Functional Composable Cross-Layer Security

Irfan Simsek
University Duisburg-Essen

SPONSORED BY THE
Federal Ministry of Education and Research

Overview

- Motivation
  - Overview G-Lab DEEP Future Internet Architecture
  - G-Lab DEEP – Key Ideas (Security Focus)
- Detection
  - Distributed Sensor System
  - Intrusion Correlation and Aggregation Centre
- Mitigation
  - Distributed SIP Call Filter System
  - Rating Collector Centre
- Experiment scenarios
- Conclusion

Motivation

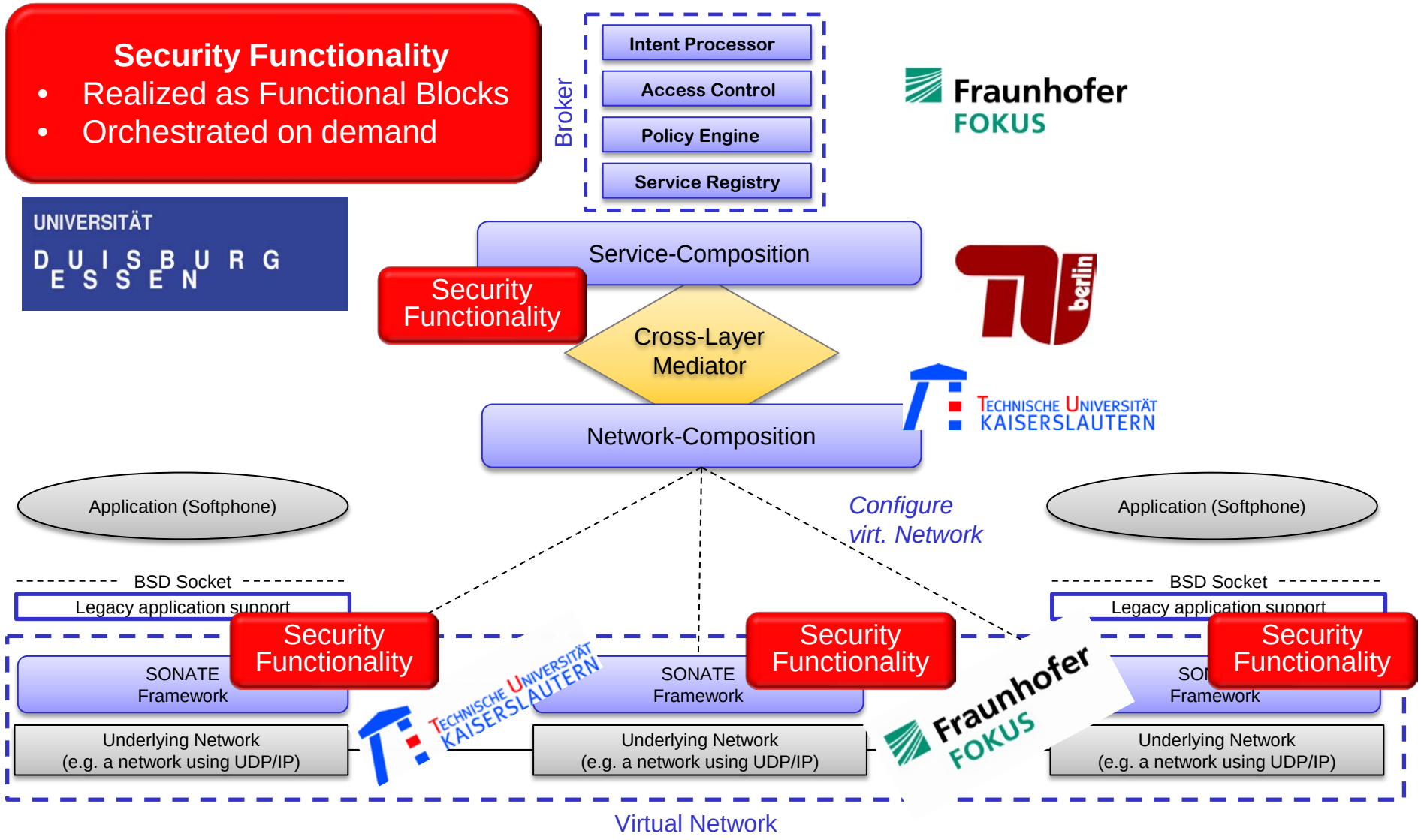
- Security in the today's Internet
  - "Fix it as you go"
    - Was the only viable strategy as yet
  - → Multiple fragmented and complex solution approaches
    - Obviously inadequate from conceptual as well as operational perspective

