UNIVERSITÄT DUISBURG ESSEN

The Future Internet as second chance for security – Challenges and first ideas

Erwin P. Rathgeb
Computer Networking Technology Group
Institute for Experimental Mathematics
University Duisburg-Essen

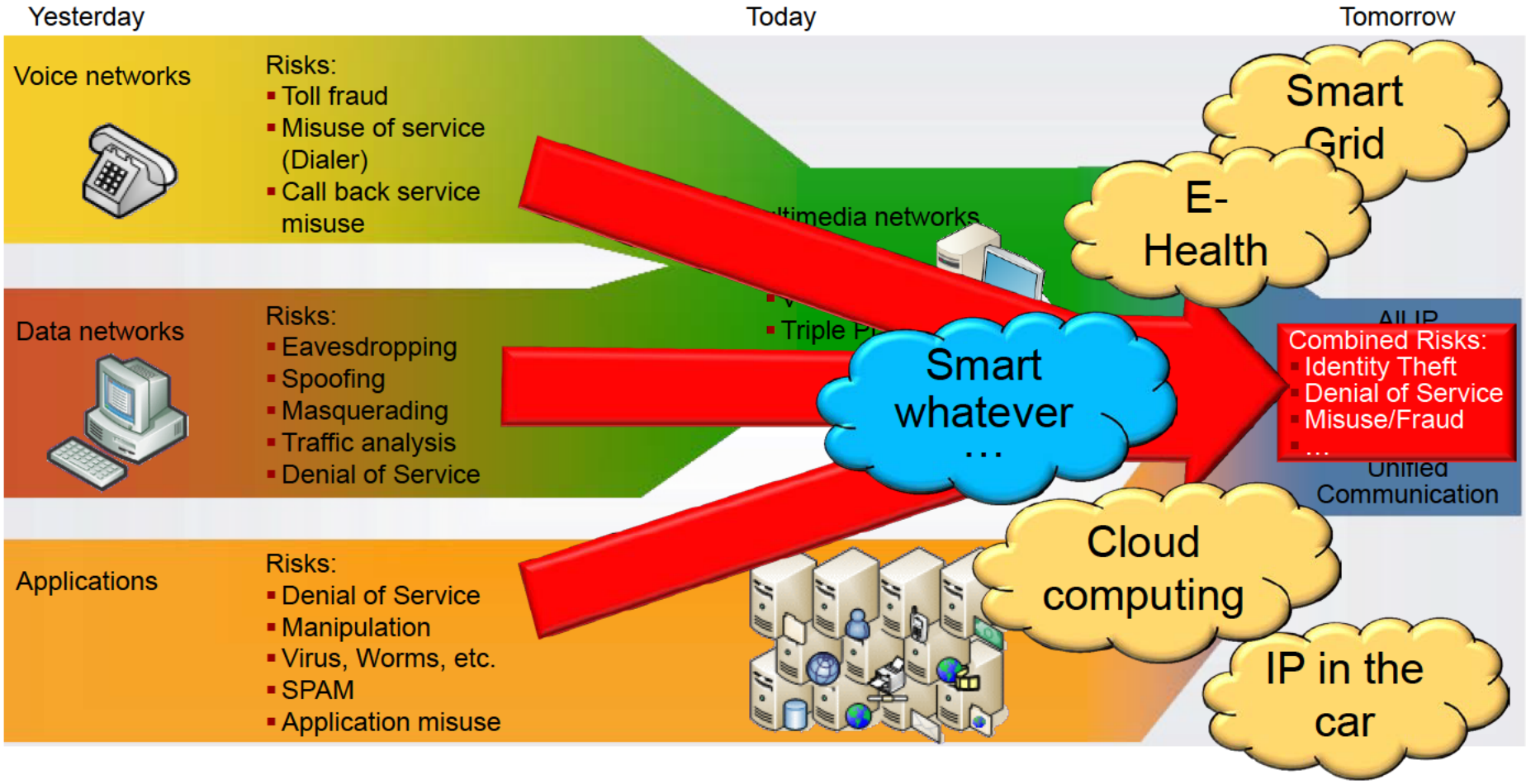
SPONSORED BY THE

Federal Ministry of Education and Research

Overview

- Introduction
  - Convergence of networks ➔ convergence of risks
- Network and service security
  - Some observations and trends
  - Typical example: SIP-based VoIP
- Future Internet as a second chance for security
  - Why do we need a second chance?
  - Why the Future Internet?
- Security activities in the G-Lab context
  - Overview
  - G-Lab DEEP – Cross-Layer detection and mitigation
- Conclusion
  - Major challenges for (Future Internet) security reasearch

