Zukunft der Netze 2012, 28.09.2012, Wien

Future Internet Security – Applying Cross-Level Cooperation and Functional Composition

Results and Experiments from G-Lab DEEP

Erwin P. Rathgeb, Irfan Simsek

Alfried Krupp von Bohlen und Halbach-Stiftungsprofessur

Technik der Rechnernetze

Institut für Experimentelle Mathematik und

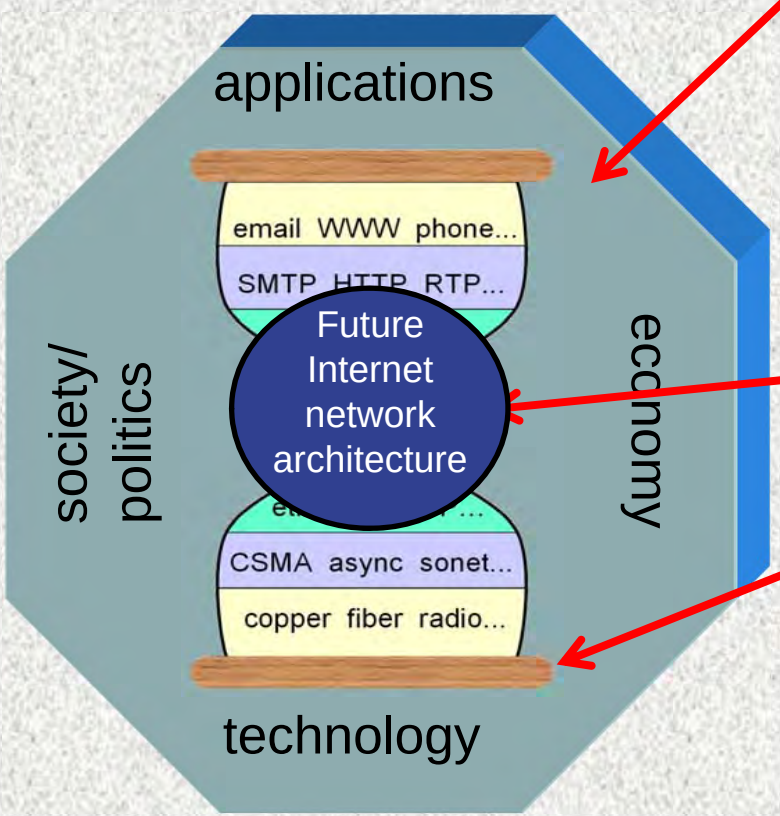
Institut für Informatik und Wirtschaftsinformatik

Universität Duisburg-Essen (Campus Essen)

G-Lab DEEP overview

- G-Lab Phase II project
- Project duration
  - 36 month
  - 01.09.2009 – 31.08.2012
- Partner
  - Fraunhofer FOKUS (lead)
  - TU Kaiserslautern
  - Universität Duisburg-Essen
  - TU Berlin

Motivation – Internet ecosystem evolution



- Dynamic innovations in applications
  - the Web
  - File sharing / overlays
  - VoIP, Triple play, …
  - …the future is Web2.0/3.0 …

„Ossification“ of the core protocols

Future Internet core architecture?

- Permanent evolution of the underlying technologies
  - Wireless / mobile
  - All over ethernet
  - Optical
  - … the future is optical/mobile …

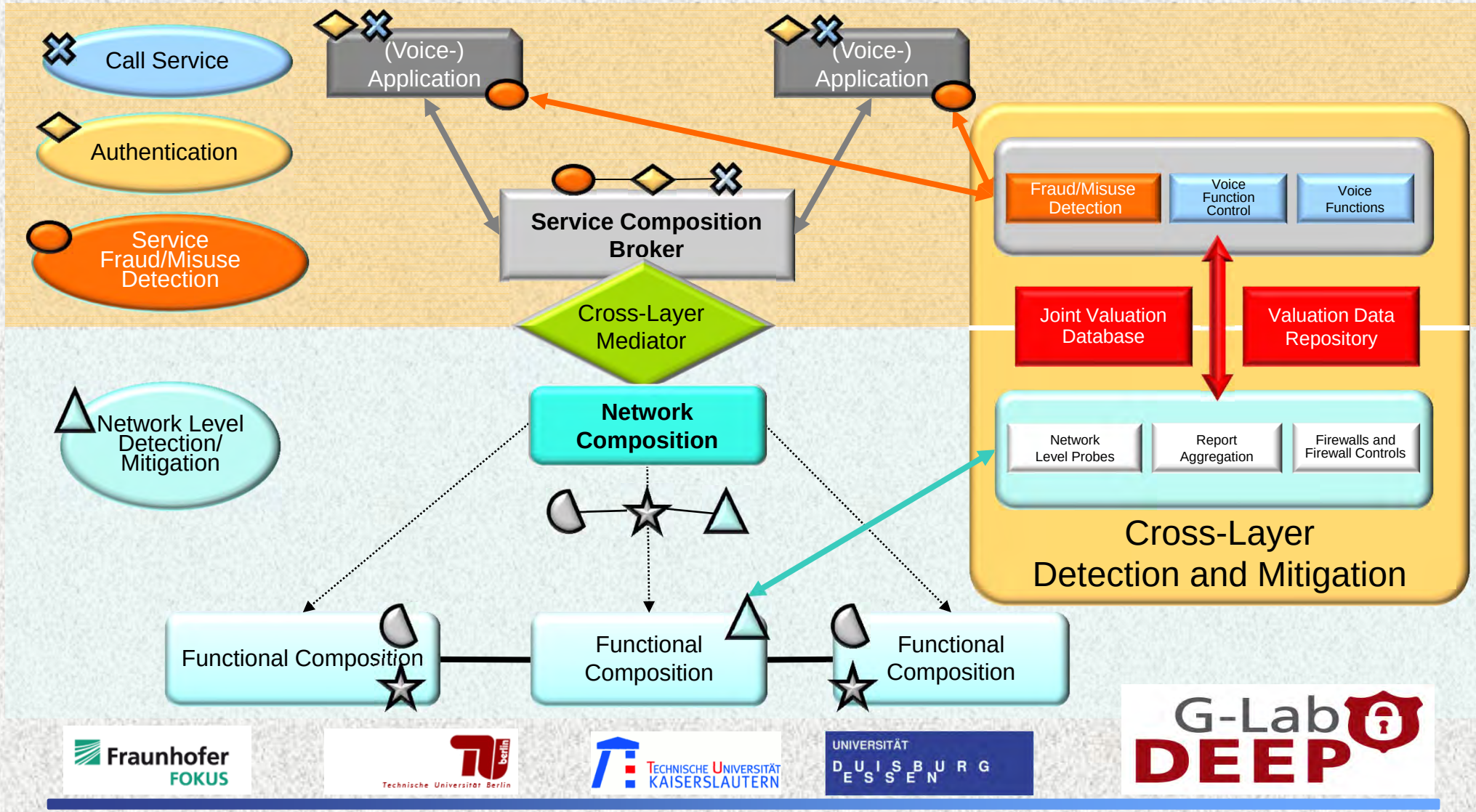
Adopted from a slide by Paul Müller, TU Kaiserslautern