- Completely new Future Internet Architecture
  - More disruptive ideas on Internet security feasible

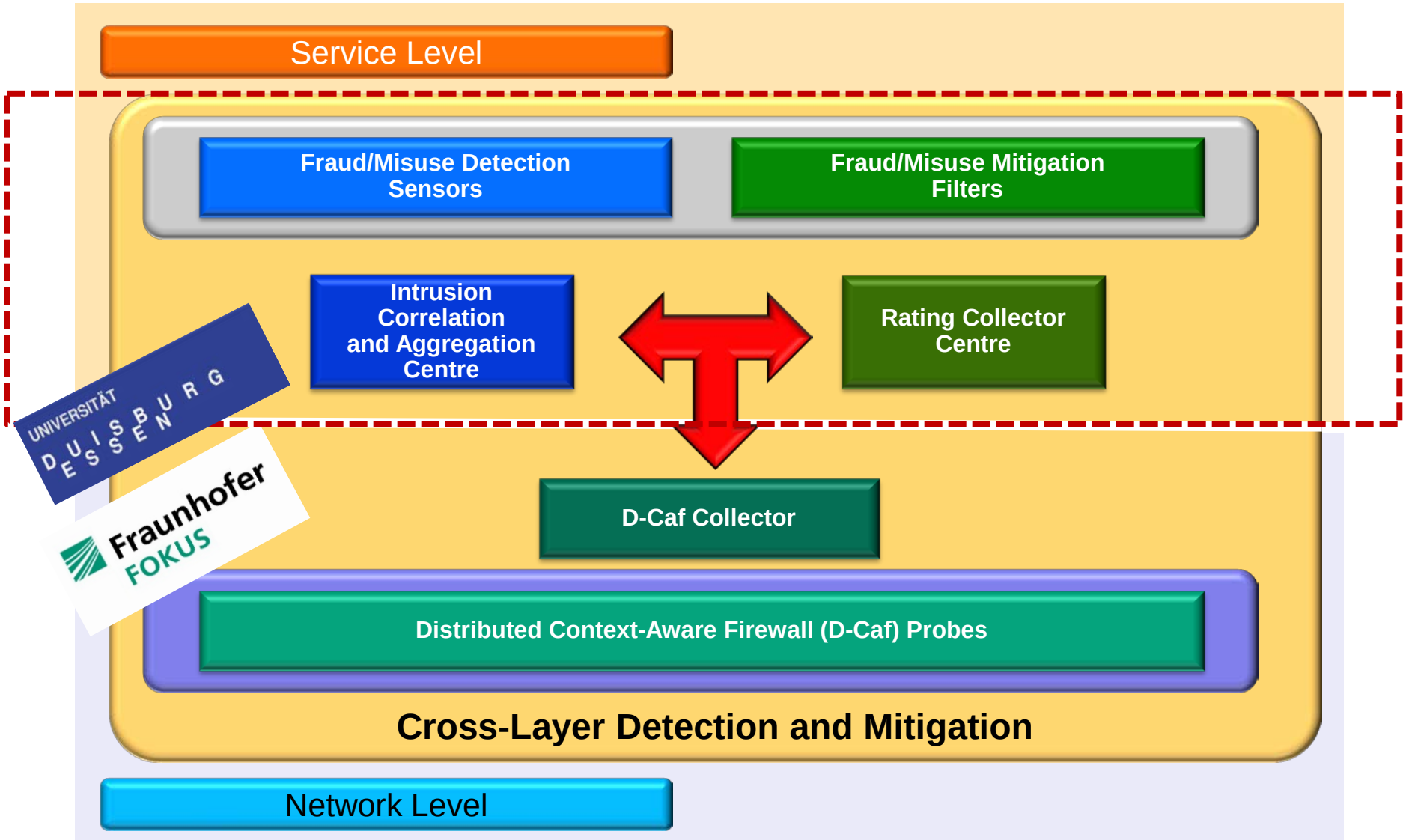
  ➔ Cross-Layer security functionalities
    - Can dynamically be added when required in infrastructure
    - Combining the strengths of network and service level security approaches