Converging networks and services – Convergence of risks



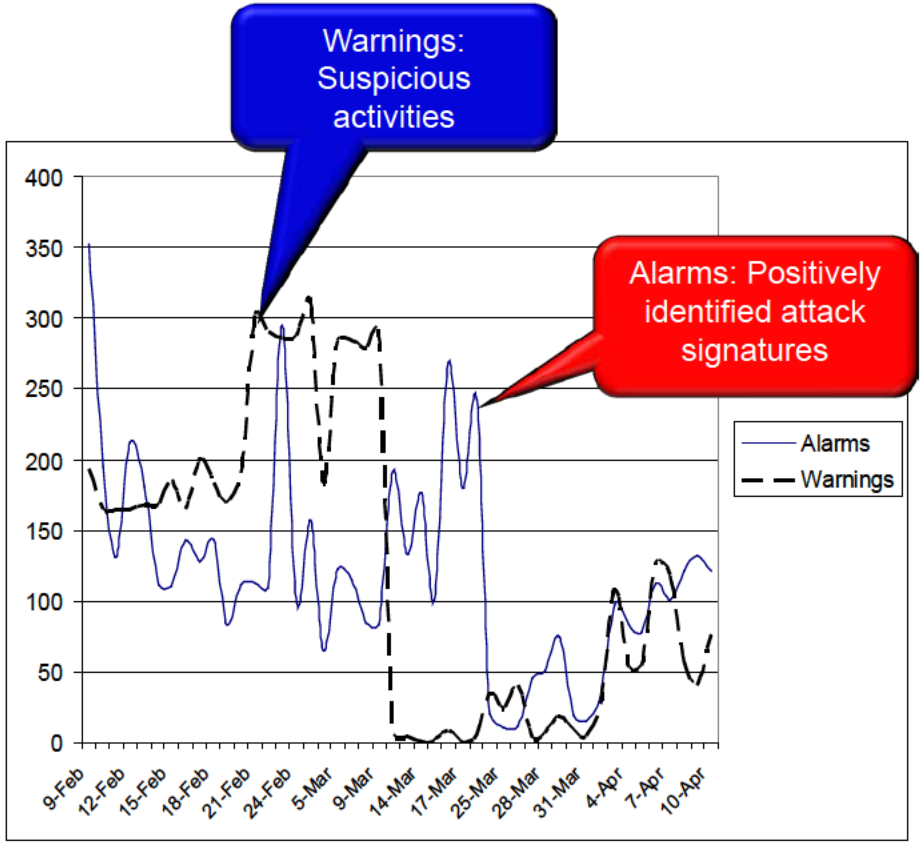
Based on a contribution of Steffen Fries to the ITG Expert Group 5.2.2 "Network Security"

Security in the net – also a matter of architecture

PSTN/ISDN	Strict separation of control and user data	Access difficult
	Specific, complex protocols and interfaces	Manipulation difficult
Cellular	Trust by wire SIM	Attacker trackable
	Functionality mainly in infrastructure nodes	Limited vulnerability
	Few, distinct and well defined services	Limited motivation
TCP/IP	Integration of control and user data	Access simple
	Open, widely used protocols and interfaces	Manipulation simple
NGN	No comprehensive authentication	Anonymous attackers
	Functionality mainly in the end devices	Enormous opportunities
	Universal network, wide variety of services	High motivation
	Converged networks	Alternatives
	Additional, centralized functionality in infrastructure	Vulnerable for DoS
	Services and software from many different sources	Vulnerabilities
Future Internet	????	????

State of Internet security 2004 – Malware

- Field study 2003-2005
  - Dedicated „Honeynet“
- Honeynet was attacked immediately
  - No further actions needed to make Honeynet known
- Further observations
  - Nearly 100% automated attacks
  - Dominating OS was main target
  - Attack types and frequencies are external factors

