Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Internet Analysis System → Part 2

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet security.

Content

- Aim and outcomes of this lecture
- Idea of the Internet Analysis System
- Knowledge Base
- Outline of the Current State
- Detection of Attacks and Deflection
- Forecast of Patterns and Attacks
- Summary

Content

- Aim and outcomes of this lecture
- Idea of the Internet Analysis System
- Knowledge Base
- Outline of the Current State
- **Detection of Attacks and Deflection**
- Forecast of Patterns and Attacks
- Summary

Internet Analysis System (IAS)
→ Defined targets

Target 3

- **Detection of attacks and of deflections.**

With the knowledge of the current state and with the help of historical data, a warning will be issued if there are significant changes can be identified.
And this function helps us to reduce the damage in the Internet

Detection of Anomalies
→ Principle idea (1/3)

- **The detection of anomalies** can be used to observe behavior deflecting from the normal state

- In contrary to **misuse detection**, using **patterns** to find behavior that is not permitted
  - Which does not allow the detection of threats that are so far **unknown**

- **Problem**: What can be defined as “normal”?
  - Description of the “normal state” is difficult
  - Requires adequate representation

- **Important:** the **detection of anomalies** does not generate alerts concerning attacks, but informs of **abnormal behavior**
  - After a successful alert further **analysis** is necessary

- The detection of anomalies allows so far **unknown** threats to be identified

- By doing this, the risk of false alarm also rises (we need real experts!)

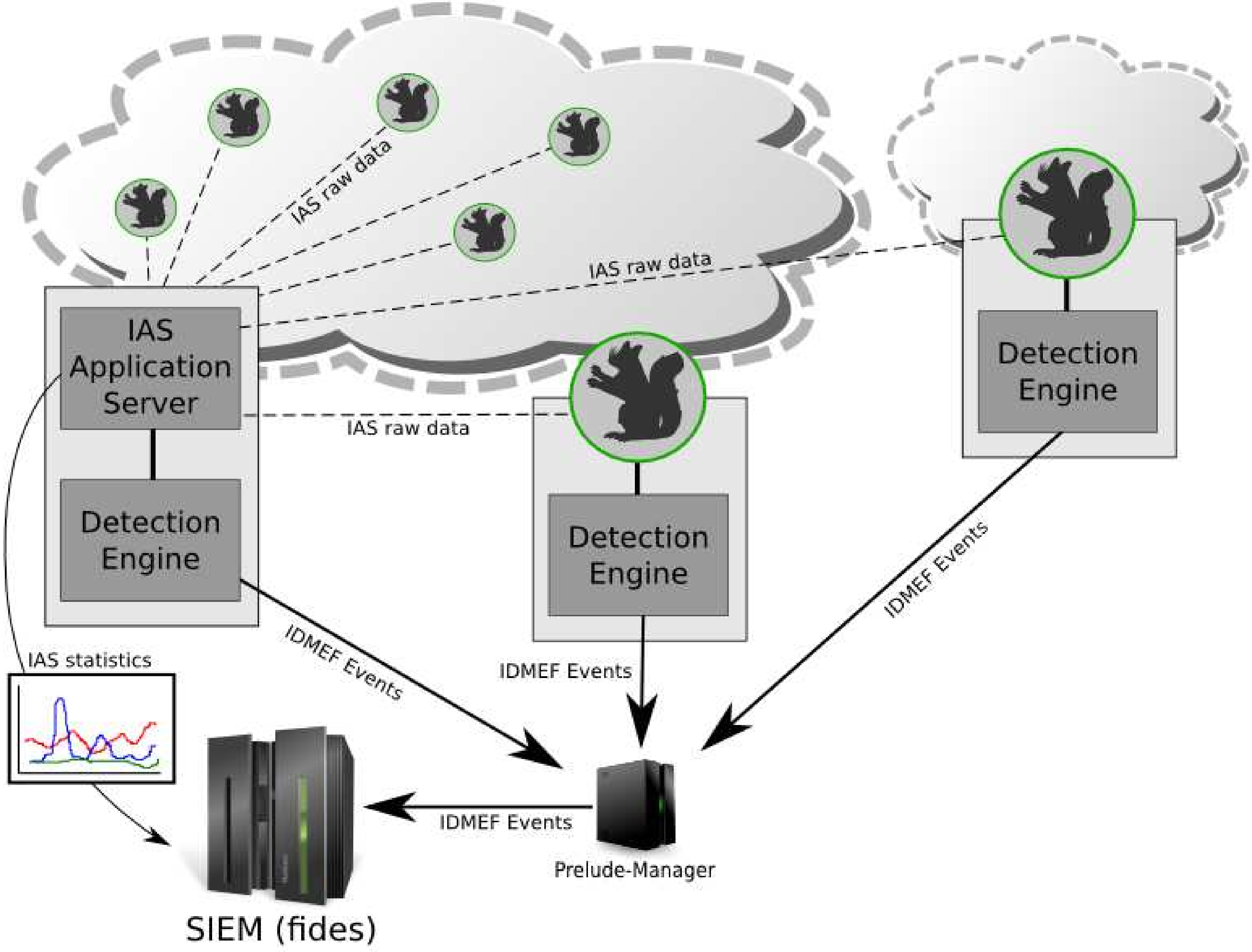
Detection of Anomalies
→ Principle idea (2/3)

- Basis of the method to detect anomalies is the **development** of a **model which describes the normal state!**
- **Problem**
  - What can be defined as “normal”?
    - Are regular port scans normal or should they be reported as an anomaly?
    - Isn’t an anomaly more likely to be a successful exploit after performing a port scan?
    - **Precise definition** of the normal state is required
  - Description of the **“normal state”** is difficult
    - Useful data needs to be collected, which help to describe the current state
    - Adequate **representation** of the data is necessary

Detection of Anomalies
→ Principle idea (3/3)

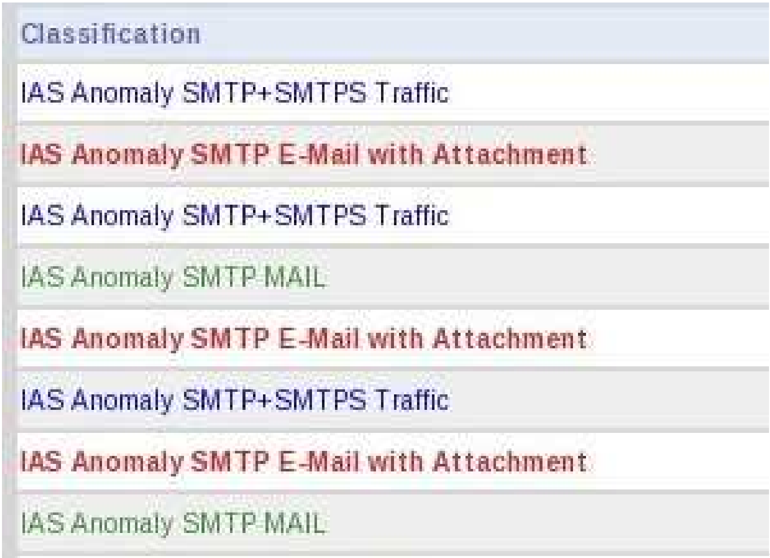
- **Problem**
  - The normal state changes over time
    - These changes need to be considered
    - In principle comparable to the misuse detection, where new patterns reflecting attacks need to be considered
    - The process of the detection of anomalies needs update itself continuously
  - The normal state is different at every location
    - Methods need to learn a different normal state at each location they are used

