Fachhochschule
Gelsenkirchen

Privacy compliant analysis and global early warning with the Internet Analysis System

Workshop on Future Internet Design
28. Sept. 2009, Brussels

Mathias Deml
Dominique Petersen
deml/petersen (at) internet-sicherheit.de

Institute for Internet-Security - if(is)
University of Applied Sciences Gelsenkirchen
https://www.internet-sicherheit.de

if(is)
internet security.

Agenda

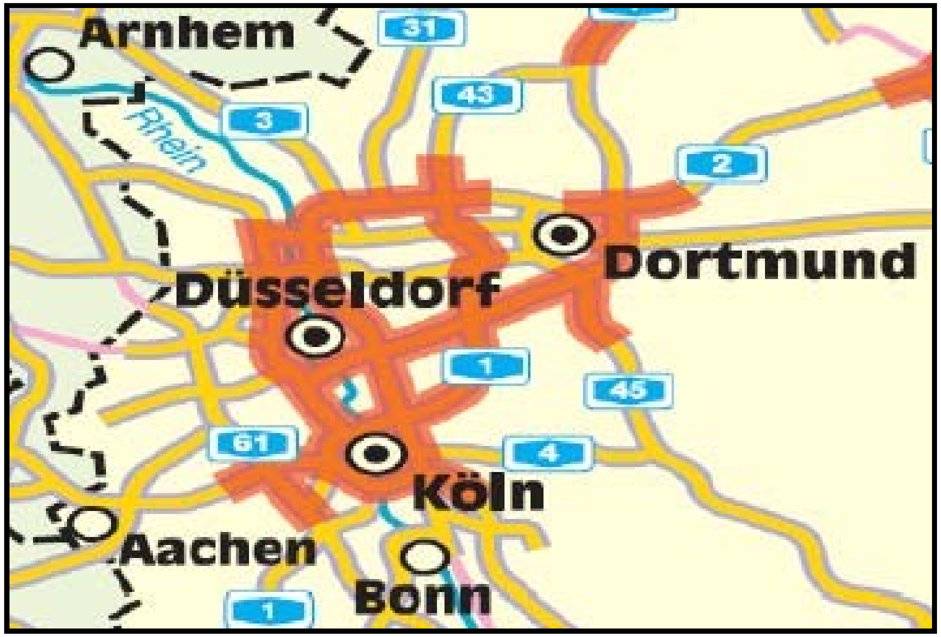
- Motivation
- Internet Analysis System
- IAS Sensor Technology
- Separation to other Systems
- Anomaly Detection with the IAS
- Anomaly Detection Examples
- Conclusions

Motivation
# Analogy (1/2)

Local View

Motivation
# Analogy (2/2)

