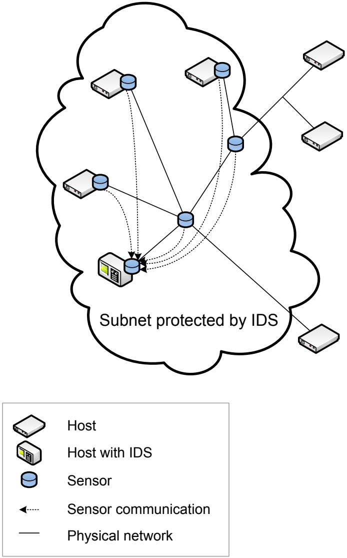
Self-Adaptive Intrusion Detection Agents Based on OC Techniques

Dominik Fisch, Bernhard Sick

University of Passau
Department of Informatics and Mathematics
Research Group "Computationally Intelligent Systems"

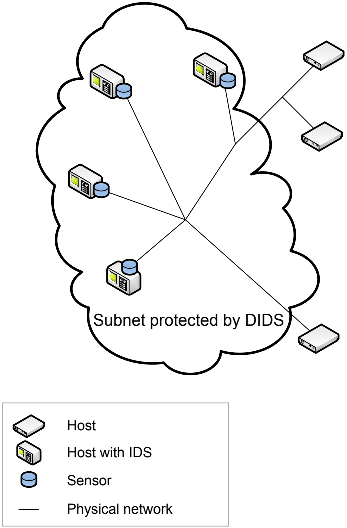
10th Colloquium of the DFG Priority Program 1183
"Organic Computing"
February 22./23. 2010, Hannover

Intrusion Detection System (IDS)



- IDS protect computer systems
  - Objective: Scan data for intrusions and alert administrator
  - Scanned data: Network traffic, log files, firewall messages, ...
- Shortcomings of conventional IDS:
  - Single point of failure
  - Bottlenecks

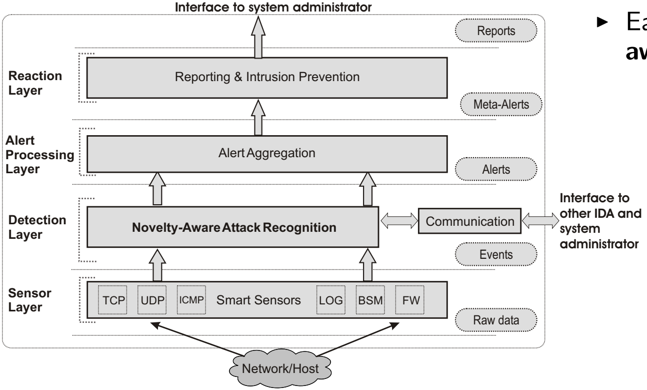
Distributed Intrusion Detection System (DIDS)



- DIDS to the rescue
- Existing work:
  - uses hierarchies with one or more central components
  - collaboration focuses on correlation of attacks

DIDS With OC Techniques

- Structurally similar Intrusion Detection Agents (IDA)

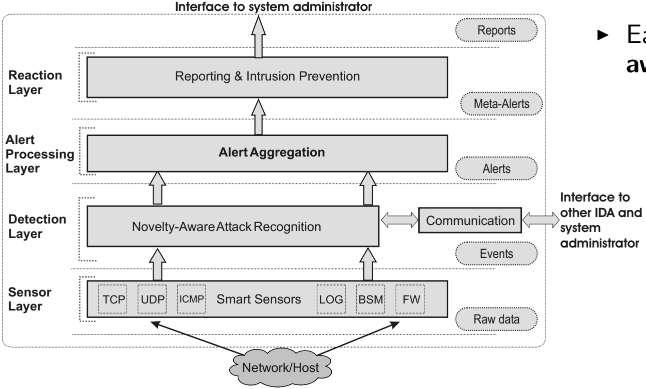


- Each IDA is **situation-aware** and **self-adaptive**:
  - ★ performs its own detection task locally
  - ★ is able to detect the need for new knowledge (i.e., new attack types)
  - ★ is able to handle this situation, i.e., learn new classification rules

- **Novelty-Aware Attack Recognition – Intrusion Detection With Organic Computing Techniques**, BICC2010 (review)

DIDS With OC Techniques

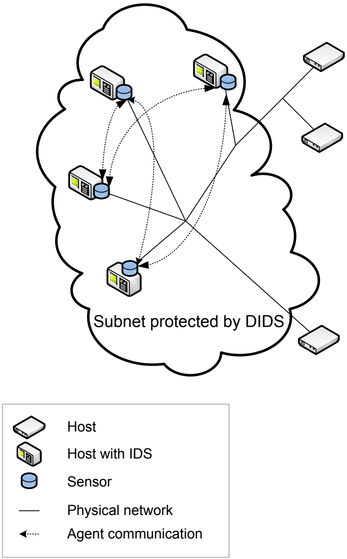
- Structurally similar Intrusion Detection Agents (IDA)



- Each IDA is **situation-aware** and **self-adaptive**:
  - ★ aggregation of produced alerts
  - ★ representation of current attack situation
  - ★ new knowledge corresponds to new attack instances

- **On-Line Intrusion Alert Aggregation With Generative Data Stream Modeling**, IEEE TDSC

DIDS With OC Techniques: Knowledge Exchange



- IDA exchange learned rules
  - enables **pro-active** behavior
  - rule integration is controlled by an assessment of rules

Thanks a bunch for your attention!

More information: `http://www.cis-research.de`