IAS: Detection Mechanism
→ Detection Engine

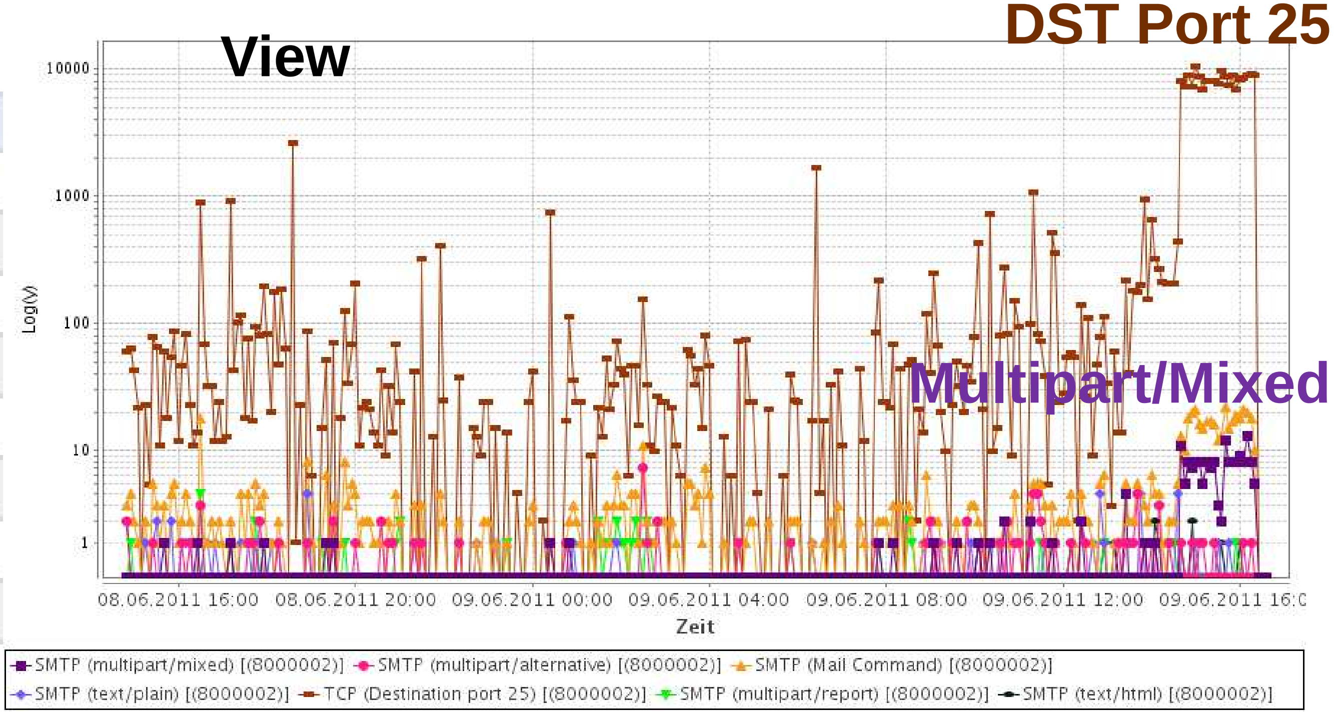


IAS: Detection Mechanism
→ Outgoing E-Mails

Events



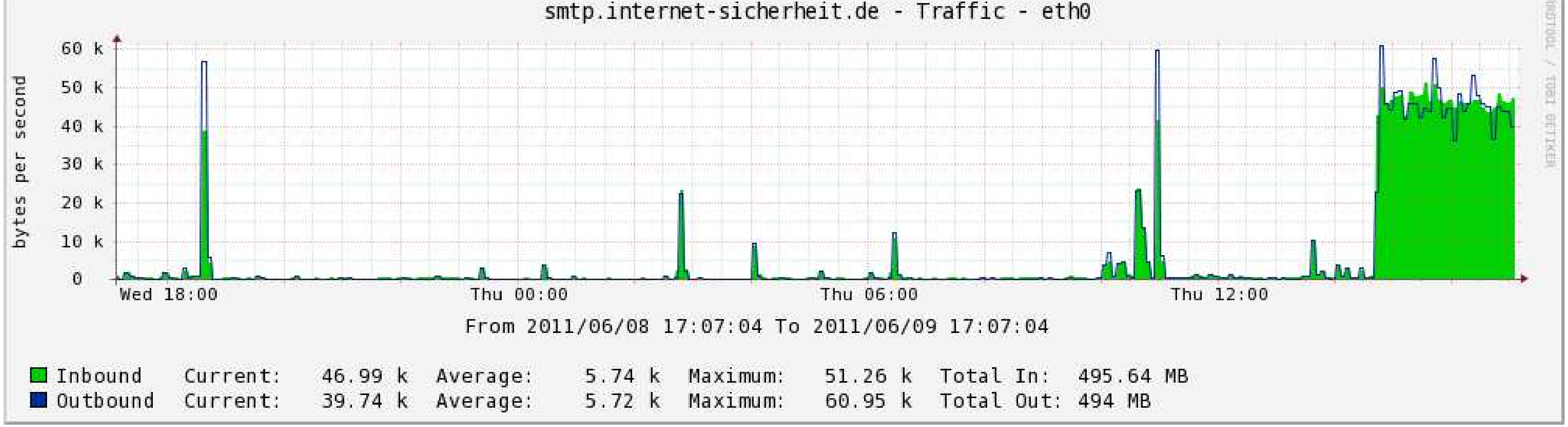
Classification
IAS Anomaly SMTP+SMTPS Traffic
IAS Anomaly SMTP E-Mail with Attachment
IAS Anomaly SMTP+SMTPS Traffic
IAS Anomaly SMTP MAIL
IAS Anomaly SMTP E-Mail with Attachment
IAS Anomaly SMTP+SMTPS Traffic
IAS Anomaly SMTP E-Mail with Attachment
IAS Anomaly SMTP MAIL