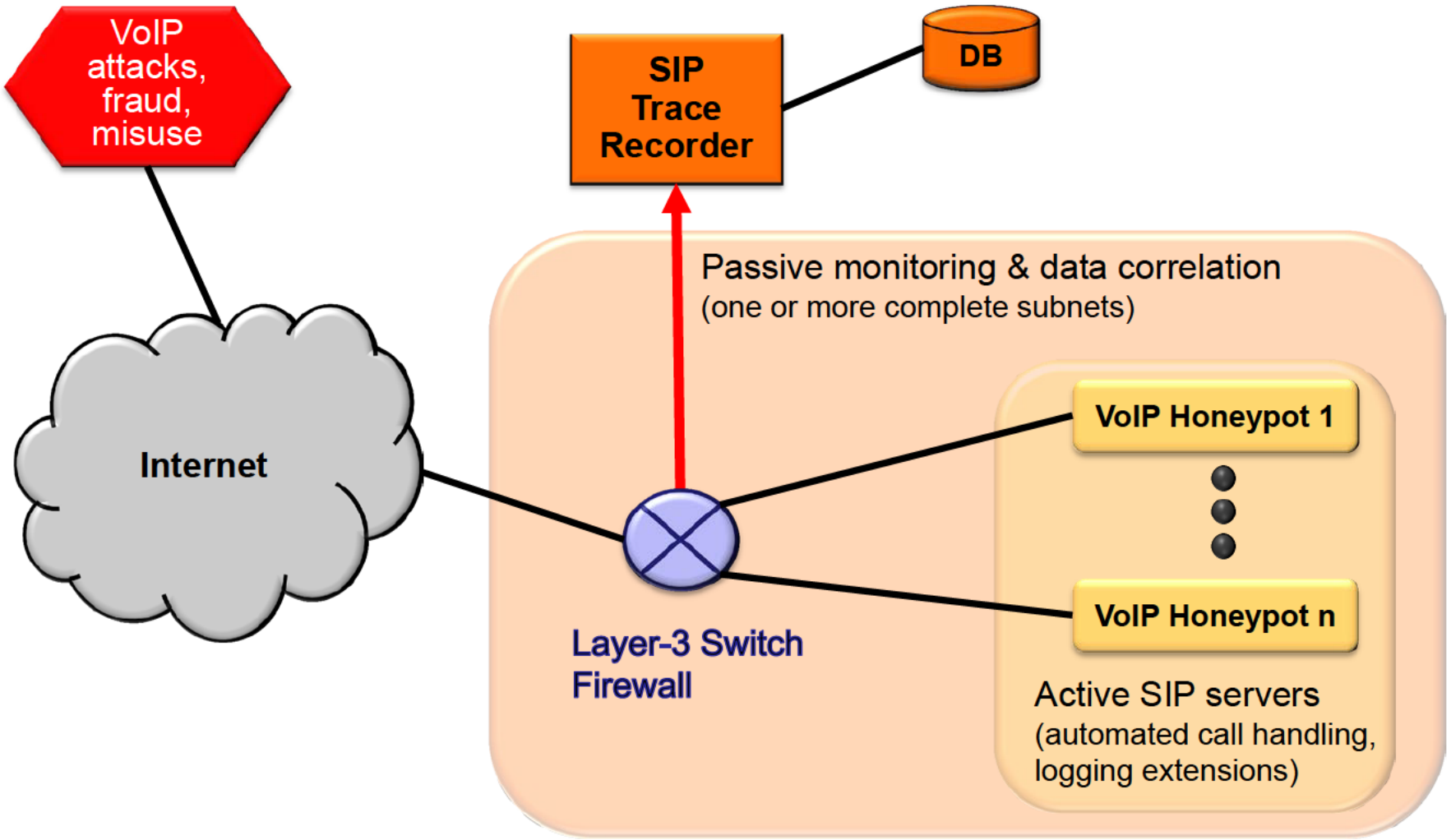


Riebach, S.; Rathgeb, E.P.; Toedtmann, B.:
Efficient Deployment of Honeynets for Statistical and Forensic Analysis of Attacks from the Internet.
In: Proceedings of "IFIP NETWORKING 2005“, Waterloo Ontario, Canada (2005)