- Use Case: Interactive voice and multimedia services
  - Vulnerabilities and possible attack scenarios are already fairly well known

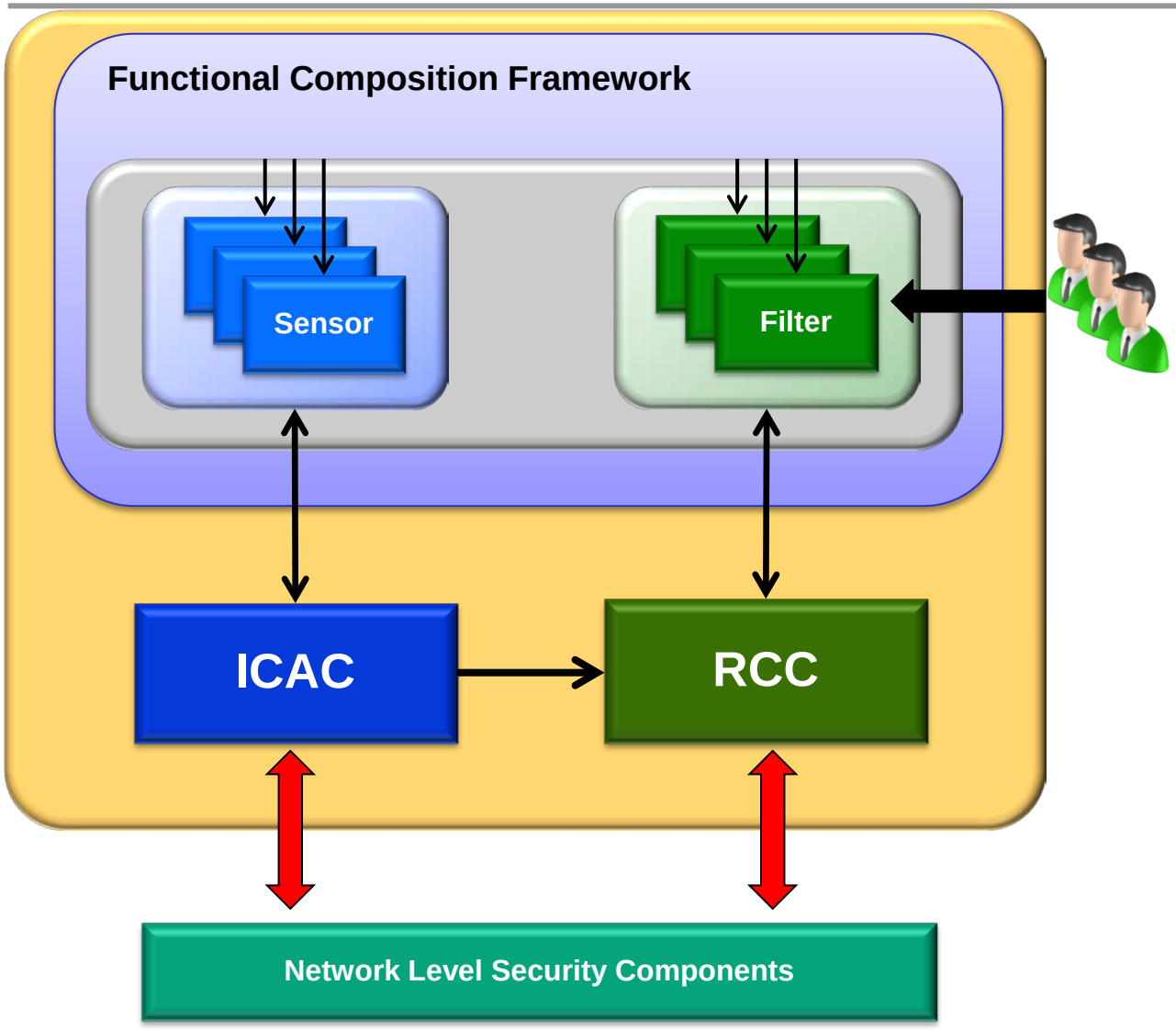
Overview
DEEP Functional Composition (FC) System



Overview
G-Lab DEEP – Key Ideas (Security Focus)