DST Port 25

Multipart/Mixed

Mail Server

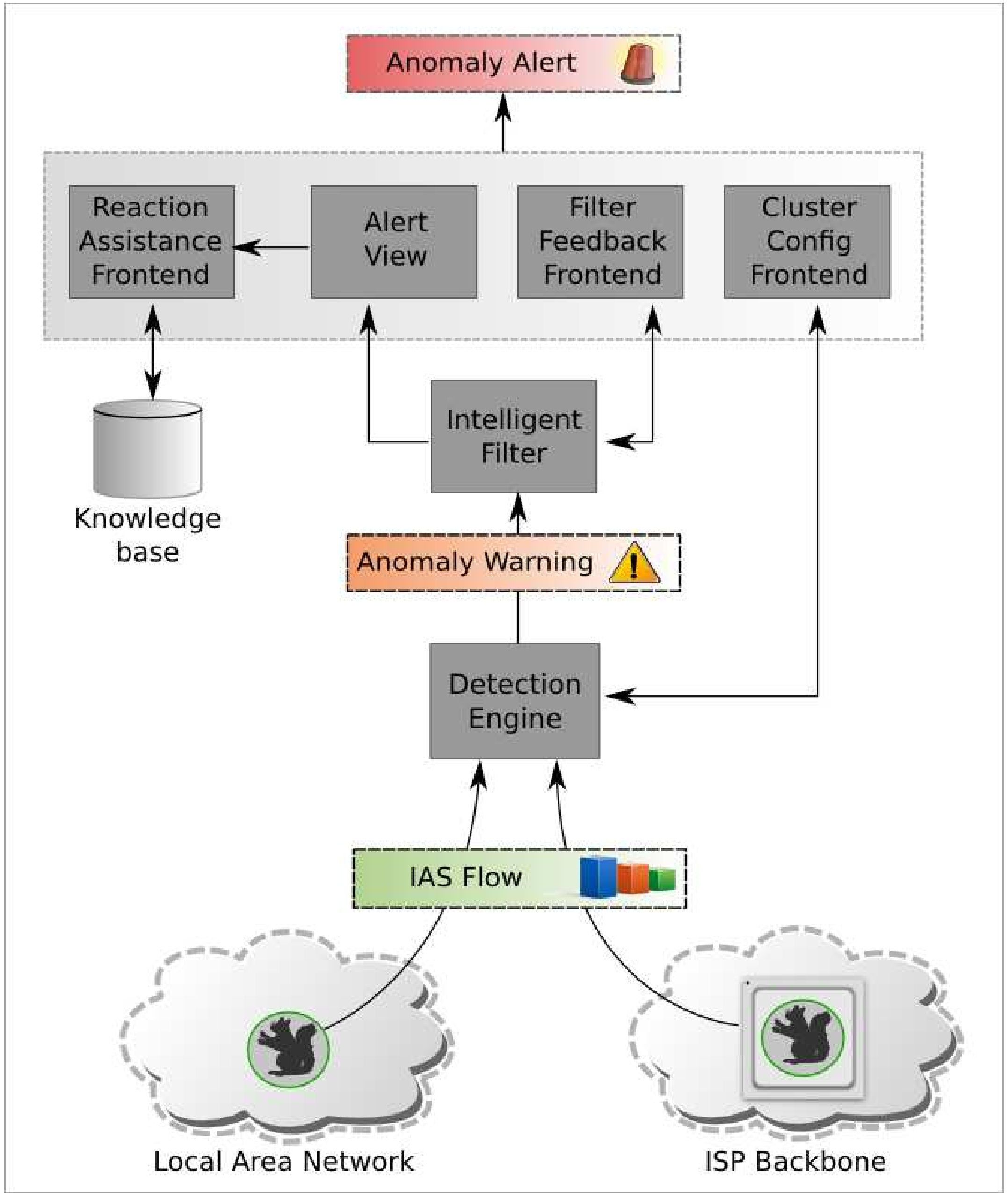


From 2011/06/08 17:07:04 To 2011/06/09 17:07:04

```
🟩 Inbound    Current:    46.99 k   Average:    5.74 k   Maximum:    51.26 k   Total In:   495.64 MB
🟦 Outbound   Current:    39.74 k   Average:    5.72 k   Maximum:    60.95 k   Total Out:  494 MB
```

IAS-Flow Anomaly Detection (1/3)

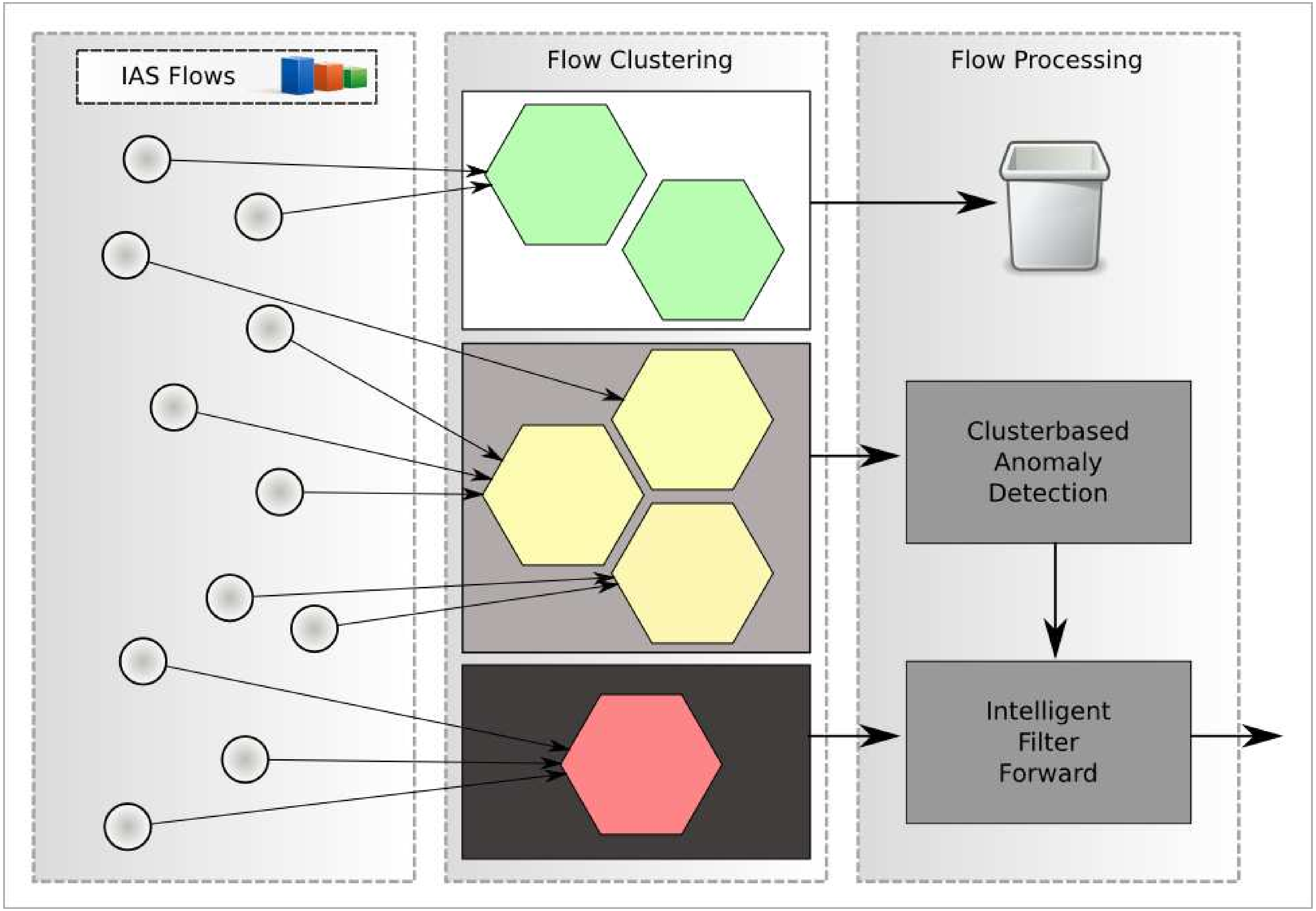
- Discover abnormal communication and assist by identifying abnormal communication as malicious or „undesirably“
- More technical: Detection of abnormal network flows (TCP/UDP) with root cause analysis (what caused the anomaly and is it dangerous?)
- Usage of hardware acceleration to realize analysis of high amount of flows (GPU/FPGA)