Motivation and key ideas

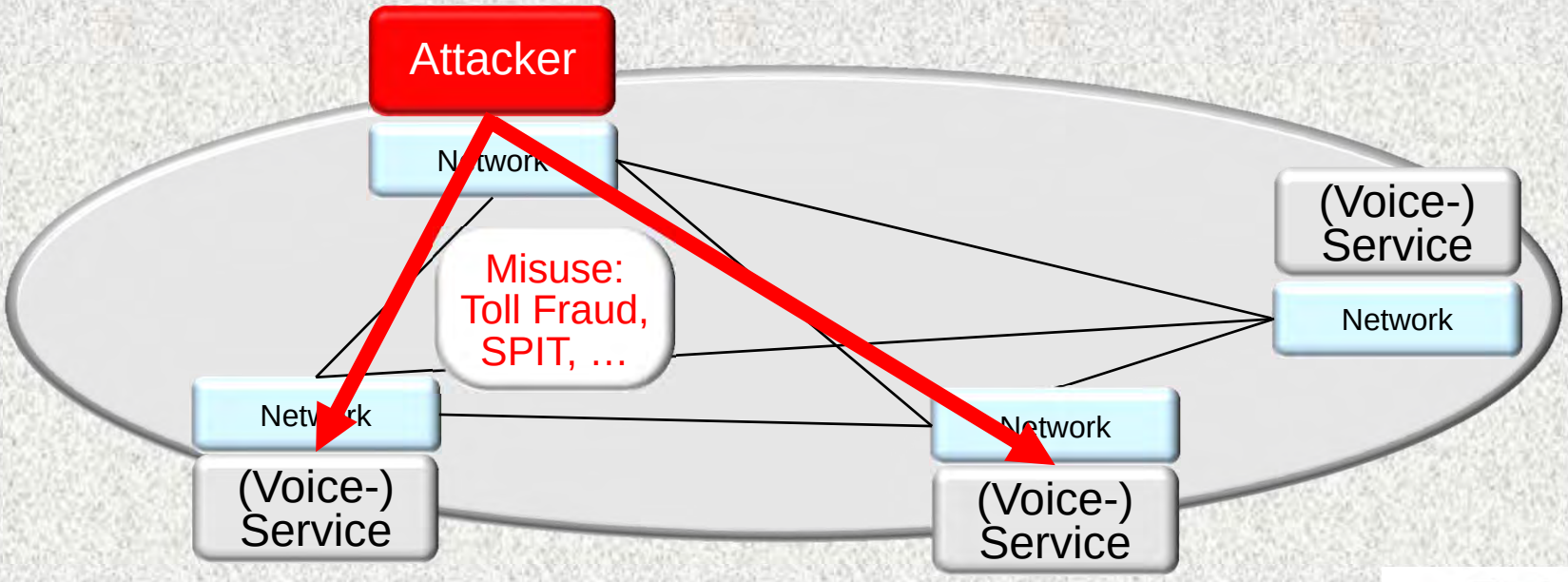
UNIVERSITÄT DUISBURG ESSEN

- Security in the today's Internet
  - "Fix it as you go"
    - Was the only viable strategy as yet
  - ➔ Multiple fragmented and complex solution approaches
    - Obviously inadequate from conceptual as well as operational perspective
- Completely new Future Internet architecture
  - More disruptive ideas on Internet security feasible
- Dynamic Functional Composition of security functions
  - Adaptation to network/service threat level
  - "Security on Demand"
- Cross-level cooperation
  - Combining the strengths of network and service level security approaches
    - Service level: Detailed view (service logic) but limited scope
    - Network level: Coarse view (protocol type only) but wide scope
- Use Case: Interactive voice and multimedia services
  - Vulnerabilities and possible attack scenarios are already fairly well known

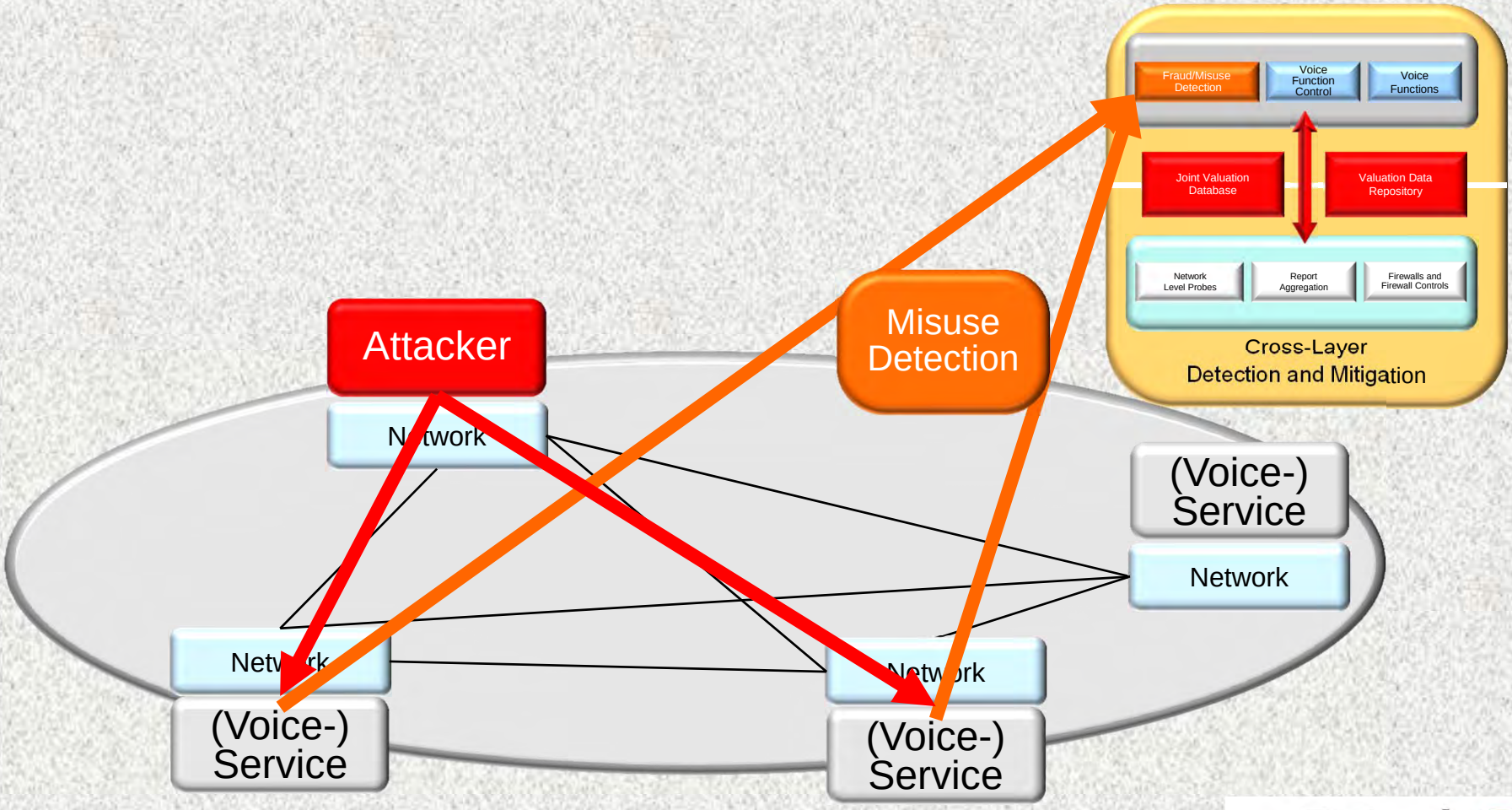
G-Lab DEEP – Key ideas (security focus)