Overview
Protection on the Service Level



Distributed Sensor System (DSS)

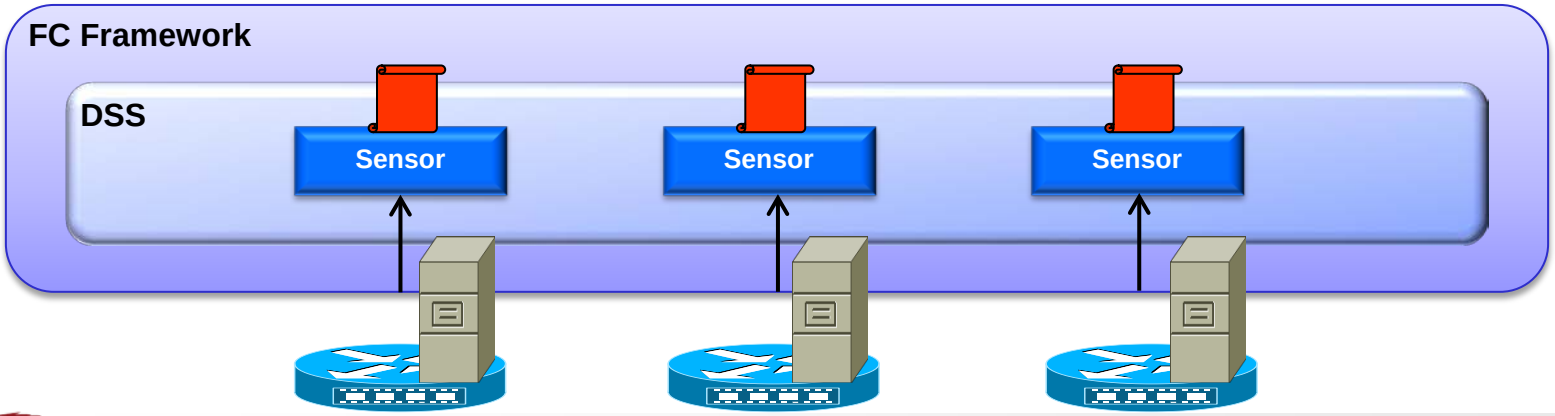
Intrusion Correlation and Aggregation Centre (ICAC)

Distributed SIP Call Filter System (DCFS)