IAS-Flow Anomaly Detection (2/3)

- First we want to cluster/group flows by different attributes (like application layer protocol)
- Possibility to create policies that define which clusters of flows are malicious or normal in general
- Remaining clusters are analyzed with anomaly detection for each cluster seperately (which flows are statistical abnormal for a given cluster?)
- Abnormal flows or flows defined as malicious by policy are passed to an intelligent filter
  - This filter learns by user feedback which warnings should be escalated to alerts and which can be ignored
  - User is supported by frontend with all available data to find the root cause of the anomaly
- Alerts can be mapped to reaction hints for assistance

IAS-Flow Anomaly Detection (3/3)

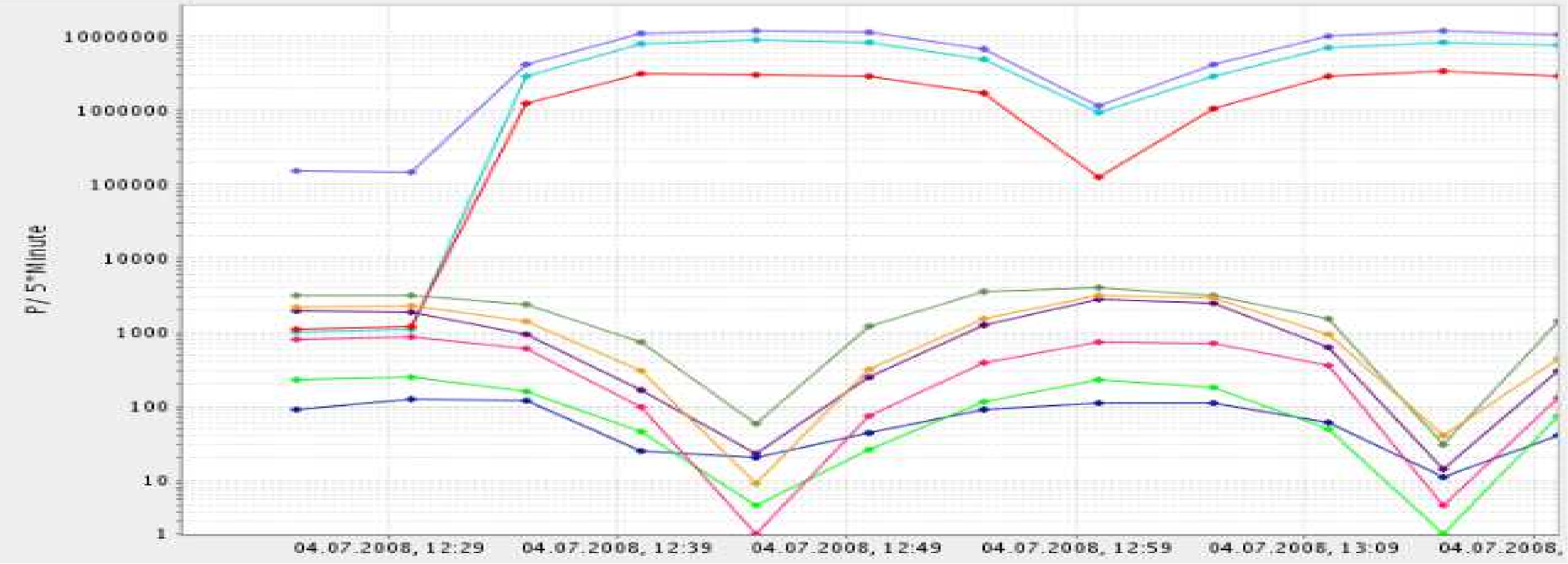


Summary

- We cannot forecast all possible attack vectors that are used for intrusion (exploits/vulnerabilities)
- => Focus on detection of compromised hosts or networks
- Try to detect with different methods as early as possible and isolate/clean before information can be stolen or system can be abused for botnet attacks / Spam