Global view



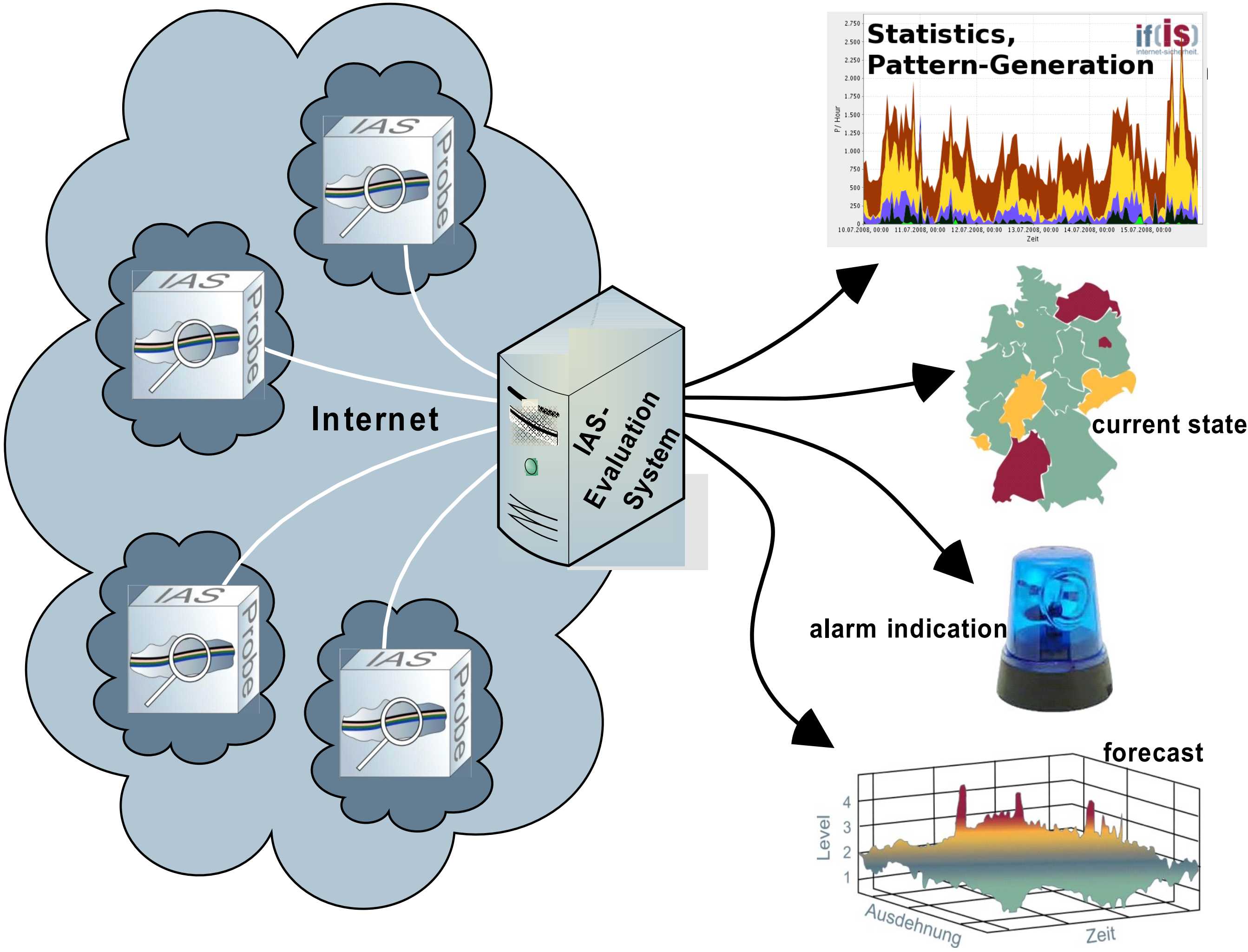
Air Traffic Control

Early Warning
# Internet Analysis System (1/2)

Privacy compliant by design

- **Sensor-technology which collects only necessary statistical data**
  - **No** user data
  - **No** ip adresses
  - **No** states or connection tracking
- **Open Access**
  - GNU General Public License
  - Well-documented with free access
- **Certified privacy (according to the German Data Protection Law)**
  - Common Criteria – Level 2

Early Warning
# Internet Analysis System (2/2)