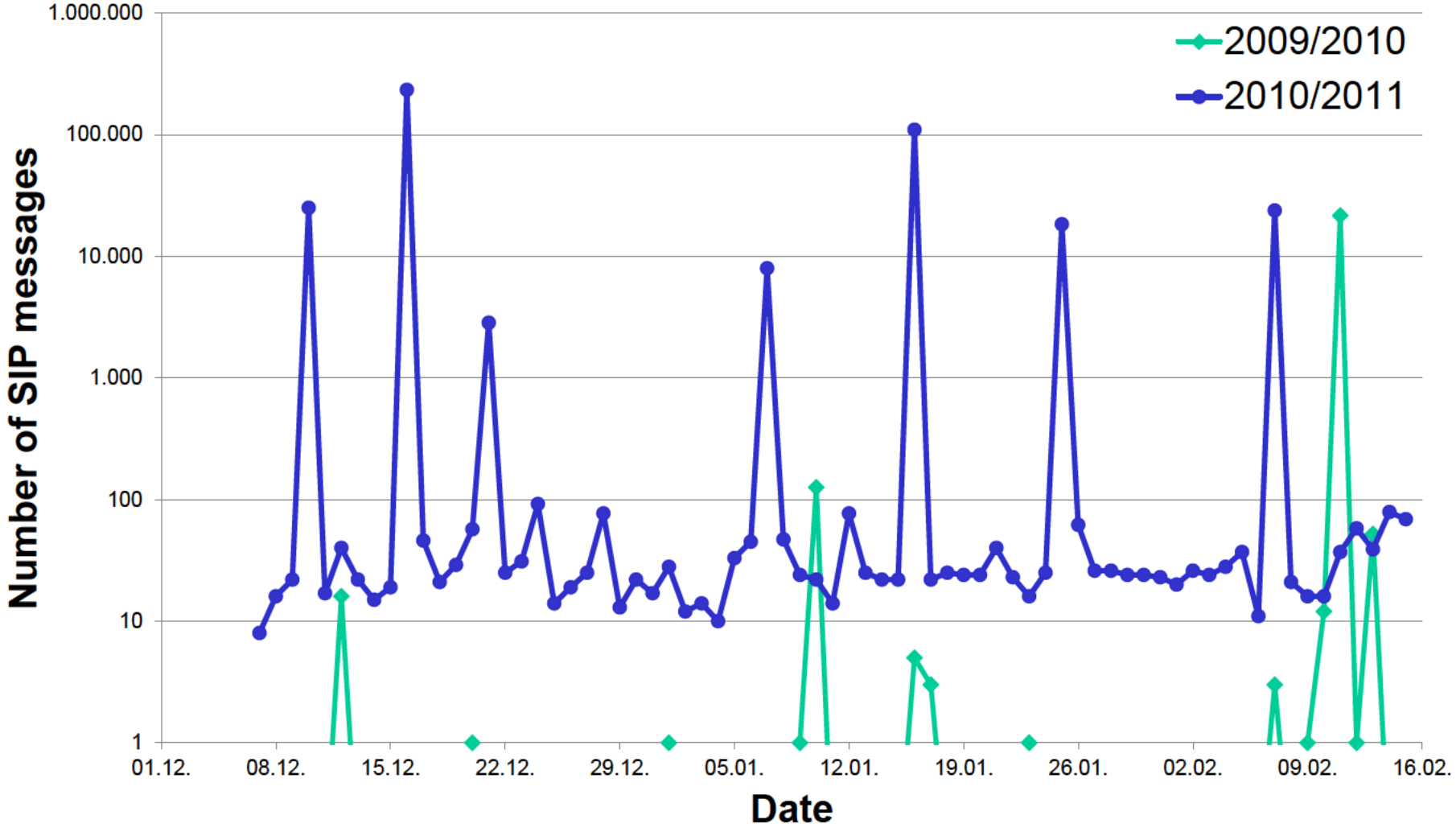
Attacks and misuse schemes – Some observations

- Every new technology is exploited
  - Voicemail systems (1990)
    - Got hacked to get e.g. credit card information
    - Were used to distribute messages with explicit content
  - Malware
    - PCs ➔ Smartphones ➔ Game consoles (first reports) ➔ ???
- Successful attack patterns are adapted and reused
  - SPAM/Phishing
    - Paper mail ➔E-Mail ➔SMS ➔ VoIP (SPIT)
- Each service/application provides specific attack/misuse opportunities
  - Example Voice over IP
    - Registration Hijacking and Toll Fraud

VoIP Fraud & Misuse Detection System – Basic setup



VoIP Fraud & Misuse Detection System results – Attack intensitiy is increasing significantly