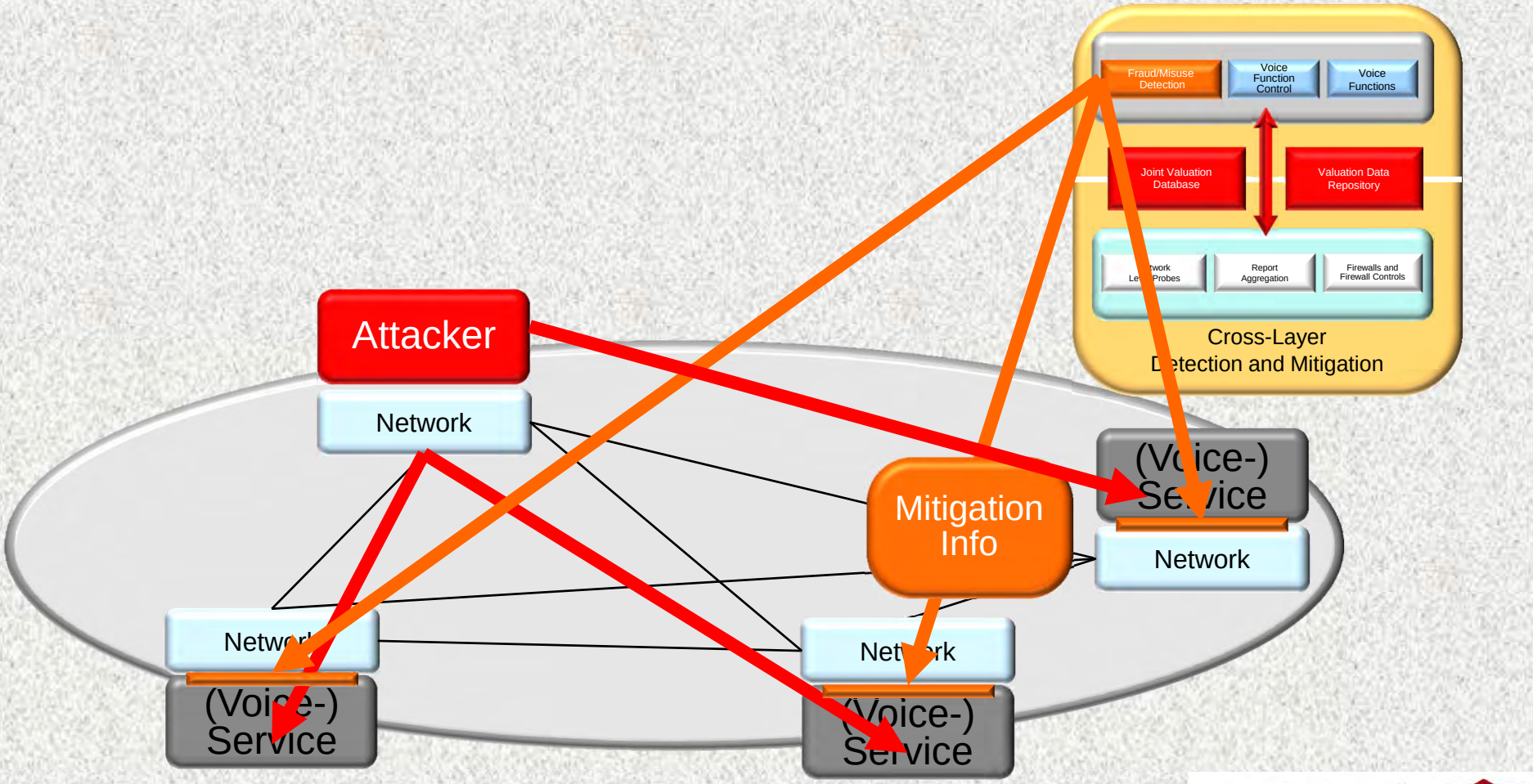
G-Lab DEEP –
Cross-level monitoring and attack mitigation