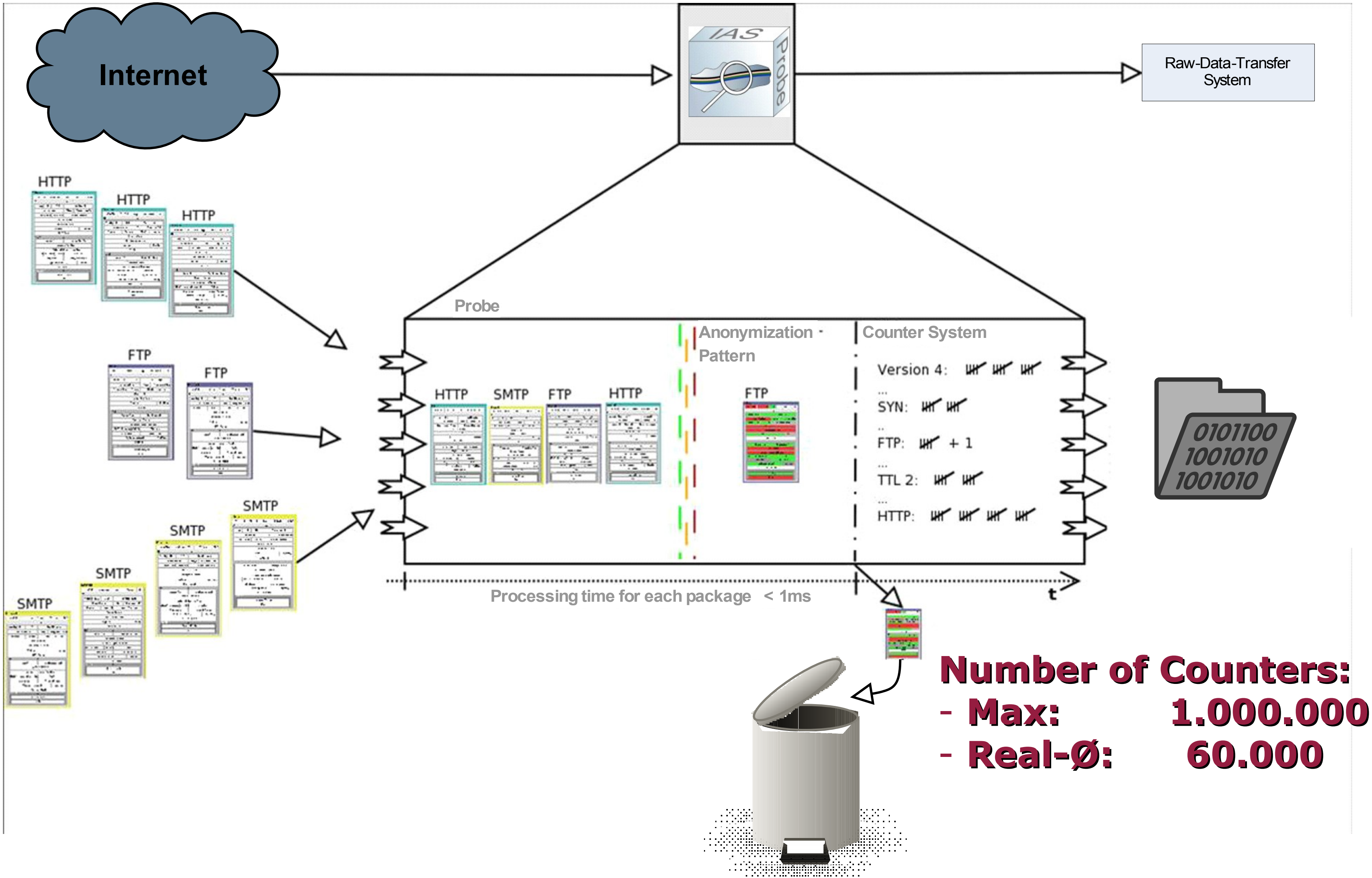
Description of profiles, patterns and coherences, creation of a knowledge base.

Outline of the current state of the internet.