VoIP Honeynet project – Registration Hijacking & Toll Fraud examples

Registration Hijacking

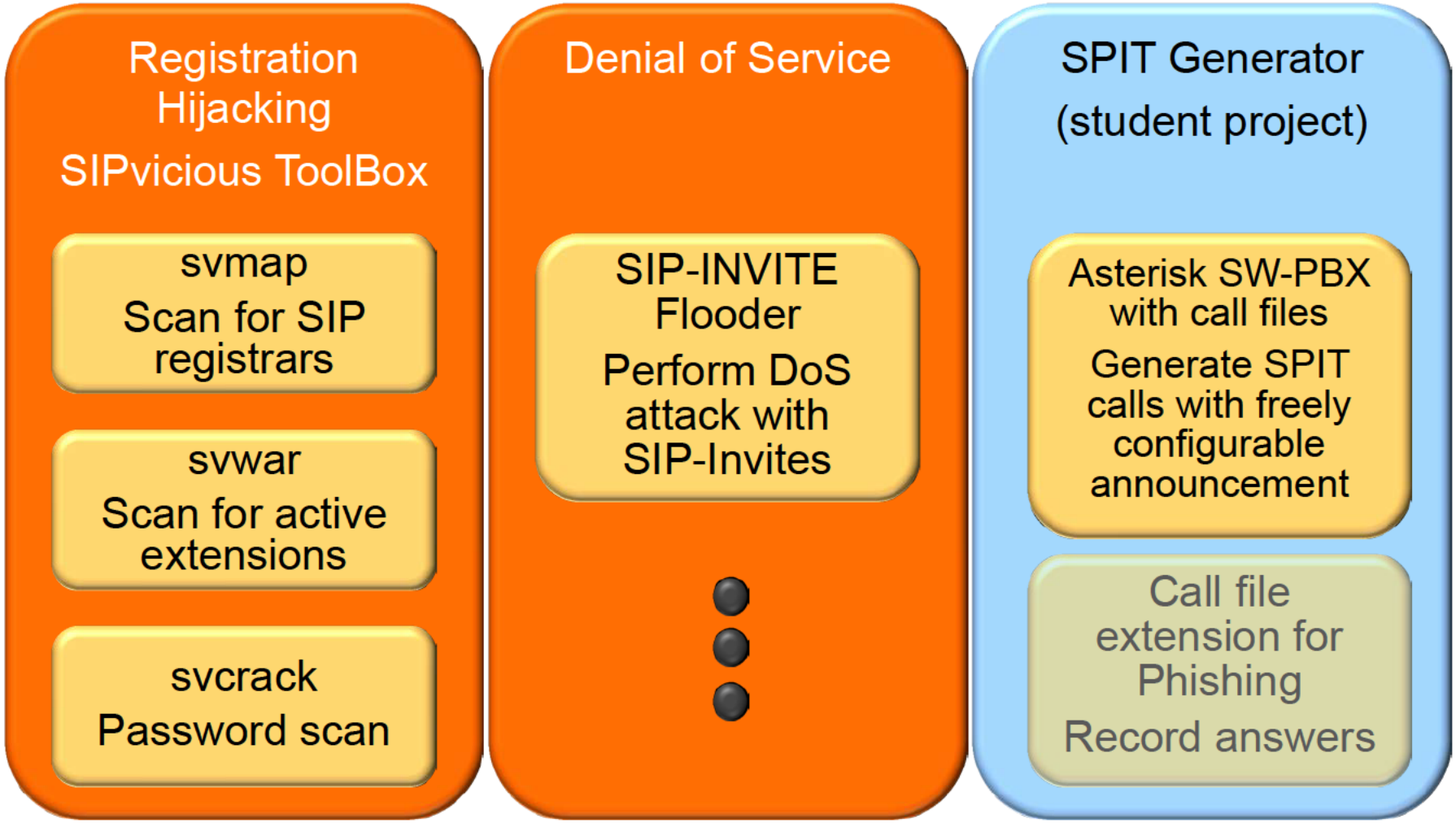
[Feb 11 19:58:37] NOTICE[3062] chan_sip.c: Registration from '"768"<sip:768@132.252.152.211>' failed for '77.48.88.60
[Feb 11 19:58:37] NOTICE[3062] chan_sip.c: Registration from '"769"<sip:769@132.252.152.211>' failed for '77.48.88.60'
[Feb 11 19:58:37] NOTICE[3062] chan_sip.c: Registration from '"770"<sip:770@132.252.152.211>' failed for '77.48.88.60
[Feb 11 19:58:37] NOTICE[3062] chan_sip.c: Registration from '"771"<sip:771@132.252.152.211>' failed for '77.48.88.60
[Feb 11 19:58:38] NOTICE[3062] chan_sip.c: Registration from '"772"<sip:772@132.252.152.211>' failed for '77.48.88.60
[Feb 11 19:58:38] NOTICE[3062] chan_sip.c: Registration from '"773"<sip:773@132.252.152.211>' failed for '77.48.88.60
[Feb 11 19:58:38] NOTICE[3062] chan_sip.c: Registration from '"774"<sip:774@132.252.152.211>' failed for '77.48.88.60'
[Feb 11 19:58:38] NOTICE[3062] chan_sip.c: Registration from '"775"<sip:775@132.252.152.211>' failed for '77.48.88.60