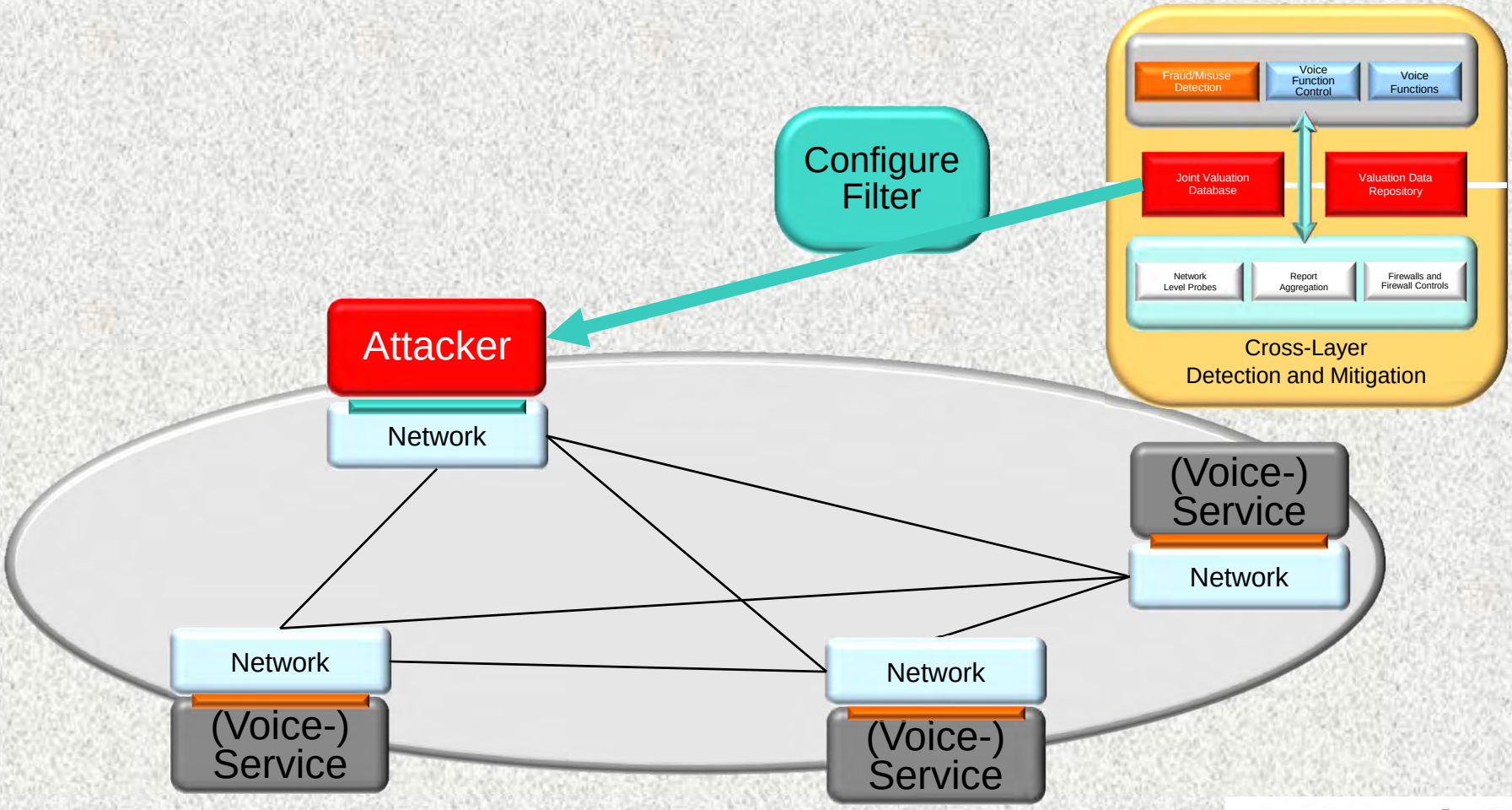
G-Lab DEEP –
Cross-level monitoring and attack mitigation



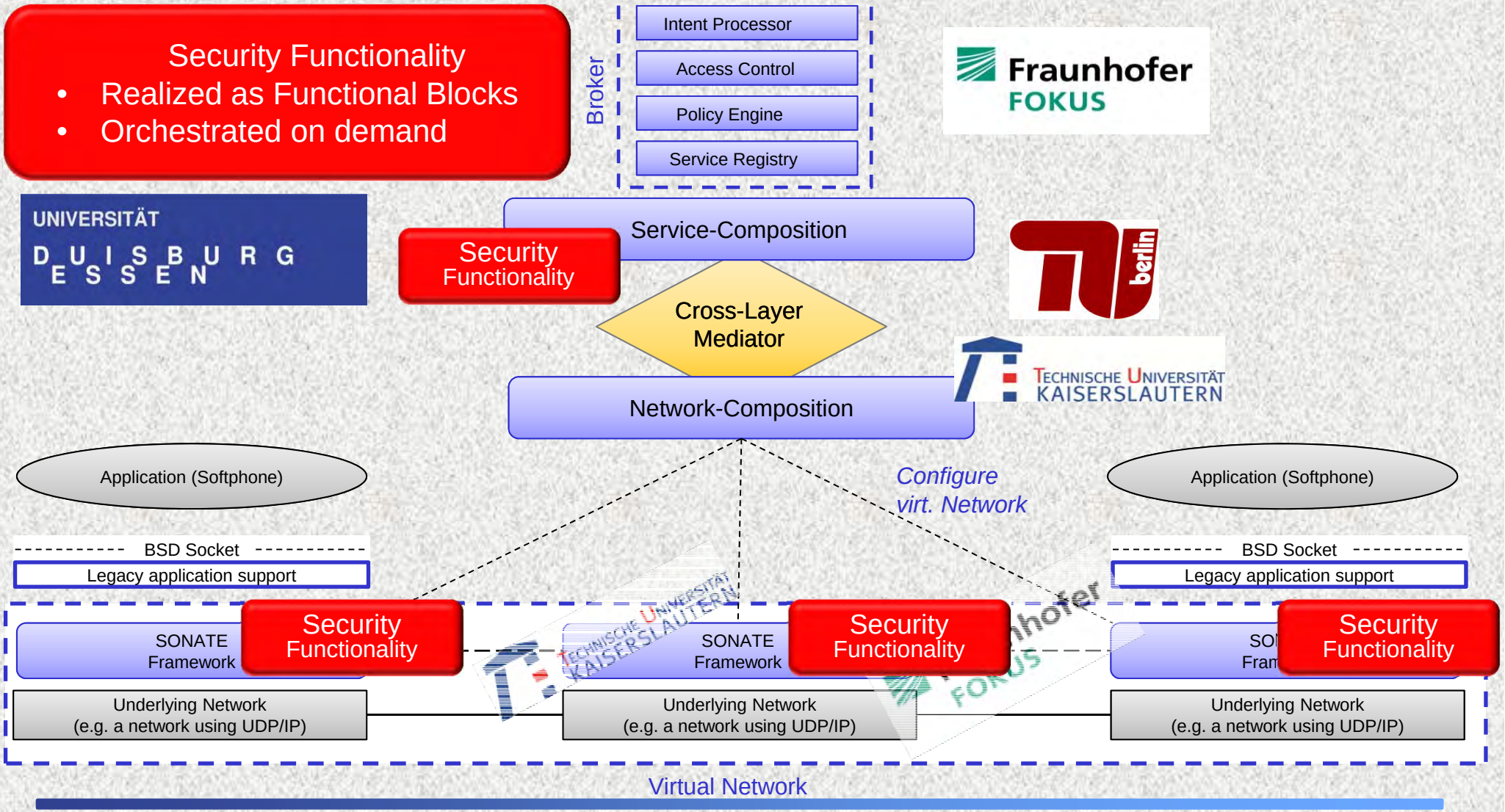
G-Lab DEEP –
Cross-level monitoring and attack mitigation



