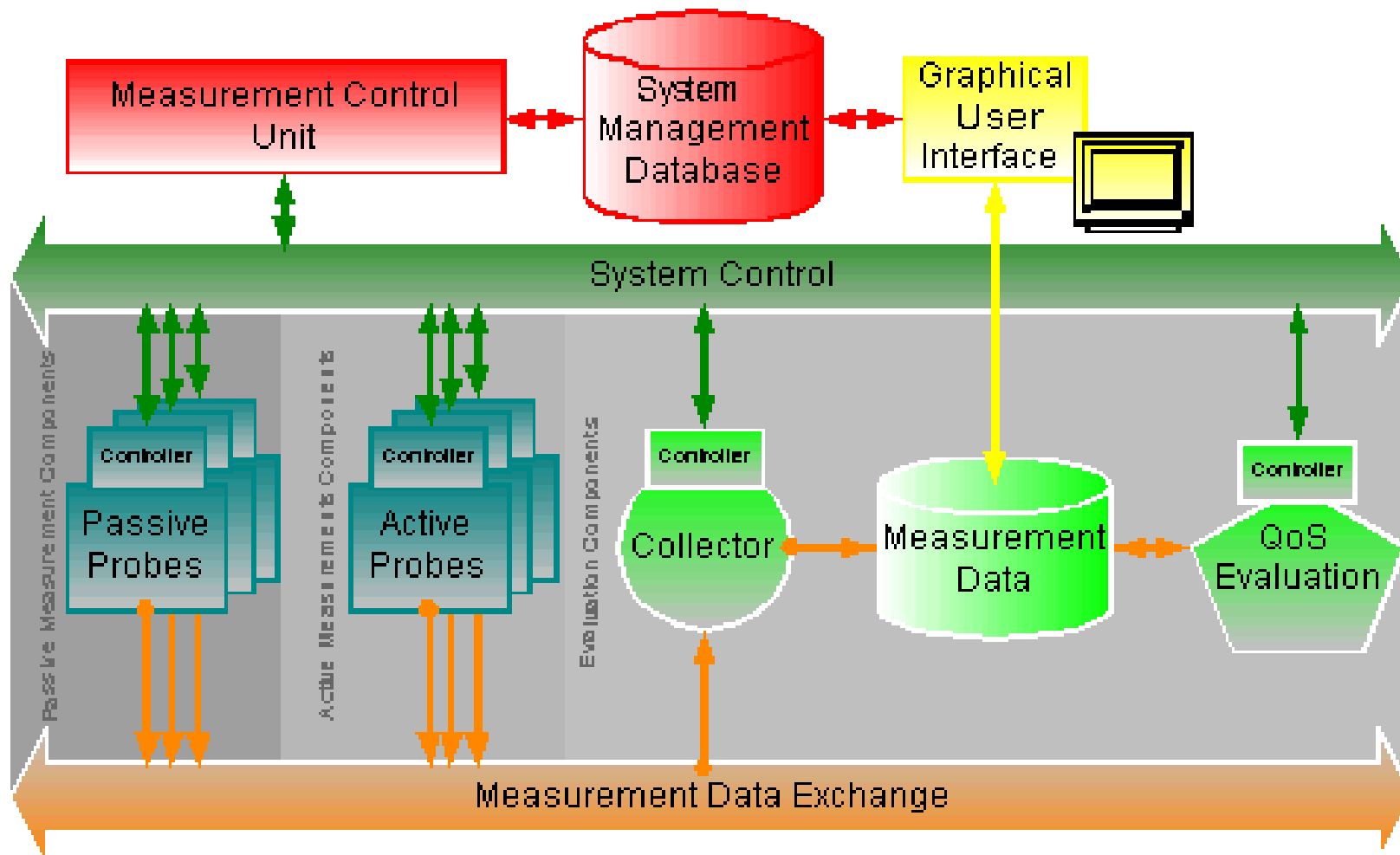
- Mitigation can be effective when implemented on ISP and/or core routers
- This requires
 - high-speed traffic analysis
 - Information aggregation from various sources