Toll Fraud

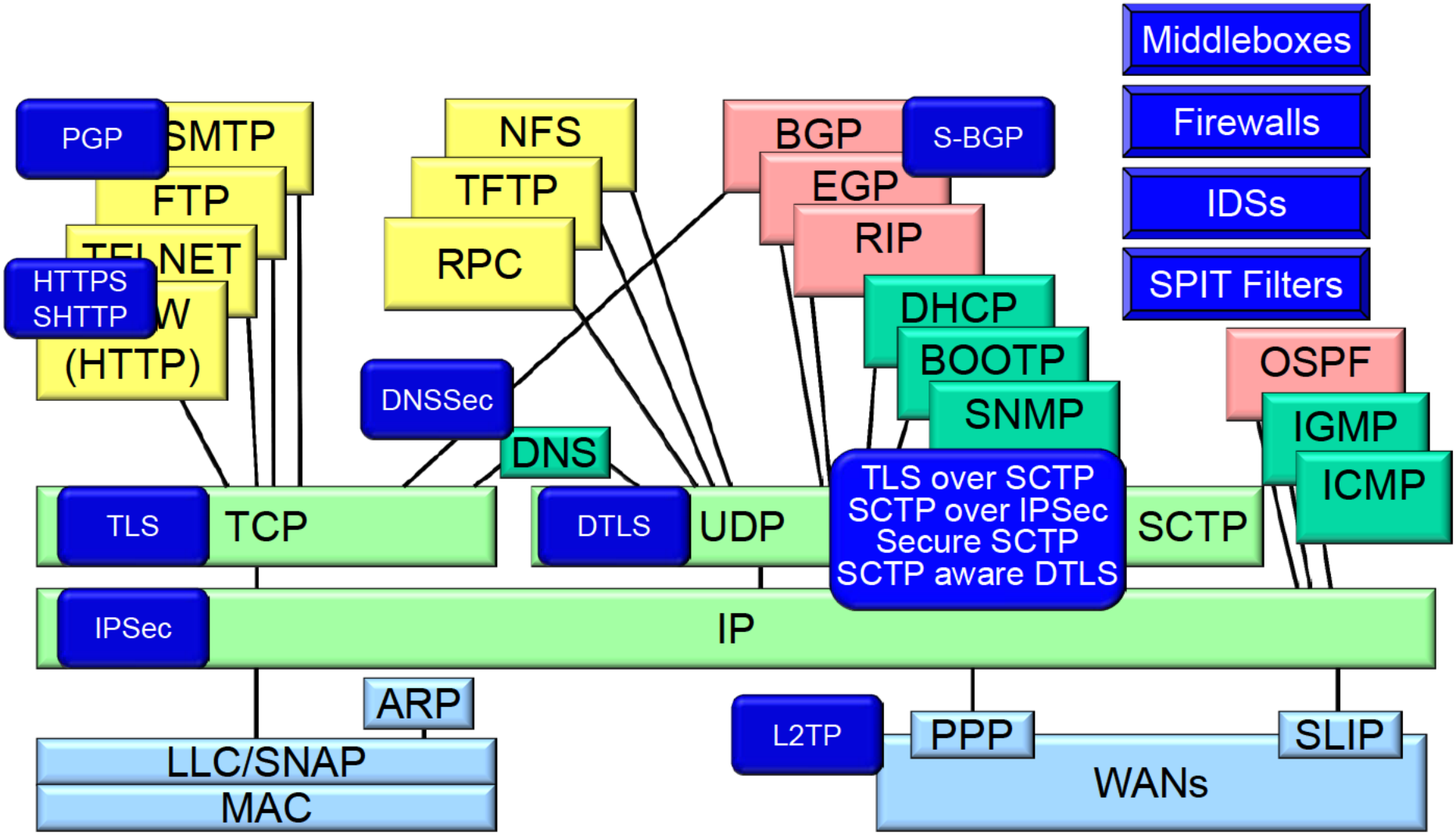
+ Sat Feb 13 02:21:45 117.41.229.31 call to: 90441383417547 von sip, UserAgent: Asterisk PBX, URI: sip:sip@117.41.229.31
+ Sat Feb 13 02:21:55 117.41.229.31 call to: 0441206751586 von sip, UserAgent: Asterisk PBX, URI: sip:sip@117.41.229.31
+ Sat Feb 13 02:21:56 117.41.229.31 call to: 9011441763837000 von sip, UserAgent: Asterisk PBX, URI: sip:sip@117.41.229.31
+ Sat Feb 13 02:21:57 117.41.229.31 call to: 000447850019298 von sip, UserAgent: Asterisk PBX, URI: sip:sip@117.41.229.31
+ Sat Feb 13 02:21:58 117.41.229.31 call to: 1447768993716 von sip, UserAgent: Asterisk PBX, URI: sip:sip@117.41.229.31
+ Sat Feb 13 02:21:59 117.41.229.31 call to: 90441383417547 von sip, UserAgent: Asterisk PBX, URI: sip:sip@117.41.229.31
+ Sat Feb 13 02:22:09 117.41.229.31 call to: 0441206751586 von sip, UserAgent: Asterisk PBX, URI: sip:sip@117.41.229.31
+ Sat Feb 13 02:22:10 117.41.229.31 call to: 0011442075964032 von sip, UserAgent: Asterisk PBX, URI: sip:sip@117.41.229.31
+ Sat Feb 13 02:22:13 117.41.229.31 call to: 00000441628481177 von sip, UserAgent: Asterisk PBX, URI: sip:sip@117.41.229.31
+ Sat Feb 13 02:22:13 117.41.229.31 call to: 0001442078493108 von sip, UserAgent: Asterisk PBX, URI: sip:sip@117.41.229.31
+ Sat Feb 13 02:22:14 117.41.229.31 call to: 90441383417547 von sip, UserAgent: Asterisk PBX, URI: sip:sip@117.41.229.31