Results
→ DDoS

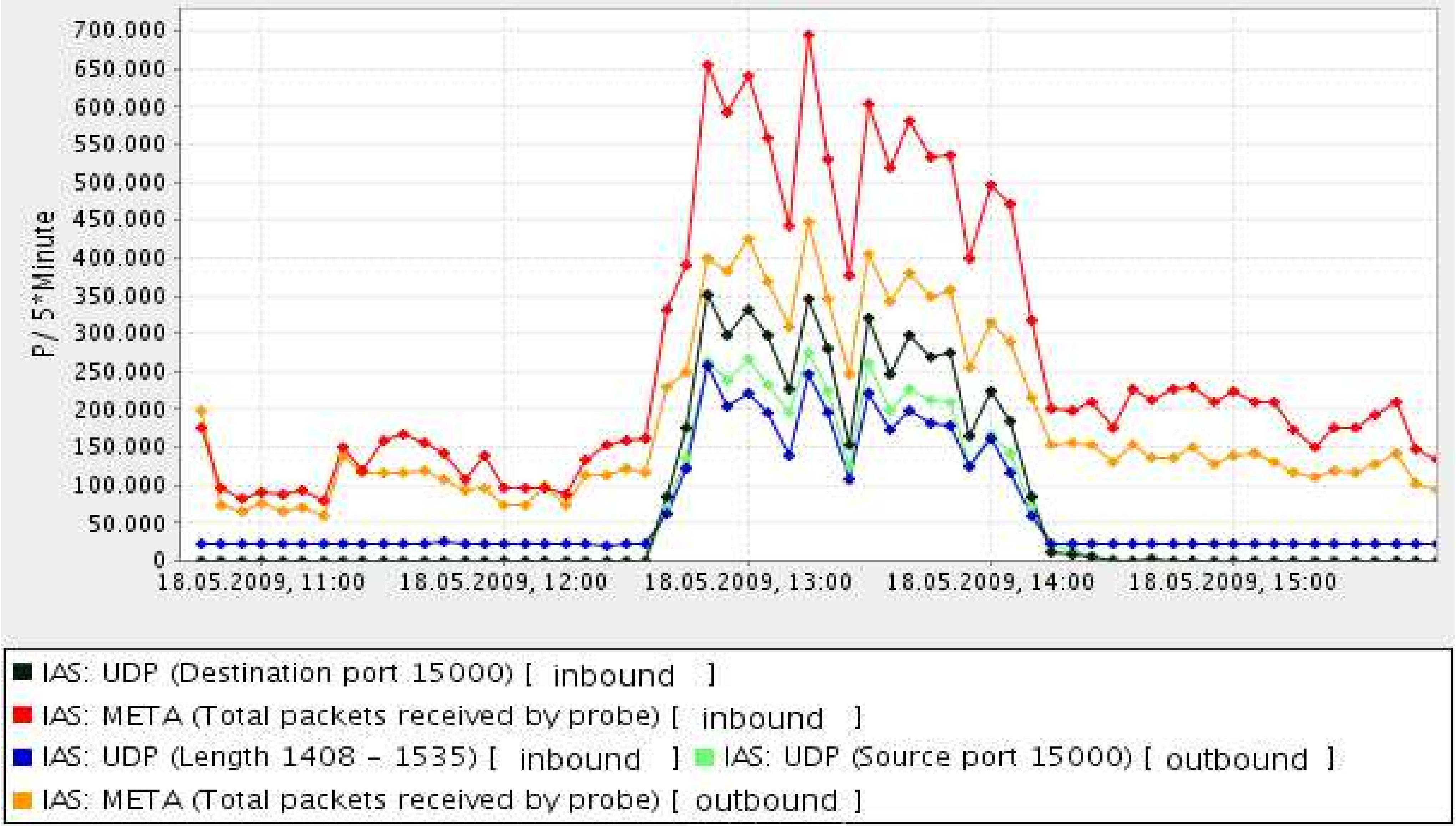
	12:35	12:40	12:45	12:50	12:55	13:00	13:05	Color
Total-Packets	●	●	●	●	●	●	●	🟪
TCP-SYN	●	●	●	●	●	●		🟥
TCP-FIN-ACK	●	●	●					🟧
TCP-SYN-ACK	●	●	●		●	●		🟪
TCP-RST	●	●	●					🟦
DNS	●	●	●	●			●	🟫
SMTP	●	●	●	●			●	🟪
HTTP-GET	●	●	●	●			●	🟩
ICMP	●	●	●	●	●	●	●	🟦



Results
→ P2P-Traffic

- An anomaly was detected on Port 15.000
- Increasing number of packets on this port
- With the help of other descriptors we approximate 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

Results
→ P2P-Traffic



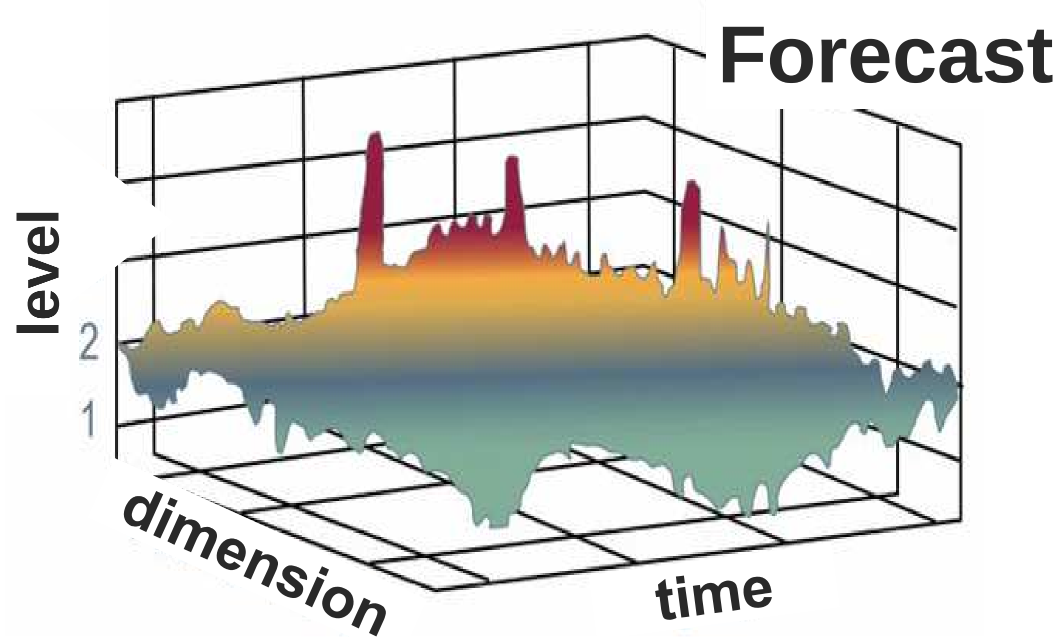
Content

- Aim and outcomes of this lecture
- Idea of the Internet Analysis System
- Knowledge Base
- Outline of the Current State
- Detection of Attacks and Deflection
- **Forecast of Patterns and Attacks**
- Summary

Internet Analysis System (IAS)
→ Defined targets

Target 4

- **Forecast of patterns and attacks.**



By investing and analyzing the extrapolated profiles, technological trends, correlations and patterns it is possible to make forecasts about the changes in the state of the internet by an evolution process of the findings.
In this way attacks and important changes can already be identified early and this helps us to avoid damage in the internet.

Internet Analysis System (IAS)
→ Forecast of patterns and attacks

- Two aspects are of relevance to secure the operability of the Internet:
  - The network has to be prepared for emerging technology
  - Attacks have to be detected in time and the distribution has to be prevented efficiently

What is important?

=> 1. Technology trends have to be detected early enough!

2. The initial phase of attacks needs to be better understood and described!

3. The distribution of attacks needs to be understood!

4. Security mechanisms need to enhance secure cryptographic methods

=> Ability to forecast and to identify patterns

Forecast for the Internet Analysis System → Targets

- Assistance to generate forecasts, project measured values to the future

- **Short time forecasts**
  - Minutes up to days
  - Forecast and detection of deflections from the normal behavior, which can be used for “Early Detection” of attacks and anomalies

- **Long term forecasts**
  - Weeks up to months
  - Forecast and detection of technology trends

Characteristics of the measured values

- **The IAS collects measured values in the interval of (at the moment) 5 minutes**

- **Identical monitoring at the same location (IAS sensor)**

- **Parameters are discrete**
  - **=> analysis of “time series”**
    - **Moving average**
      (arithmetic mean)
    - **Exponential smoothing**
      (arithmetic mean including the loading with past values)
    - **Linear regression**
      (Trend +/- seasonal examination)
    - **Holts-Winters-Method**
      (Trend +/- seasonal examination including loading)