System Overview

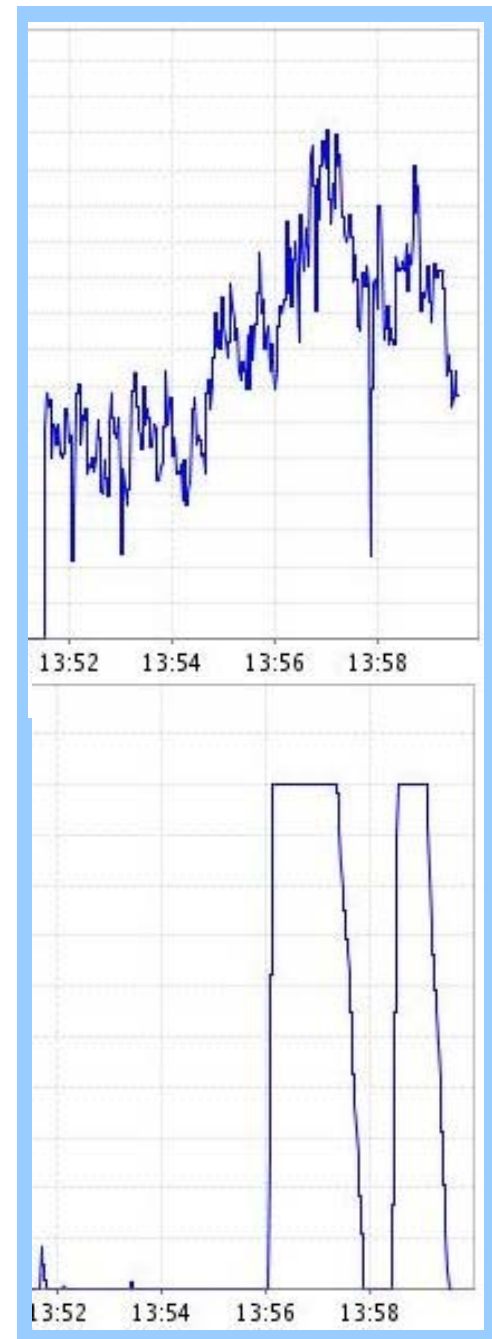


OpenIMP



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?