+ Wed Feb 10 17:25:36 113.105.152.104 call to: 909000331828029 von sip, UserAgent: Asterisk PBX, URI: sip:sip@113.105.152.104
+ Wed Feb 10 18:21:46 113.105.152.104 call to: 0900331828029 von sip, UserAgent: Asterisk PBX, URI: sip:sip@113.105.152.104
+ Wed Feb 10 19:20:36 113.105.152.102 call to: 00090033182802 von sip, UserAgent: Asterisk PBX, URI: sip:sip@113.105.152.102

Automated tools for VoIP attacks – Already available in the Internet

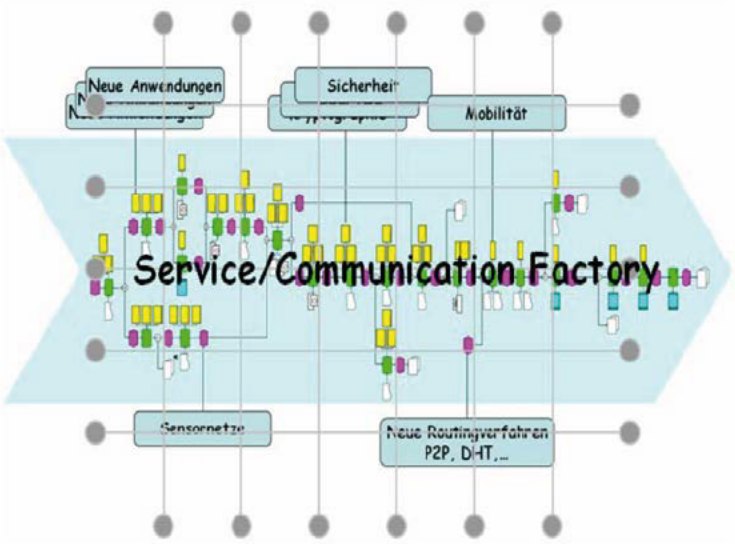


Why do we need a second chance for security?
„Fix it as you go“ approach



The Future Internet – Chance to start all over again?