Detection of attacks and of deflections.

Forecast of patterns and attacks.

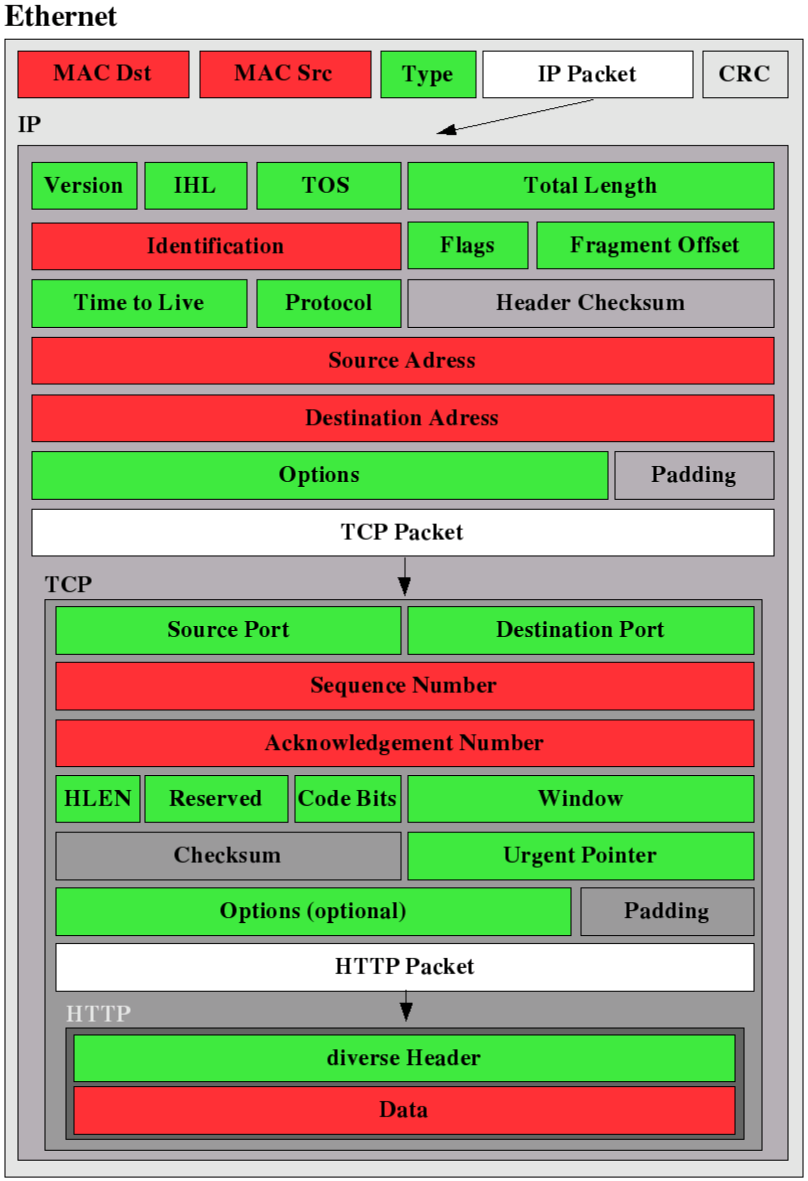
IAS Sensor Technology
# Counting of header information