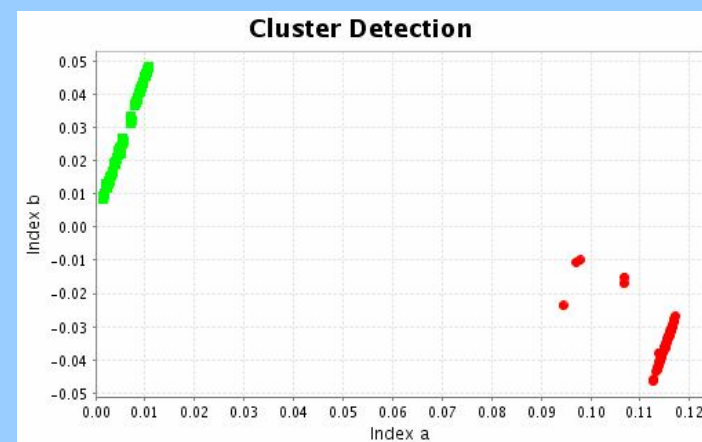
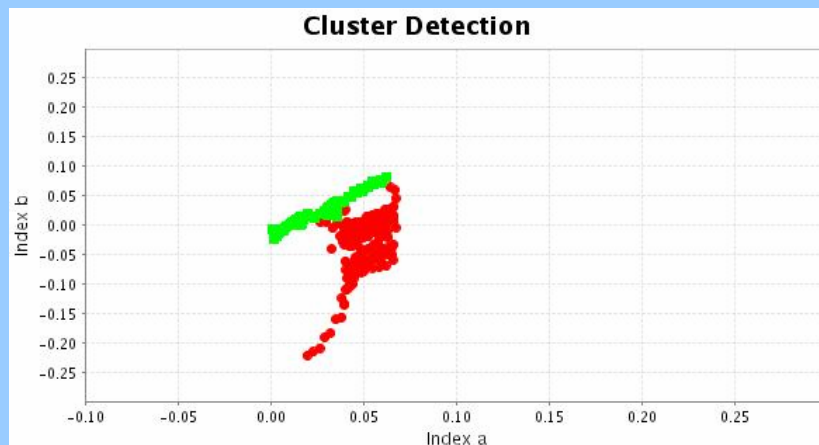
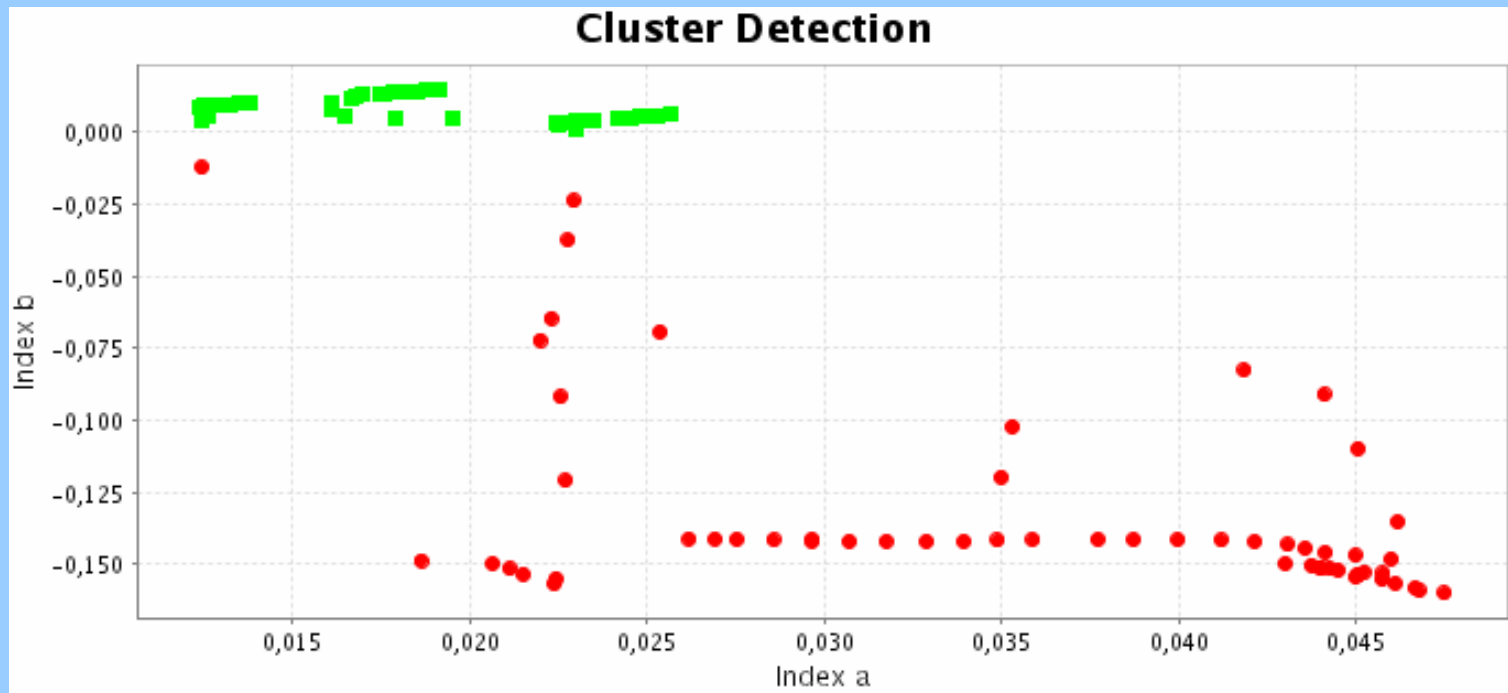
Latent Semantic Indexing

- 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*

$$\left\{ \begin{array}{l} \text{metric 1} \\ \text{metric 2} \\ \text{metric 3} \\ \dots \\ \dots \\ \dots \\ \text{metric N} \end{array} \right\} \times \text{LSI}(k) = \left\{ \begin{array}{l} \text{index a} \\ \text{index b} \\ \dots \\ \dots \\ \text{index k} \end{array} \right\}$$



