Fachhochschule Gelsenkirchen

Internet Early Warning System → Combination

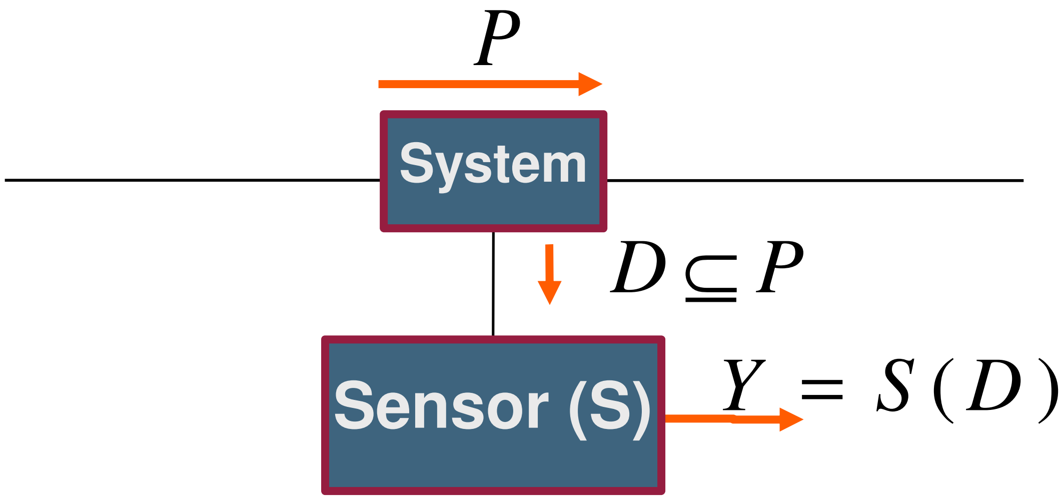
Prof. Dr.
Norbert Pohlmann

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

if(is) internet security.

Structure of an Early Warning System
→ Technical Element: Sensor (S)

- General view on a sensor connected to a communication infrastructure used to transfer data packets



- with
  - **P** := complete data traffic
  - **D** := data traffic going through the sensor
  - **Y** := result of the processing conducted by the sensor
  - **System** := tap, router, switch, computer system, …
- For the information content can be applied: $I(Y) \leq I(D) \leq I(P)$

Structure of an Early Warning System → Technical Element: Sensor (S)

- Sensor collects data, which is used to determine the current status
- Sensors are distributed throughout the entire Network (N), to gain a representative overview of the network
- Different types of sensors have been developed
  - Complete recording of the network traffic (e.g. Wireshark)
  - Netflow (Router - accounting method)
  - Packet based sensors (statistical approach)
  - Honeypots (unreal communication approach)
  - Availability of Services, Nodes and Components
  - LogData analysis (event based approach)
  - …

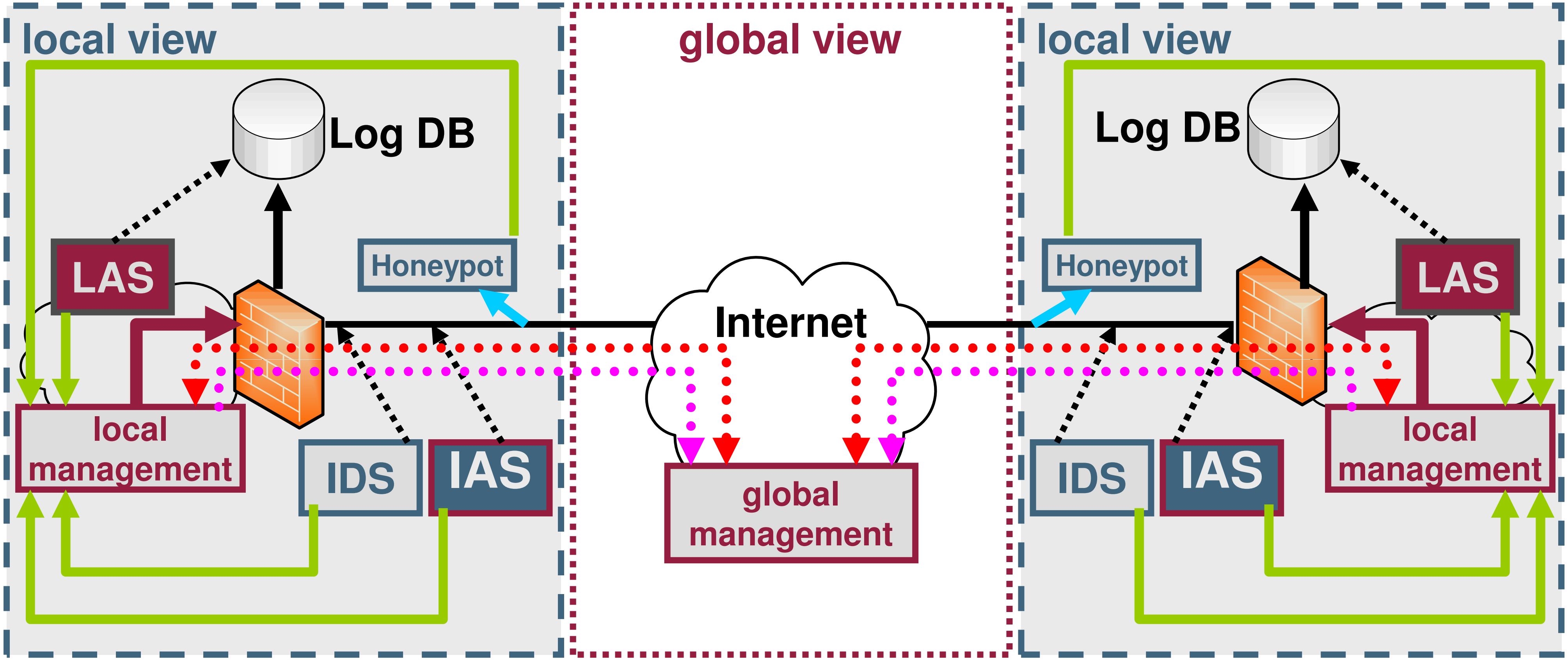
Structure of an Early Warning System → Technical Element: Sensor (S) - 1/2

- **What are the challenges?**
  - Complete data traffic (P)
    - Size of data traffic (up to 400 G bit/s – DE-CIX)
    - Legal conditions (accesses)
    - …
  - Data traffic going through the sensor (D)
    - Performance (CPU, …)
    - Size of the data (10 M/Bit -> 100,58 Gbyte/24 h)
    - Method of reduction/analyze (bytes vs. information)
    - …
  - Result by the sensor (Y)
    - What are the best information?
    - How long can we store the information (size of data)?
    - Legal conditions (pseudonymisation and anonymization)?
    - …

Structure of an Early Warning System → Technical Element: Sensor (S) - 2/2

- **The sensor could be work on different places**
  - wire (without end point influence)
  - in the endpoint (operation system, firewall, application, …)

Internet Early Warning System
→ Cooperation



← Logging of events

⇠ Analysis of traffic and log data

← Branching off of attacks

← Transfer of the findings to local management

⇠ Transfer of anonymous data to global system

⇠⇢ Exchange of data for distributed Early Warning

→ Perform counteractive measures

Fachhochschule Gelsenkirchen

Internet Early Warning System → Combination

Thank you for your attention!
Questions?

Prof. Dr.
Norbert Pohlmann

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

if(is) internet security.