Number of Counters:
- **Max: 1.000.000**
- **Real-Ø: 60.000**

IAS Sensor Technology
# Protocol stack (1/2)

- **Ethernet**
  - Type: Type of the nested packets, in this case: 0x0800 (IP)
  - Checksum (CRC) irrelevant
- **Internet Protocol**
  - e.g.: Total Length of the packet
  - Protocol: Type of the nested Packet, in this case: 6 (TCP)
  - Source- and destination address privacy critical



Ethernet

MAC Dst | MAC Src | Type | IP Packet | CRC

IP

Version | IHL | TOS | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Adress

Destination Adress

Options | Padding

TCP Packet

TCP

Source Port | Destination Port

Sequence Number

Acknowledgement Number

HLEN | Reserved | Code Bits | Window

Checksum | Urgent Pointer

Options (optional) | Padding

HTTP Packet

HTTP

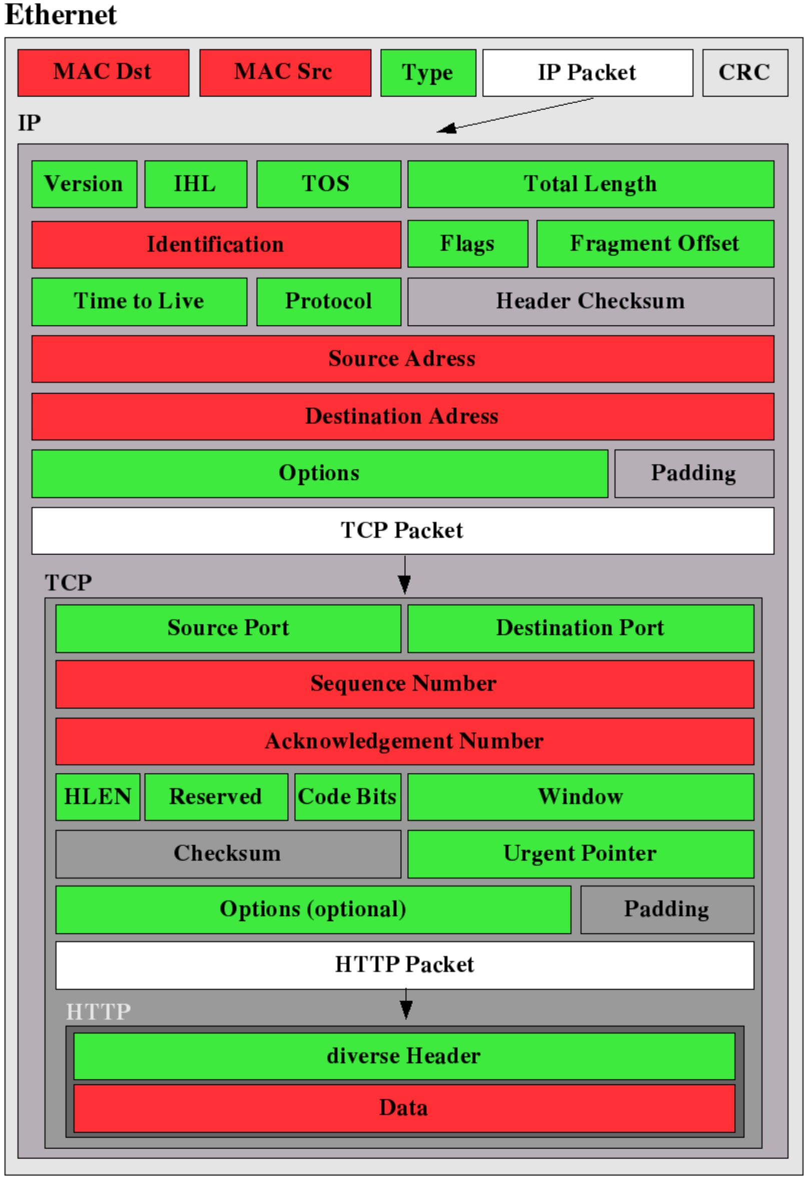
diverse Header

Data

IAS Sensor Technology
# Protocol stack (2/2)

- **Transmission Control Protocol**
  - Port: end point of the connection
    - HTTP: 80 (WWW)
    - Others e.g.:
      SMTP (25), HTTPS (443)
  - Code Bits
    - Information about the connection establishment and shut down

- **Hypertext Transfer Protocol**
  - Header:
    - e.g.: User Agent:
      describes the user’s browser
  - User data (DATA)
    e.g.: content of a web site



Ethernet

MAC Dst | MAC Src | Type | IP Packet | CRC

IP

Version | IHL | TOS | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Adress

Destination Adress

Options | Padding

TCP Packet

TCP

Source Port | Destination Port

Sequence Number

Acknowledgement Number

HLEN | Reserved | Code Bits | Window

Checksum | Urgent Pointer

Options (optional) | Padding

HTTP Packet

HTTP

diverse Header

Data

Internet Early Warning System
# Separation to other Systems

System / Characteristics	IDS	NWM-Tools	Firewall	HoneyPot	Sniffer	IAS
Function	Detection of signatures and attack patterns	Detection of Failures, configuration and performance Management, Accounting	Control of the communication by the means of rules and policies	Detection and Analyzing of the Intrusion and the used proceeding of hackers	Fault detection, spying on data and information	Actual status, pattern formation, creation of knowledge base, alarm signaling, forecasting
Location	Uplink	In the network	Uplink	Uplink	Uplink & Transit	Uplink & Transit
Realization	Complete analysis of the network traffic	Collection of Information by the means of agents	Complete analysis and control of the network traffic	Simulating the behavior of systems	Complete analysis of the network traffic	Complete analysis of the network traffic
Results	Recognition of signatures, Information for pattern formation	Accounting, fault messages, performance data	Security relevant information	Attack patterns and scenarios	Complete network traffic	Statistics, counters, results of further processing
Data privacy	Special agreement with concerned	Special agreement with concerned	Special agreement with concerned	Problem in specific scenarios	Very problematic	privacy compliant by design

IAS Sensor Technology
# Anomaly Detection

- In anomaly detection the normal behavior is described by a model
- Tries to detect attacks and threads by divergences from the meaured behavior to the behavior predicted by the model

$$|M - R| > \varepsilon$$

  - M := Model prediction of normal behavior
  - R := Actual measured behavior
  - ε := Threshold
- Many different methods for anomaly detection exists, e.g.
  - Time Series modelling
  - Feature Vector based approaches
  - …