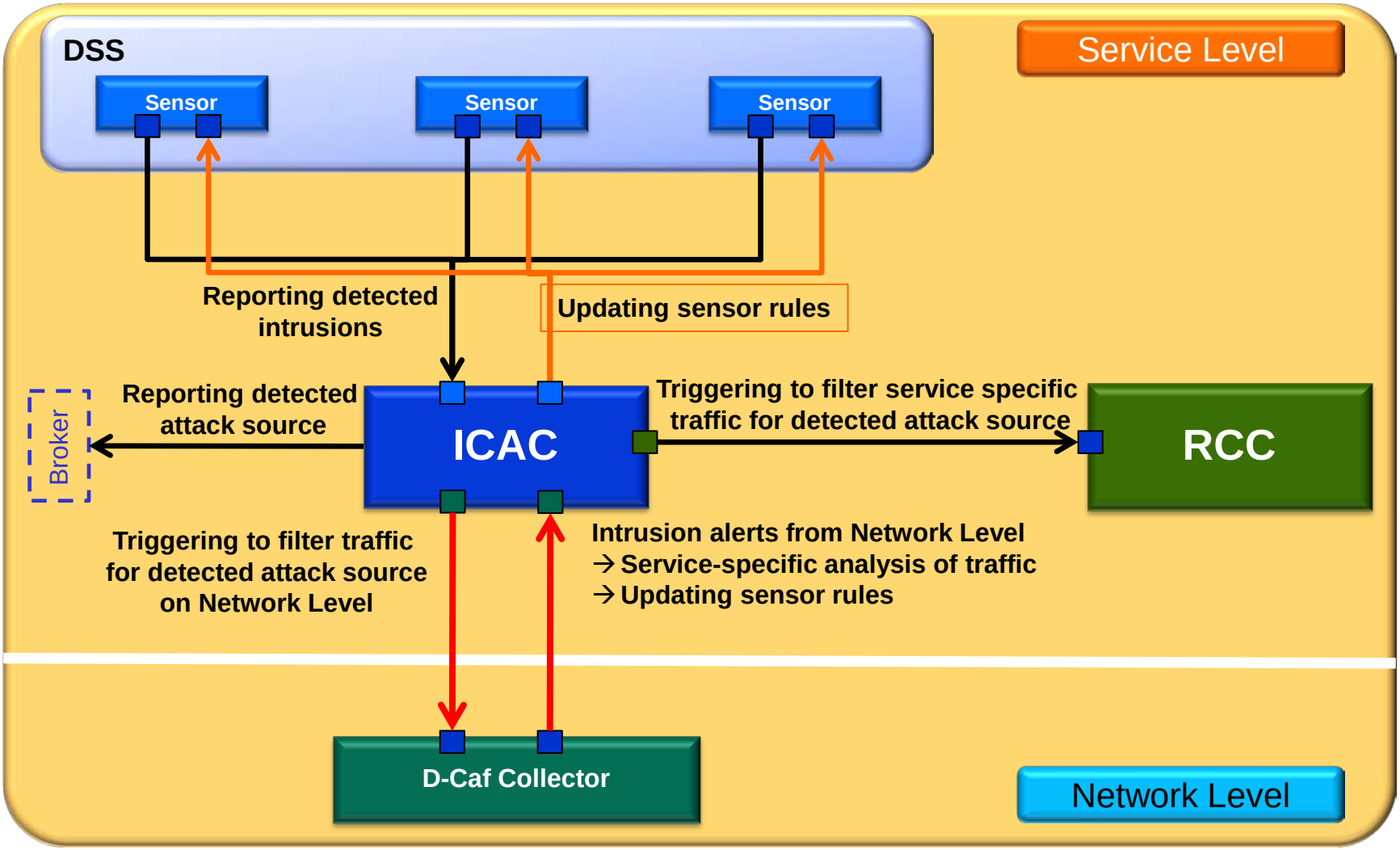
Rating Collector Centre (RCC)

Detection
Distributed Sensor System

- A single sensor acts as a Functional Block
  - Can be activated on demand
  - Via Functional Composition interface
    - Service specific traffic to be monitored
- Sensors operate rule-based
  - Rules based on experience with real attacks
    - E.g. registration hijacking and toll fraud
      - An attacker tries to steal legitimate users credentials and make premium service calls