Cluster Detection

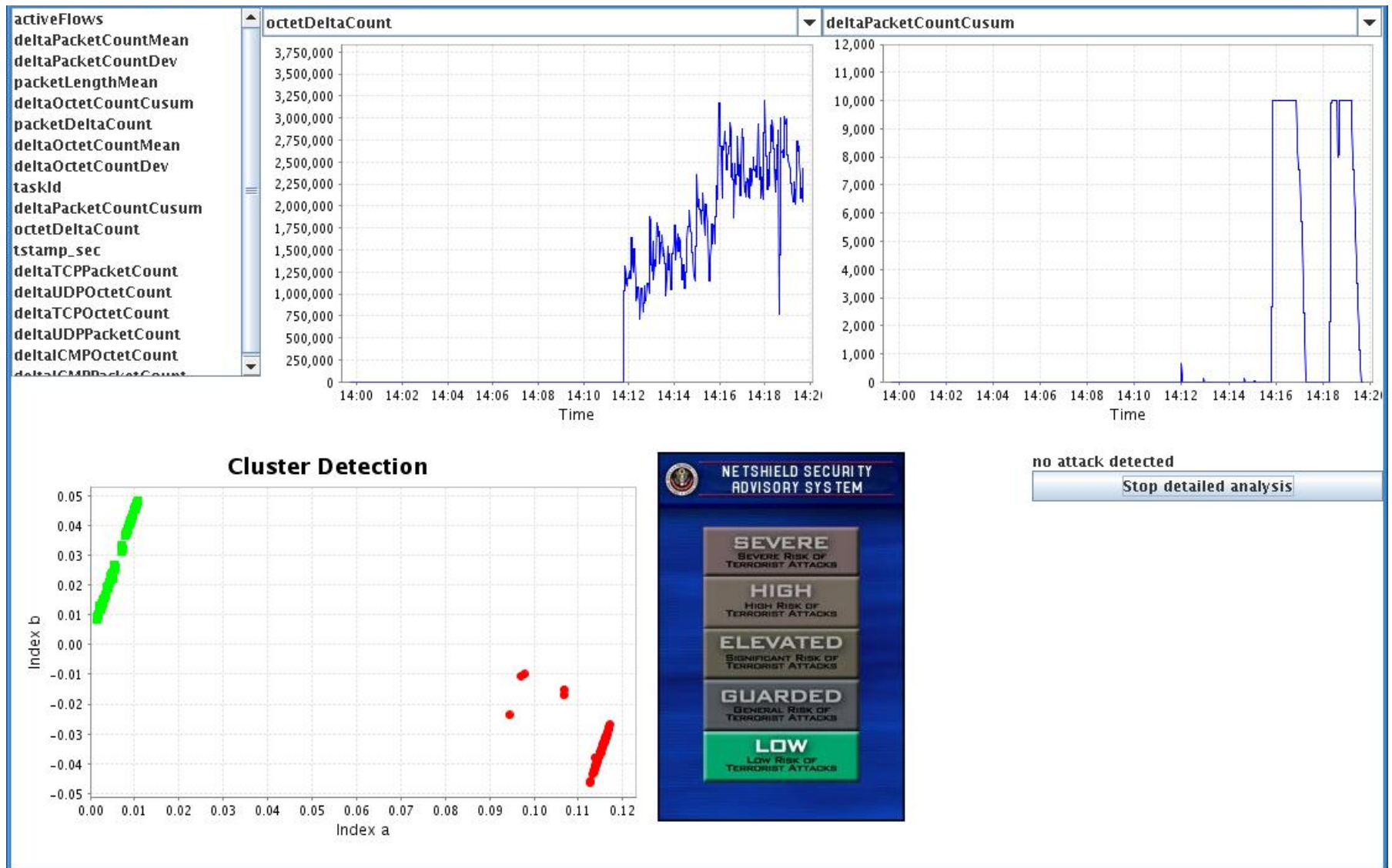


Cluster Detection

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



What it looks like...



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?

