

# Aspects of high-speed network monitoring

Prof. Dr. Georg Carle

Chair for Computer Networks and Internet  
University of Tübingen

`carle@informatik.uni-tuebingen.de`

`http://net.informatik.uni-tuebingen.de`

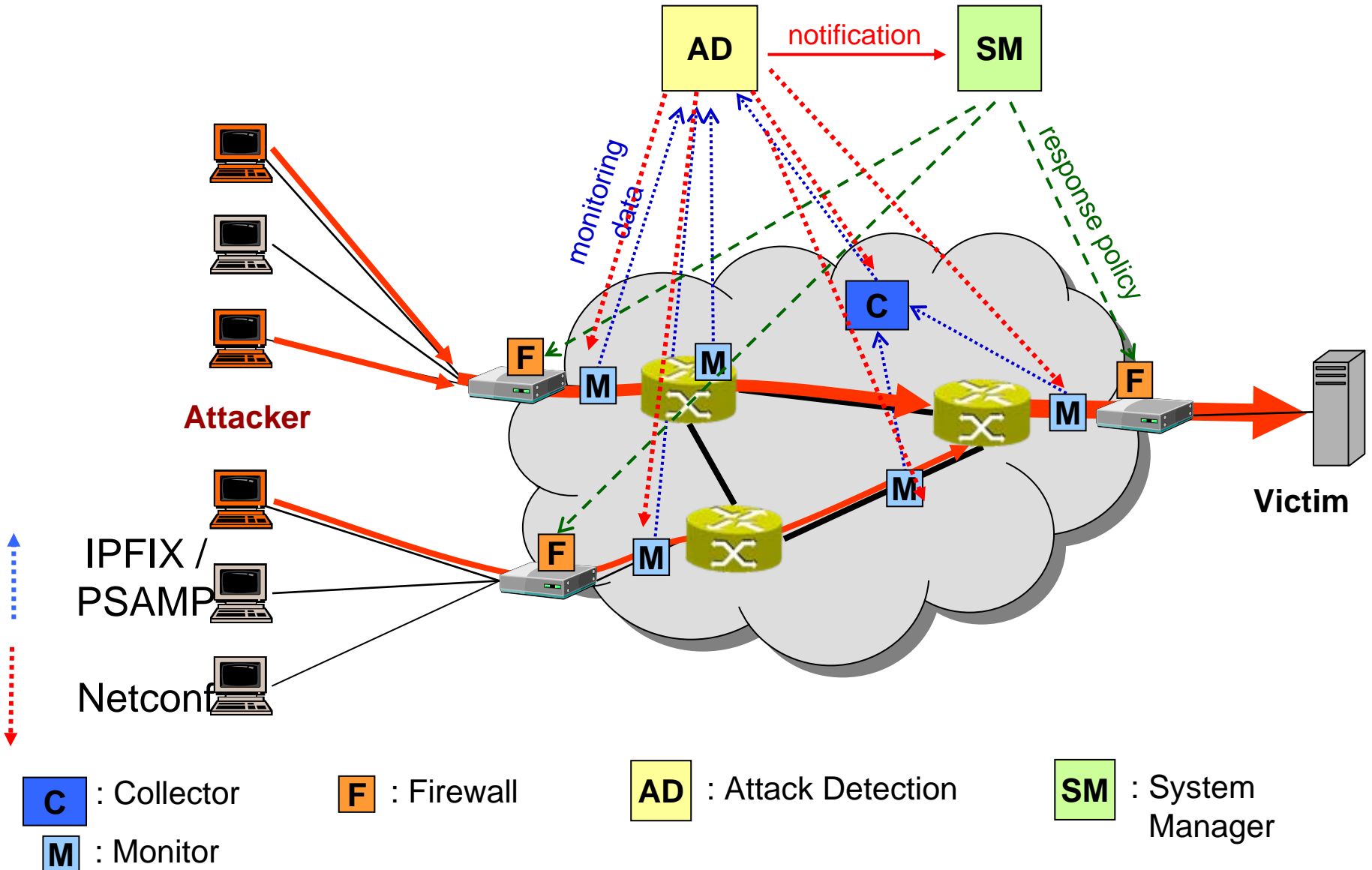
Work in cooperation with  
Falko Dressler, Gerhard Münz  
and the partners of the Diadem Firewall project

## Outline:

Distributed Monitoring → Research Questions → Approach



# Distributed Monitoring – Diadem Firewall





# Research Questions

## □ Research Questions on System Architecture

### A) Flexibility

- do we need highly flexible monitors – in order to always choose the best monitoring functionality for the available monitoring performance?
- If yes: which entity should decide this?
- Should we have programmable pre-processing?

### B) Structure

- Hierarchical - Should we have multiple stages, and if yes – how many?
  - Monitoring – Aggregation – Evaluation  
(cf. Dressler, Münz: Internet-Draft draft-dressler-ipfix-aggregation )
  - Which entity specifies the functionality of each stage, and how aggregation is done?
- „Self-Organizing“ Measurement overlay?
  - Possible role of peer-to-peer mechanisms to organize high-speed monitoring?

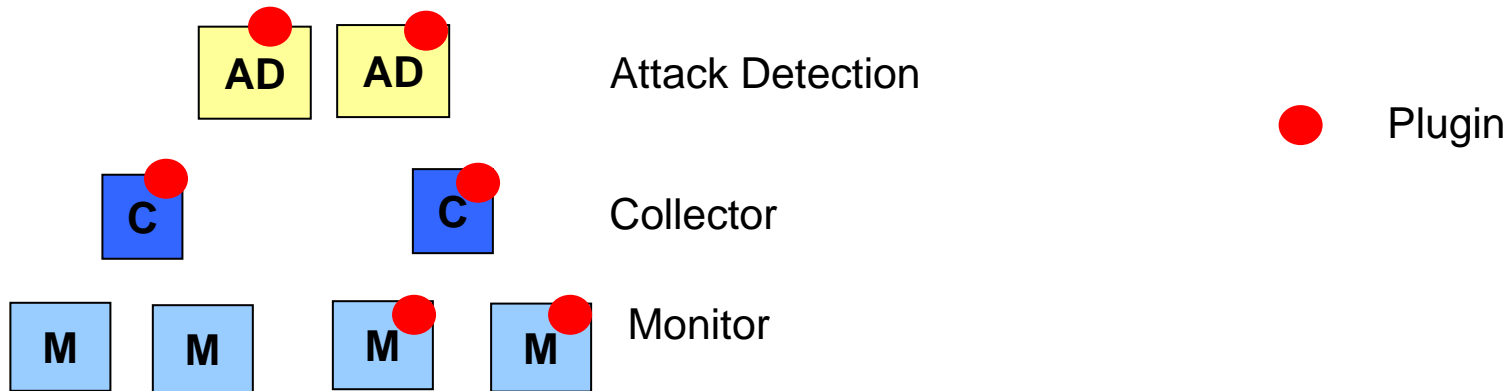


# Suggested Approach

- ❑ Identify the standard monitoring
  - Specify granularity statically
  - Fast, Hardware-supported (KISS-principle)
  - „Hard-wire“ standard monitoring
  - Store these results, make them available to a range of post-processing components

⇒ scalable, affordable high-speed solution
- ❑ Multi-stage programmable software monitoring
  - Programmable Flexibility
  - Support for service-specific / application-specific monitoring functionality

⇒ flexible solution for innovative solutions





**Thank you!**

**Questions?**