Component model of the time series

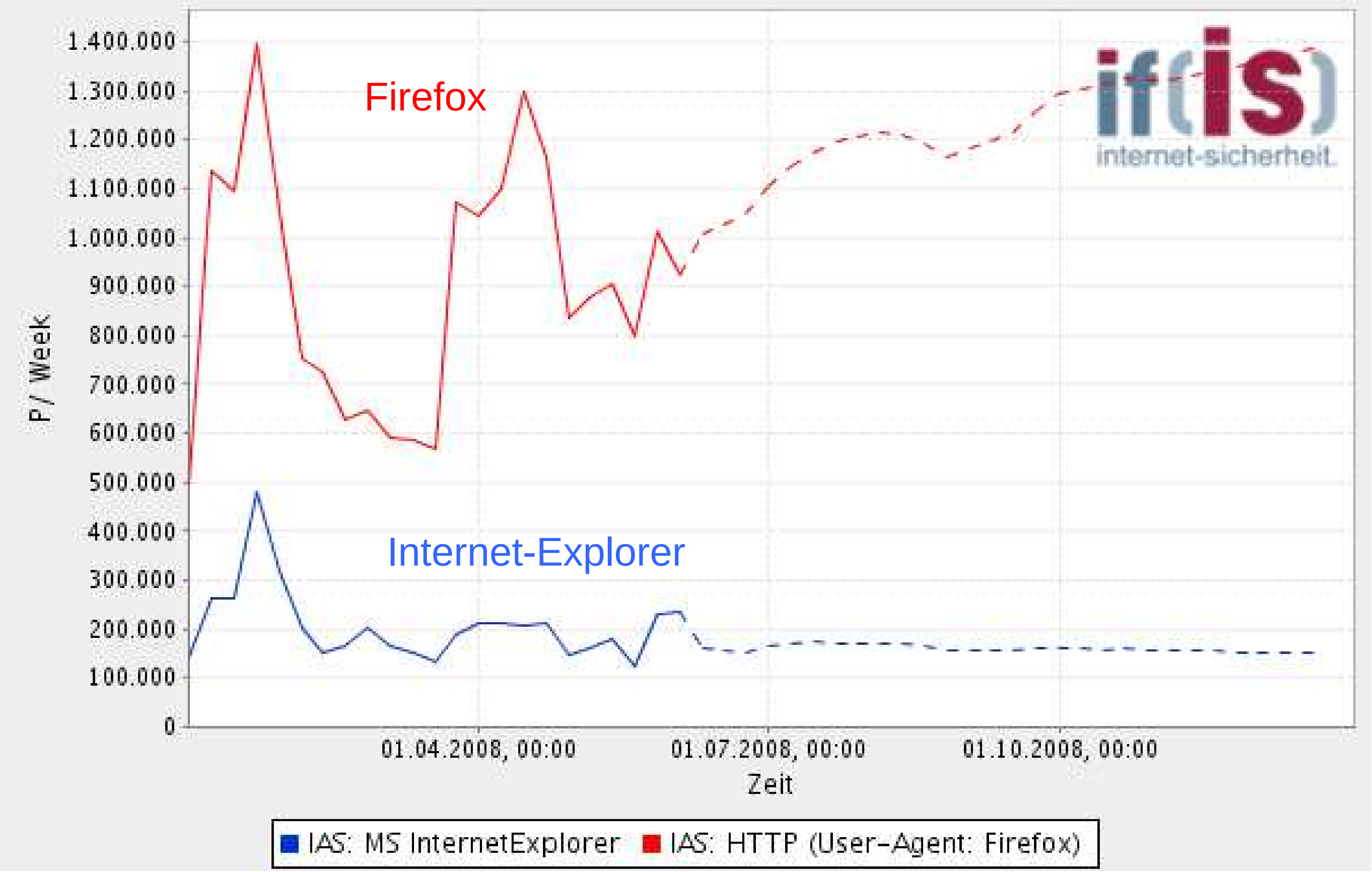
$$time\,series = Trend + economic\,cycle + seasonal + Rest$$

- Time series consists out of different components
  - **Trend**
    - Long-term changes of the average (direction)
  - **Economic cycle**
    - Short-term changes (local trends)
  - **Seasonal**
    - Variations due to day, night, weekends etc.
  - **Rest**
    - Unaccountable influences or breakdowns

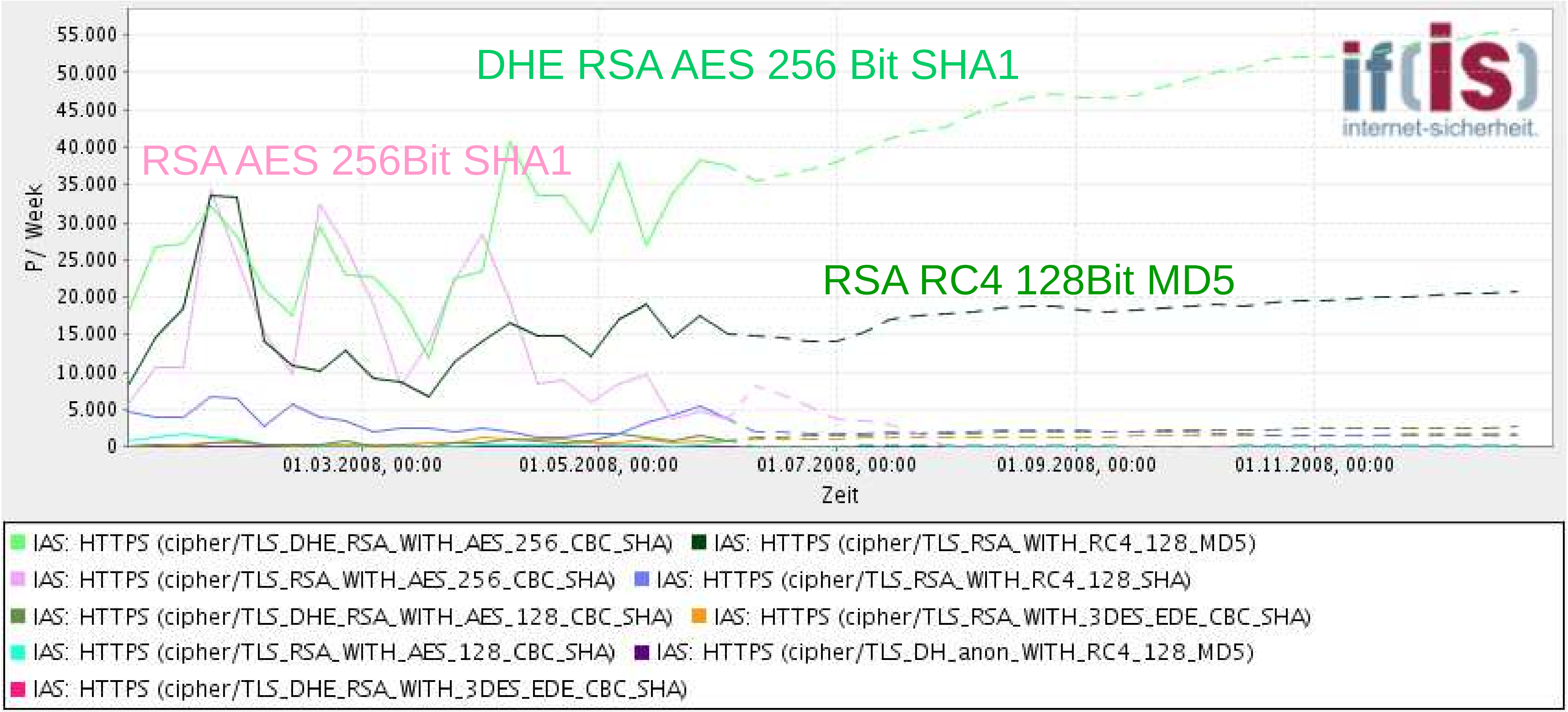
EagleX Plotter
→ Examples

- Statistics of browsers used
- SSL (HTTPS Cipher)
- Operating systems by the means of IP TTL
- Overload on the mail system