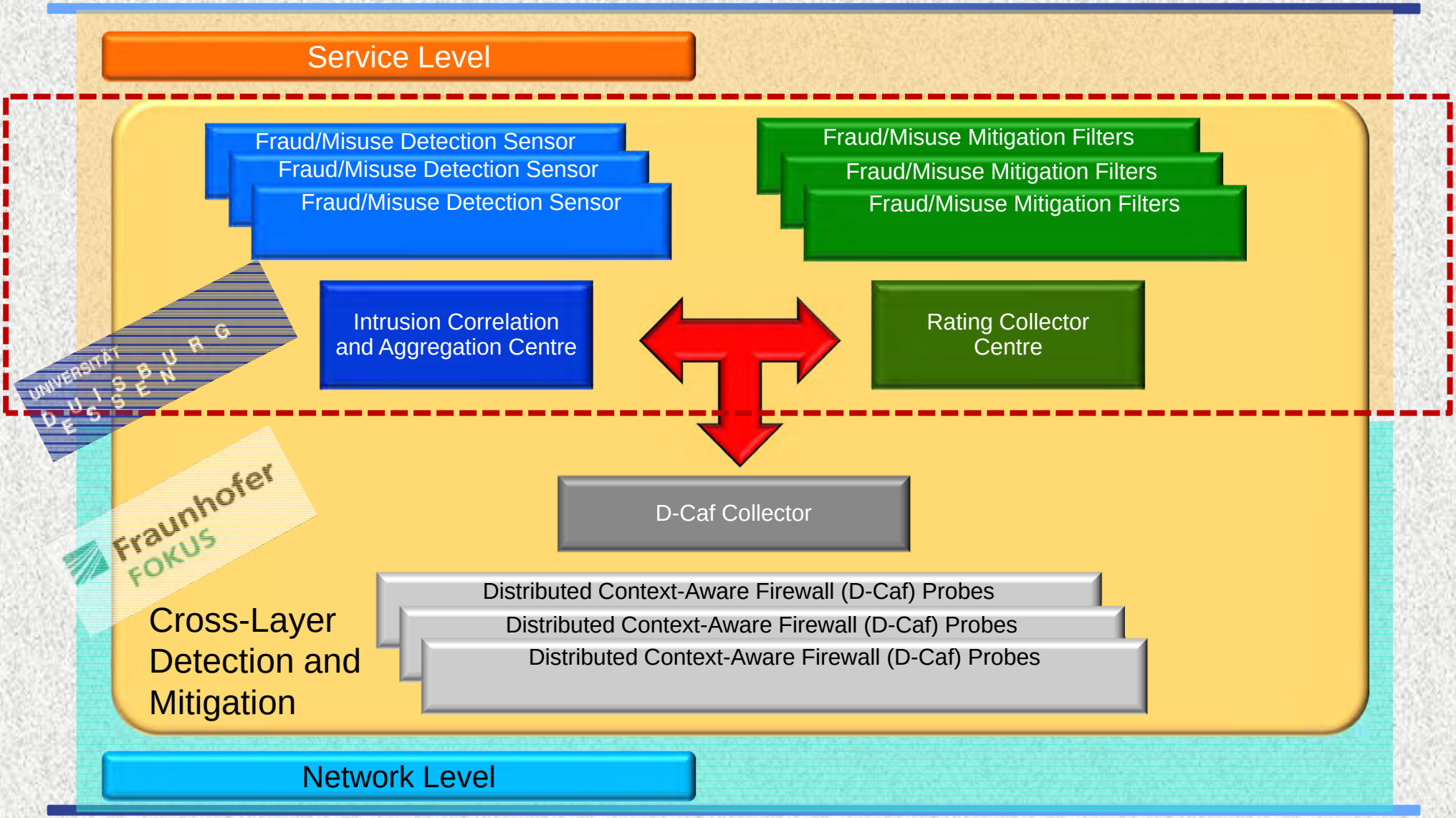
G-Lab DEEP –
Cross-level monitoring and attack mitigation