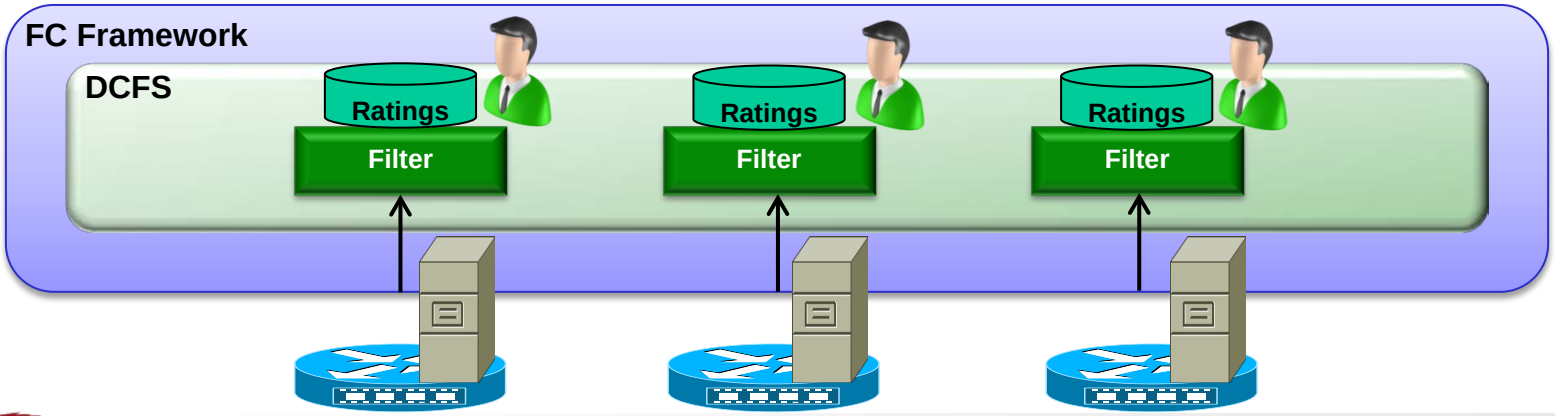


Detection
Intrusion Correlation and Aggregation Centre

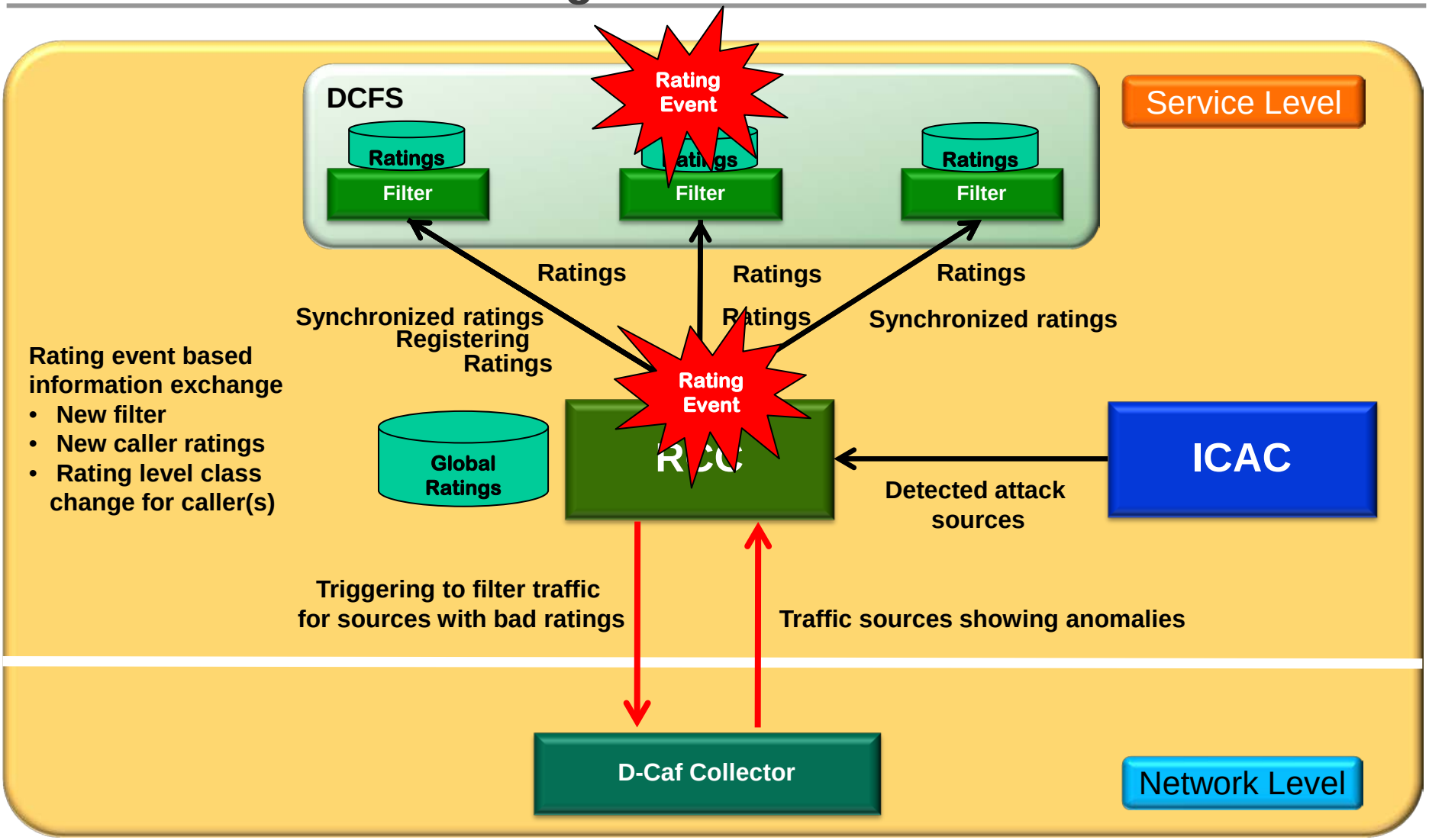


Mitigation
Distributed SIP Call Filter System

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

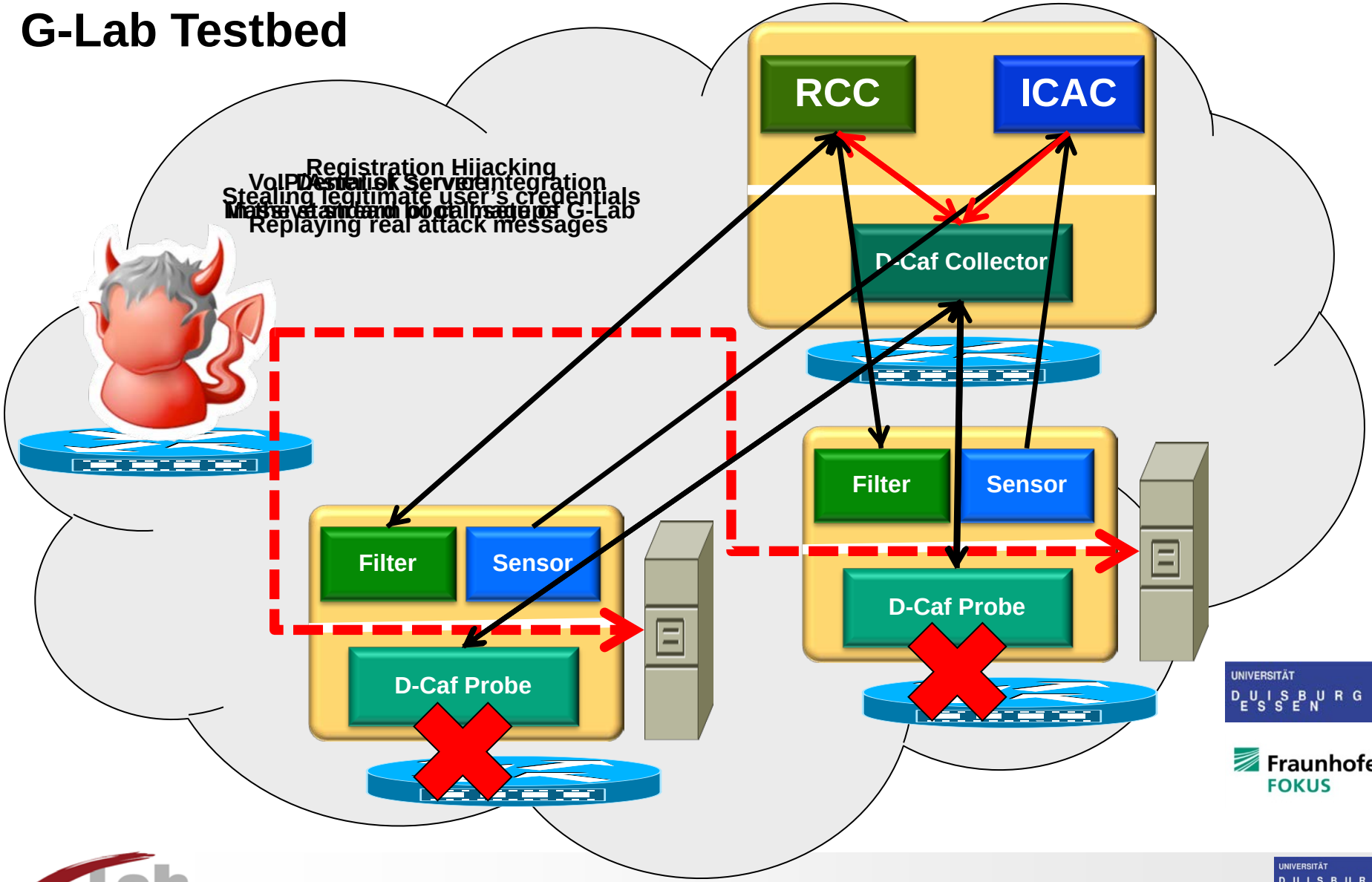


Mitigation
Rating Collector Centre