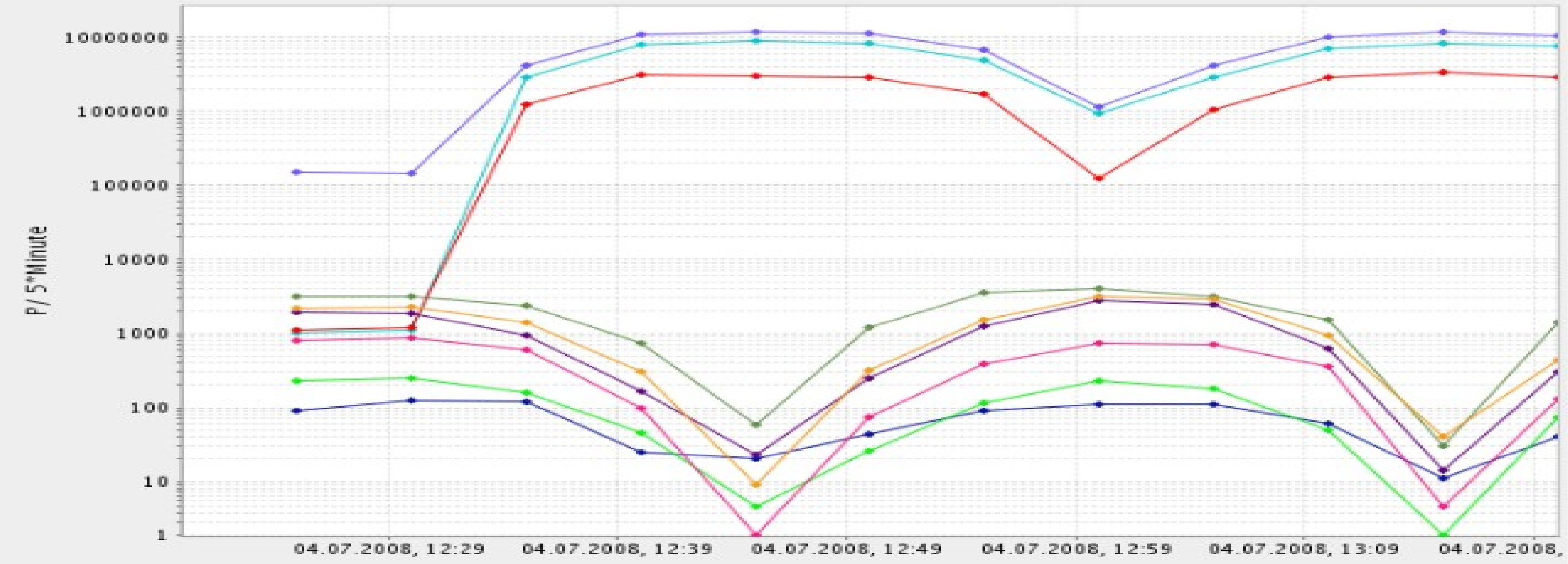
Basic idea: Combine different descriptors in feature vectors and estimate their probability density (<u>P</u>robabillistic <u>N</u>eural <u>N</u>etworks)

Anomaly Detection Example
# Distributed Denial of Service (1/2)

- Data collected during a real DDoS Attack
- Attack started with significant increase of the amount of TCP-SYN packets and ICMP-Echo-Requests
  - Ping flood combined with syn flood
- The used PNNs detected this and generate events
  - Warning was generated one interval before the system was not reachable any more
  - Reaction time of five minutes for countermeasures
- Another series of anomalies was detected when the system were not reachable any more
  - Null values on descriptors which are normally not null

Anomaly Detection Example
# Distributed Denial of Service (2/2)