Internet Analysis System (IAS)
→Technology trend (Firefox vs. IE)



Internet Analysis System (IAS)
→Technology trend: SSL (HTTPS Cipher)

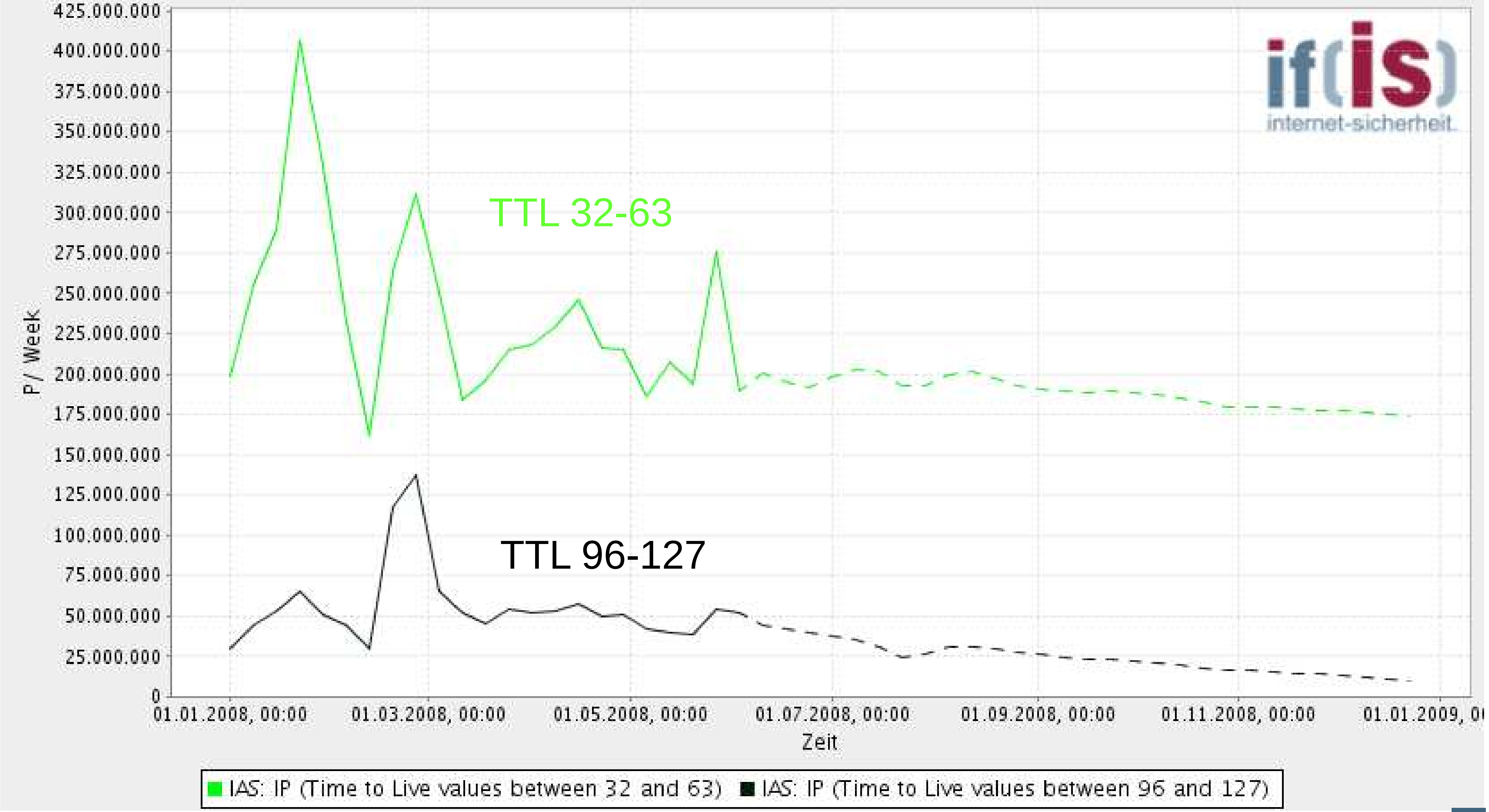


DHE RSA AES 256 Bit SHA1

RSA AES 256Bit SHA1

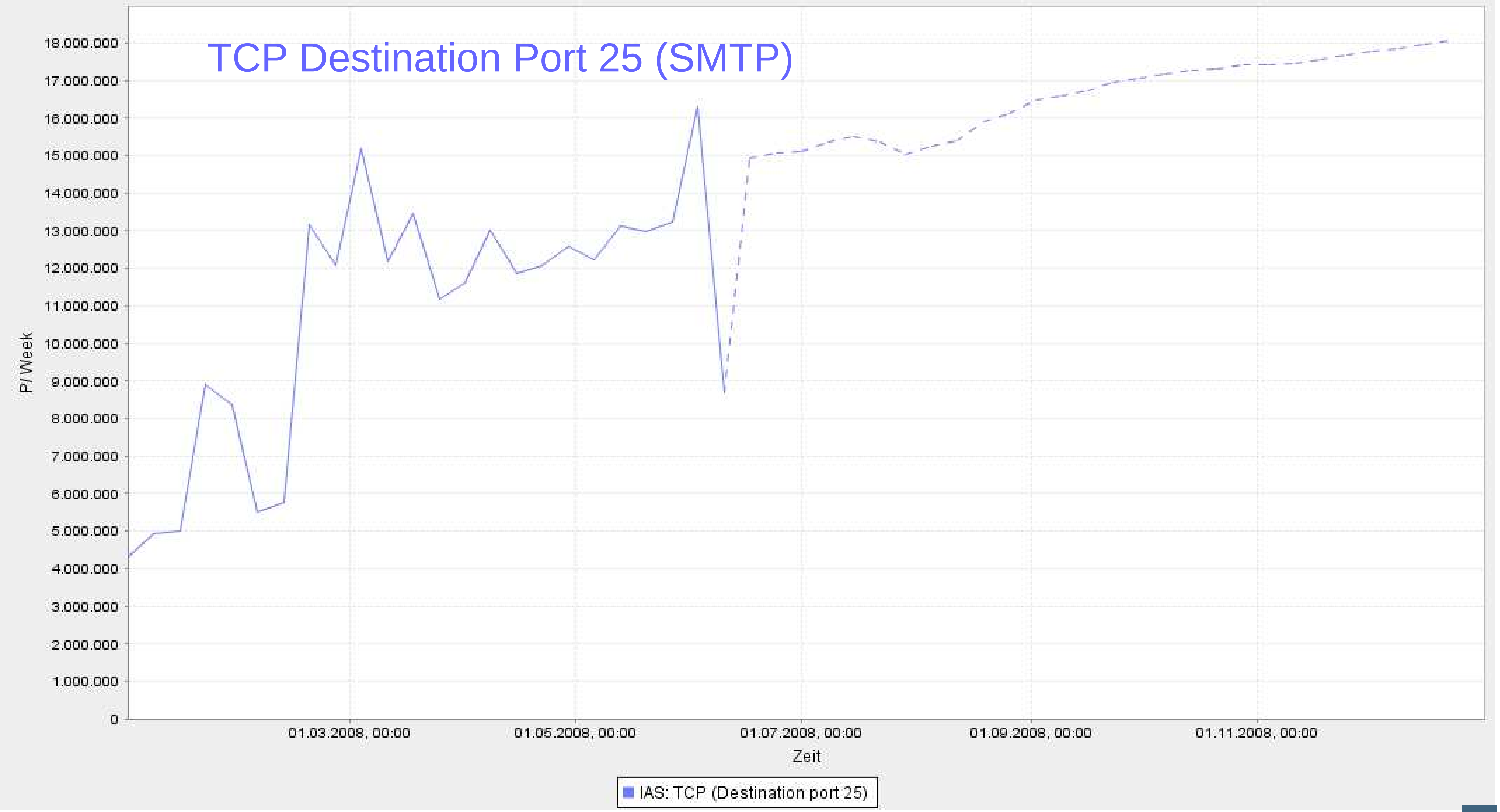
RSA RC4 128Bit MD5

Internet Analysis System (IAS)
→T-trend: Operation Systems (IP TTL)



- Default value: Linux: 64 and Windows: 128

Internet Analysis System (IAS)
→Technology trend (TCP Dst Port 25)



Results

- **Long-term forecast**
  - Possible with or without seasonal
    - Without season the trend is noticeable very clearly
  - Linear regression offers the greatest accuracy
  - In case of heavy noise methods of smoothing are more precise

- **Short-term forecast**
  - Seasonal examination is important
    - Day- and night changes, lunch break
    - Working day and holidays
  - When you break down to an interval of hours: Linear regression
  - In the interval of minutes: Holts-Winters-Method
  - The shorter the interval the more exact “Holts-Winters” turns out to be

Content

- Aim and outcomes of this lecture
- Idea of the Internet Analysis System
- Knowledge Base
- Outline of the Current State
- Detection of Attacks and Deflection
- Forecast of Patterns and Attacks
- **Summary**

Internet Analysis System (IAS)
→ Capabilities

- The use of counters enables a wide spectrum for utilization
  - No problem with laws
- All layers are being analyzed, especially the application layer as well
  - Trends in the use of technology
  - Detection of attacks even on the level of the application layer
  - Understanding of the detailed network traffic
  - Differences between theory and reality
  - ...
- Results of very many sensors can be stored for a long period of time, since very little amounts of storage are needed for archiving
- Ideal to be used for internet monitoring cooperation (global view)

Internet Analysis System (IAS)
→ Limitations

- Statistical conclusions
- No IP addresses (e-mail addresses, user data …)
- The payload is not being analyzed
- So far no conclusions on routing or similar things
- Pointed attacks towards single systems can not be detected (perishes in noise)
- So far the decision which protocol is expected to be found in the packet and which plug-in should be used for analyzing is done due to the used port
- Records cannot be used for forensics
- ...

Internet Analysis System (IAS)
→ Compensation of Limitations

- It can be determined with a certain likelihood, whether an attack is initiated by one or many computers (bots).

- If ports are used that so far have never been used, the IAS will detect this as an anomaly right away.