Experiment Scenario I
Cross-Layer Security

G-Lab Testbed

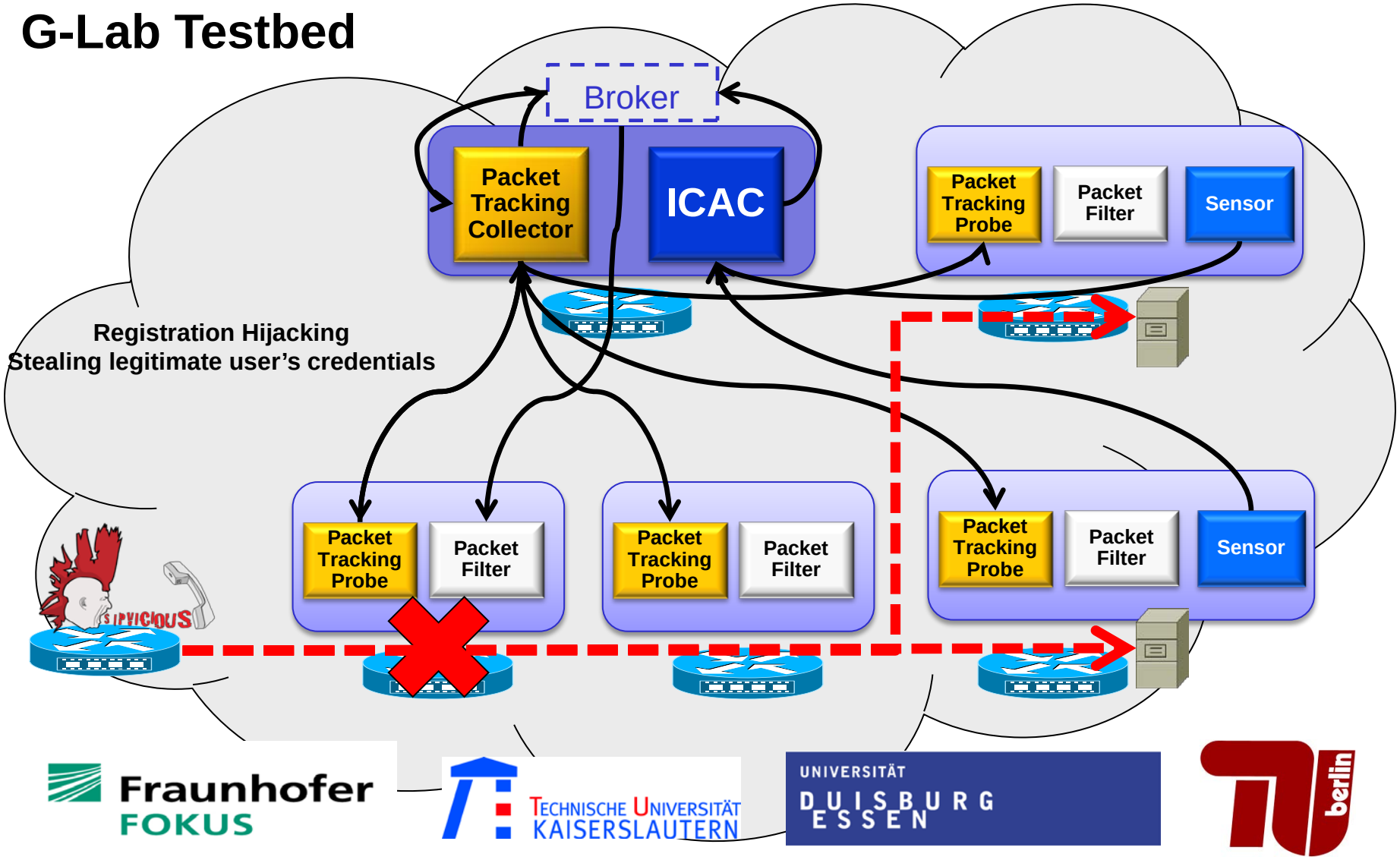


UNIVERSITÄT DUISBURG ESSEN

Fraunhofer FOKUS

Experiment Scenario II
Functional Composable Cross-Layer Security

G-Lab Testbed



Fraunhofer FOKUS

Technische Universität Kaiserslautern

Universität Duisburg Essen

berlin

Conclusion

- VoIP/Asterisk server integration in the standard boot image of G-Lab
  - Benefit from G-Lab flexibility
- Using tools provided G-Lab, e.g. ToMaTo
  - Efficiently setting up experiment scenarios
- Feasibility of Cross-Layer Security 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

Thanks for your attention

Questions?