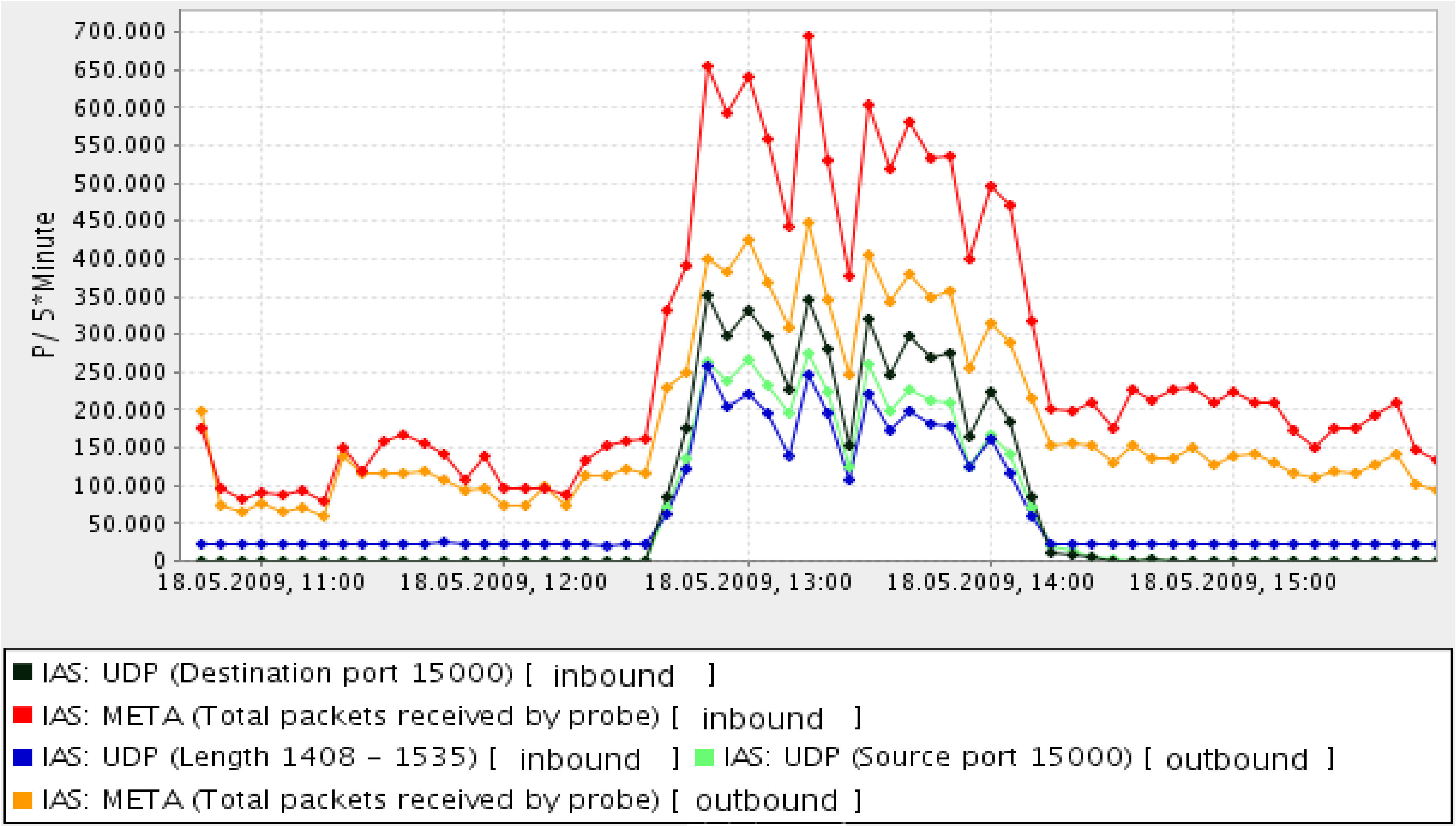
	12:35	12:40	12:45	12:50	12:55	13:00	13:05	Color
Total-Packets	●	●	●	●	●	●	●	🟪
TCP-SYN	●	●	●	●	●	●		🟥
TCP-FIN-ACK	●	●	●					🟧
TCP-SYN-ACK	●	●	●		●	●		🟪
TCP-RST	●	●	●					🟦
DNS	●	●	●	●			●	🟫
SMTP	●	●	●	●			●	🟪
HTTP-GET	●	●	●	●			●	🟩
ICMP	●	●	●	●	●	●	●	🟦



Anomaly Detection Example
# P2P Traffic (1/2)

- An anomaly was detected on Port 15000 with the IAS
- Increasing number of packets on this port
- With the help of other descriptors we approximated the transfered data to about 4.2 GB
  - Size of a DVD-5
- Further investigations showed that this port is used by a P2P file sharing client
  - Correlation with different sources of information: SNORT, Wikipedia
  - Thunder Network
  - Used in China
- Is in many cases combined with malware

Anomaly Detection Example
# P2P Traffic (2/2)



Internet Early Warning System
# Conclusions

- The sensor technology and method for anomaly detection is able to detect attacks and threads to networks privacy-compliant
- Detailed behavior description of network
- By two examples we have shown the potential of the approach
- Further research is necessary
  - Analyze the strength and weaknesses of the collected data and the detection algorithm for different kind attacks and threads
    - Long sample interval
    - Payload not analyzed
    - No flow based analysis
  - Combine events with information from other sources (showed in the second example)
    - Event Correlation

Fachhochschule
Gelsenkirchen

Privacy complient analysis and global early warning with the Internet Analysis System

Thank you for your attention!

Questions ?

Mathias Deml
Dominique Petersen
deml/petersen (at) internet-sicherheit.de

Institute for Internet-Security - if(is)
University of Applied Sciences Gelsenkirchen
https://www.internet-sicherheit.de

if(is)
internet security.