G-Lab DEEP – Functional Composition system overview

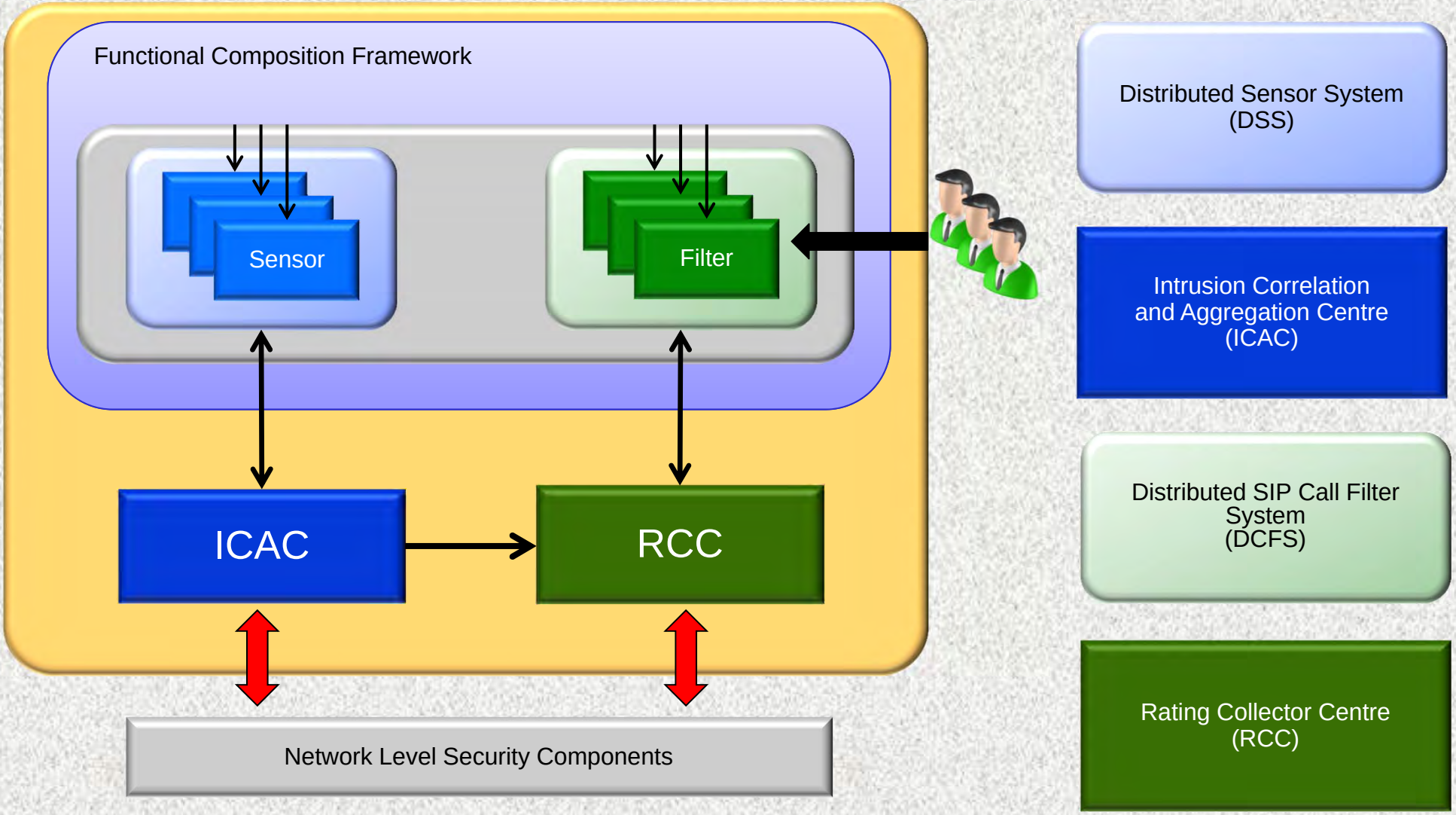


G-Lab DEEP – Security function overview



Service Level security components – Overview

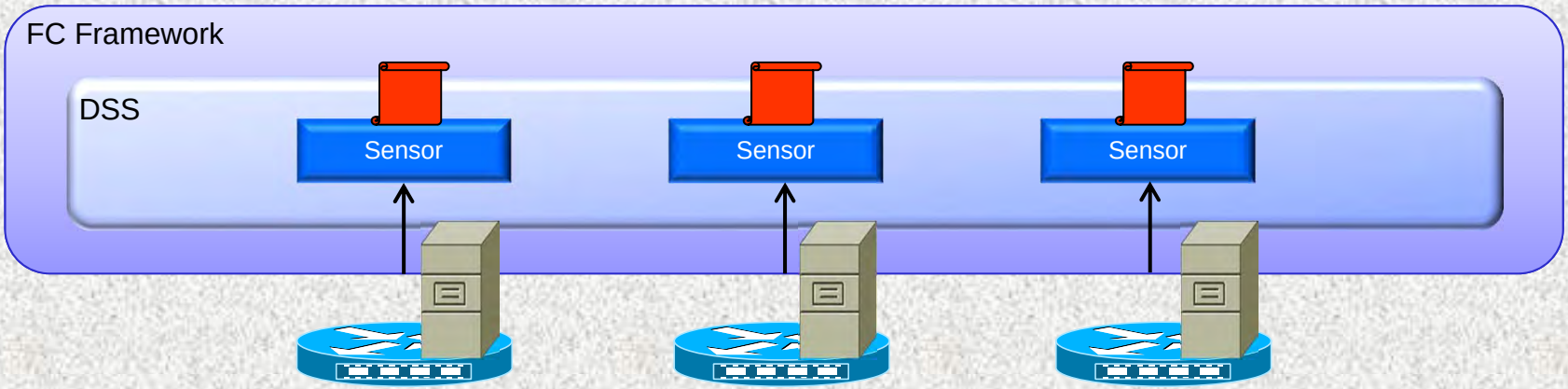
UNIVERSITÄT DUISBURG ESSEN



Service Level security components – Detection: Distributed Sensor System

UNIVERSITÄT DUISBURG ESSEN

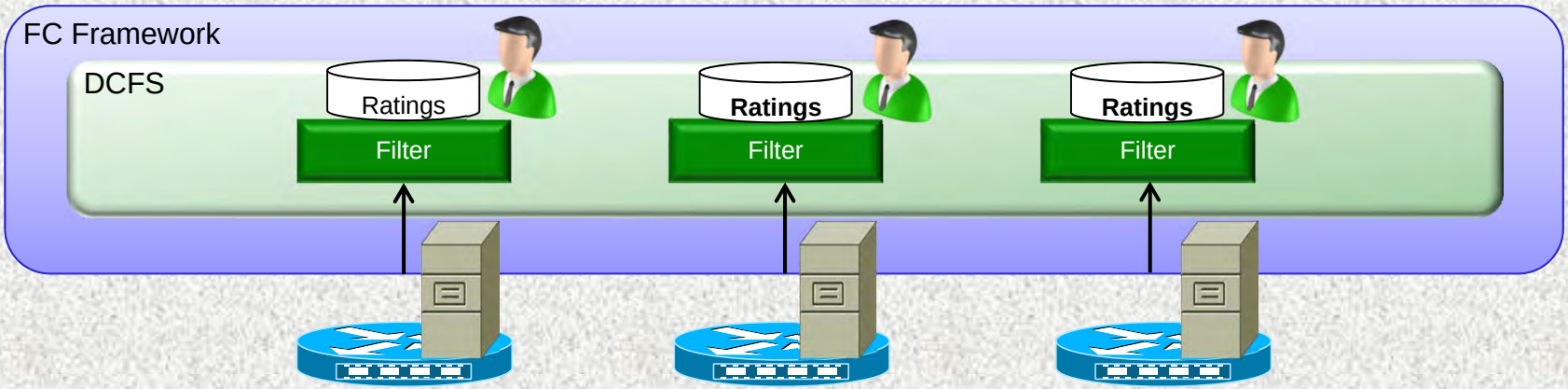
- A single sensor acts as a Functional Block
  - Can be activated on demand
  - Via Functional Composition interface
  - Service specific monitoring
- Sensors operate rule-based
  - Rules based on experience with real attacks
    - E.g. registration hijacking and toll fraud
    - Rules can be updated dynamically