- If an attack has been detected the administrator of a domain can (by law) use other sources (like log files) to look at privacy relevant data (e.g. IP addresses, ...) to identify the attacker and to initiate counteractive measures.

Internet Analysis System (IAS)
→ Summary

- The IAS comes with a comprehensive knowledge base
- The IAS allows a continuous situation awareness to be recorded and displayed.
- Attacks can be detected
- Forecasts can be made and displayed
- The IAS is a great concept to build a global view!
(Take a look at the lecture about global view.)
- In combination with other systems a comprehensive monitoring tool is created which offers a great value to the user.

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Internet Analysis System
→ Part 2

Thank you for your attention!
Questions?

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is)
internet security.

Internet Analysis System (IAS)
→ Literature (1/2)

- [1] N. Pohlmann: "Internetstatistik" (statistics of the internet), Proceedings of CIP Europe Publisher, B.M. Hämmerli, 2005.
- [2] N. Pohlmann, M. Proest: „Internet Early Warning System: The Global View", in "Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2006 Conference", Hrsg.: S. Paulus, N. Pohlmann, H. Reimer, Vieweg-Verlag, Wiesbaden 2006
- [3] N. Pohlmann: "Probe-based Internet Early Warning System", ENISA Quarterly Vol. 3, No. 1, Jan-Mar 2007
- [4] N. Pohlmann: „The global View of Security Situation in the Internet", ECN - European CIIP Newsletter, Volume 3, Brüssel 12/2007
- [5] Sebastian Spooren, Entwicklung eines profilgestützten Visualisierungssystems zur Darstellung von raum- & zeitbezogenen Soll-/Ist-Abweichungen (development of a visualization tool for the IAS), Diploma Thesis, University of Applied Sciences Gelsenkirchen, 2007.
- [6] Gianfranco Ricci, Betrachtung der vom IAS gesammelten Kommunikationsparameter auf Relevanz zur Anomalie und Angriffserkennung (evaluation of the relevance for the detection of abnormalities and attacks of the communication parameters collected by the internet analysis system), Diploma Thesis, University of Applied Sciences Gelsenkirchen, 2008

Internet Analysis System (IAS)
→ Literature (1/2)

- [7] Uwe van Heesch: Entwicklung eines Plugin basierten Analyse-Frameworks für das Internet-Analyse-System (development of a plugin-based analyzing framework for the Internet Analysis System), Diploma Thesis, University of Applied Sciences Gelsenkirchen, 2006.
- [8] Sabyasachi Basu, Amarnath Mukherjee, Steve Klivansky: Time Series Models For Internet Traffic, 1996
- [9] Peter J. Brockwell, Richard A. Davis: Introduction To Time Series and Forecasting, Springer, 2002

Links:

Institute for Internet Security – if(is):
http://www.internet-sicherheit.de/forschung/aktuelle-projekte/internet-frhwarnsysteme/