Service Level security components – Mitigation: Distributed Call Filter System

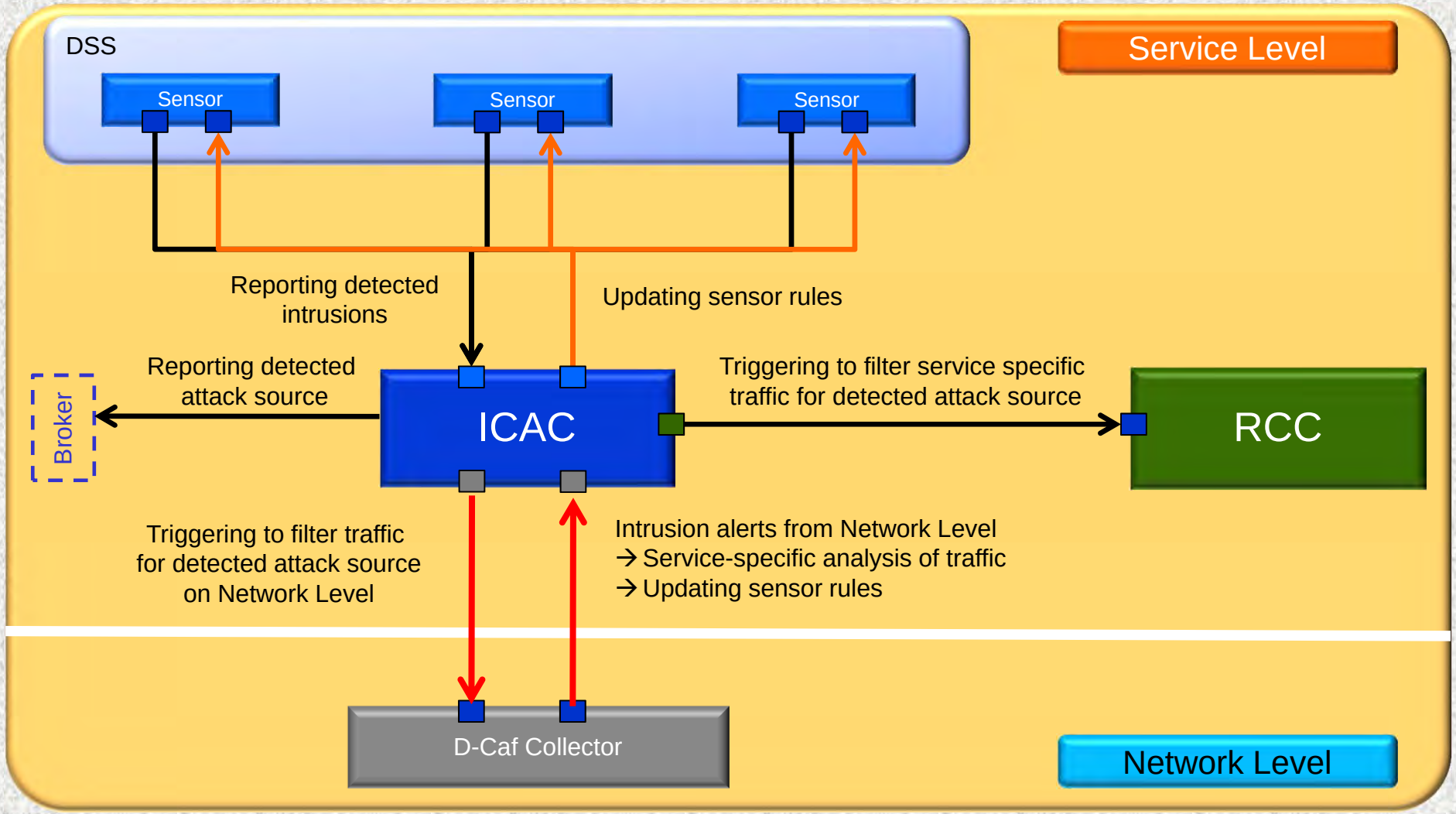
UNIVERSITÄT DUISBURG ESSEN

- A single filter acts as a Functional Block
  - Can be activated on demand
  - Via Functional Composition interface
  - Service specific filtering
- Filters operate rating-based
  - Rating level defines the reaction to incoming call attempts
- Predefined actions
  - E.g. direct completion, solving CAPTCHAs, or complete reject
- End user can rate coming calls



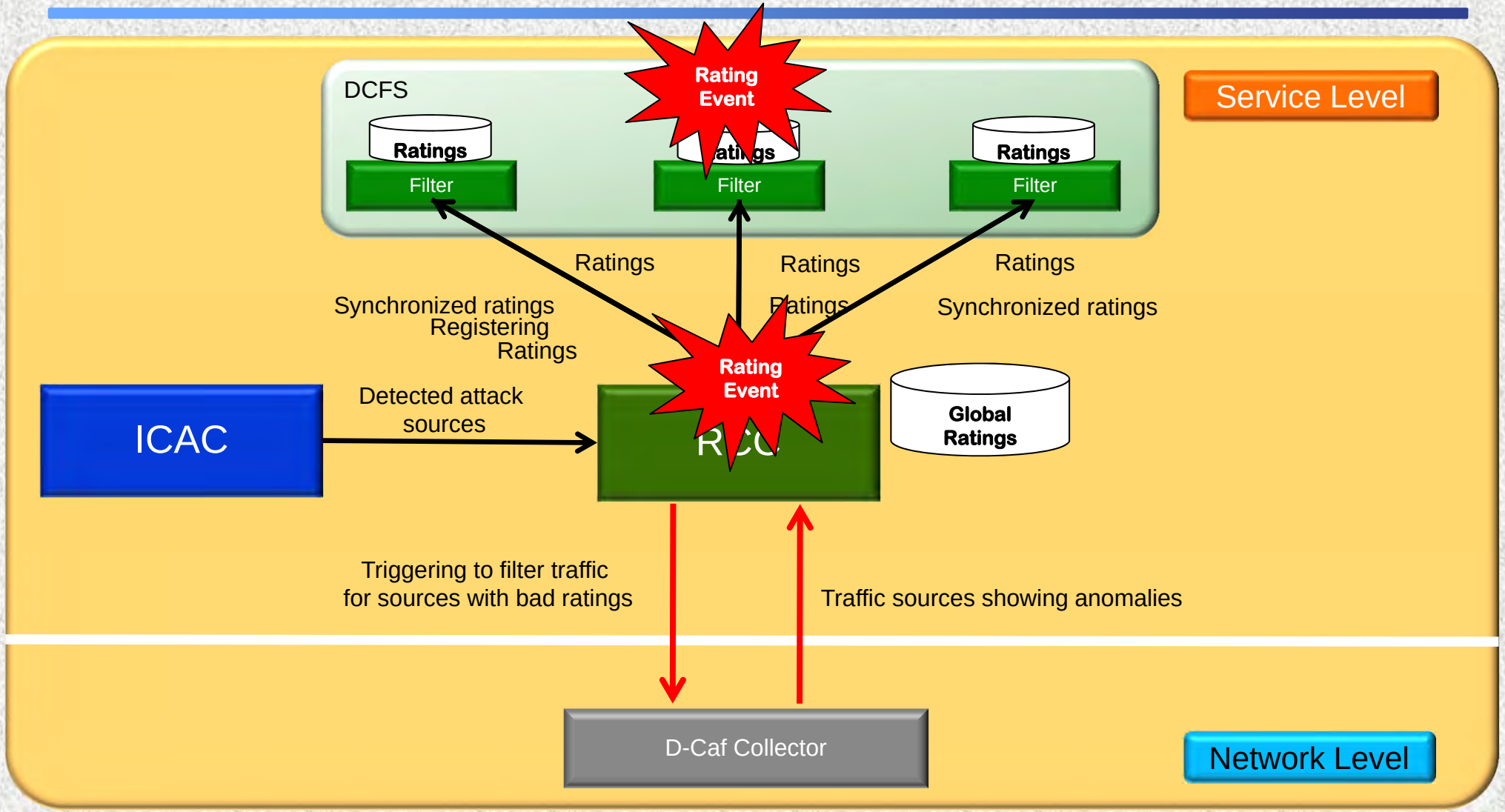
Service Level security components – Intrusion Correlation and Aggregation Centre

UNIVERSITÄT DUISBURG ESSEN



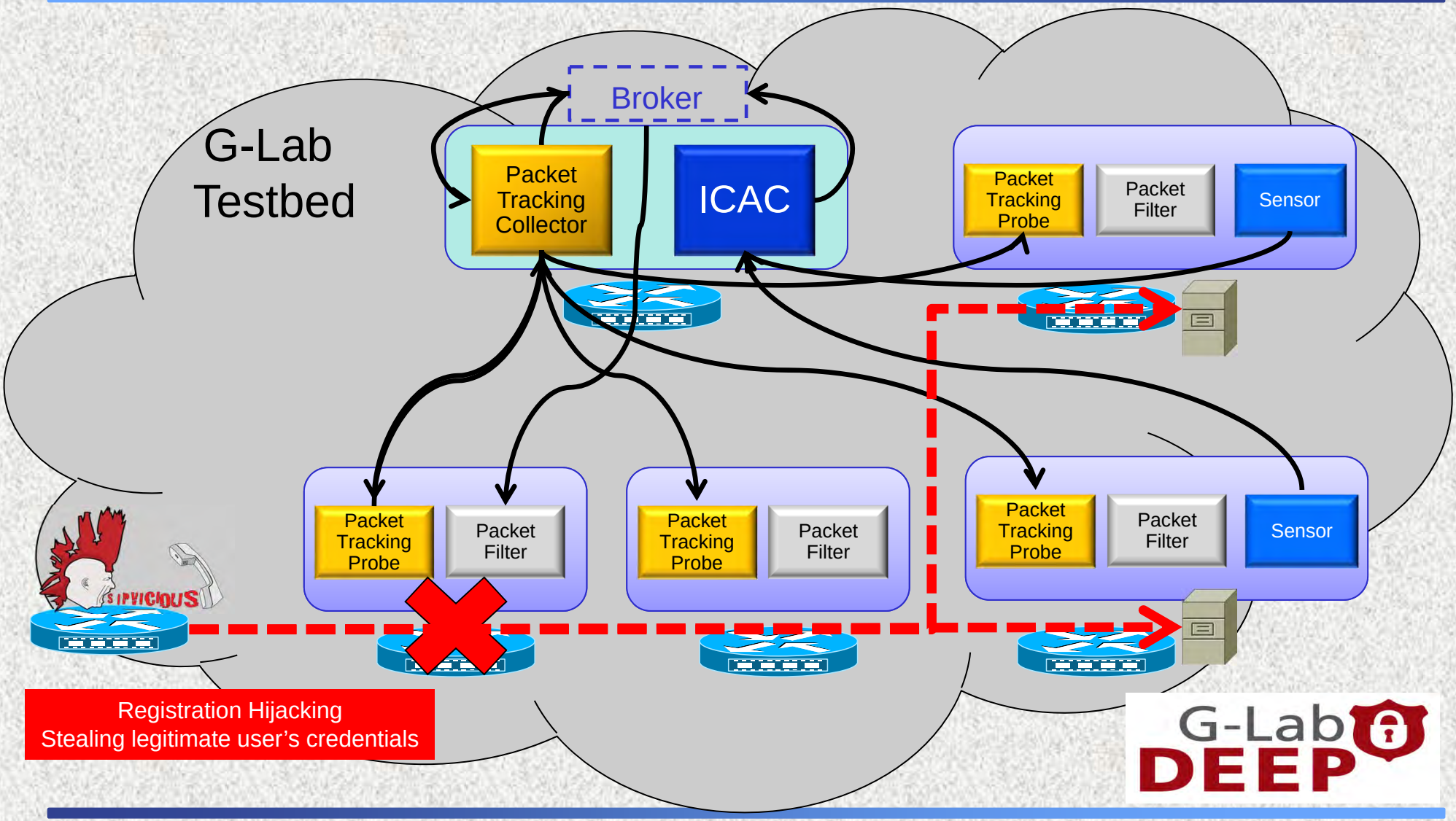
Service Level security components – Rating Collector Centre

UNIVERSITÄT DUISBURG ESSEN



G-Lab Experiment – Functional Composable Cross-Level Security

UNIVERSITÄT DUISBURG ESSEN



Conclusion

UNIVERSITÄT DUISBURG ESSEN

- Feasibility of cross-level security cooperation demonstrated
  - Combining the strengths of network and service level security functionalities
- Feasibility of Functional Composition demonstrated for security functionalities on Service Level
  - Detection and mitigation functionality realized as Functional Blocks
  - Can be orchestrated on demand
- Encouraging results
  - But still a long way to go