- Novel addressing and routing concepts
  - Locator/identifer split
  - Multihoming/Multipath
- Network virtualization
  - Multiple coexistent networks
    - optimized
- Service components instead of protocols
  - Service oriented approach
  - Orchestration of services
    - flexible
    - application specific
    - dynamic



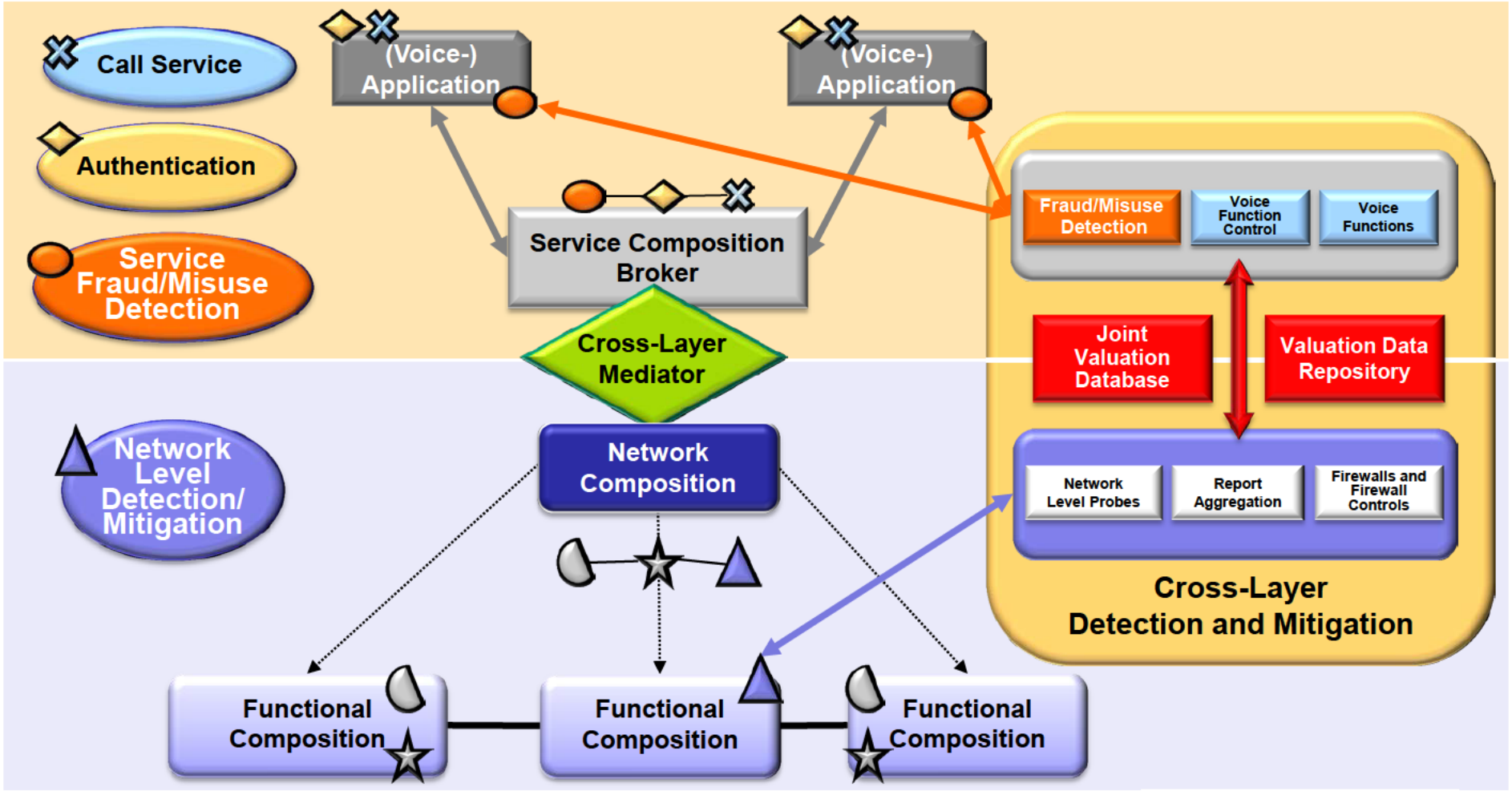
Paul Müller, Bernd Reuther, AG ICSY, University of Kaiserslautern, http://www.icsy.de

- **Security as design goal right from the start**

G-Lab security activities – Overview

- Special Interest Group „Security“
  - Stimulate cooperation among existing projects
  - Identify and discuss challenges and solutions
  - Share tools developed in the projects
- Security topics taken up in G-Lab projects (examples)
  - Security implications of network virtualization
  - Security implications of energy efficient operation of virtual networks
  - Security aspects of overlay networks
  - Cross-layer cooperative attack/misuse detection and mitigation

G-Lab DEEP – Deepening G-Lab for Cross-Layer Composition



Fraunhofer FOKUS

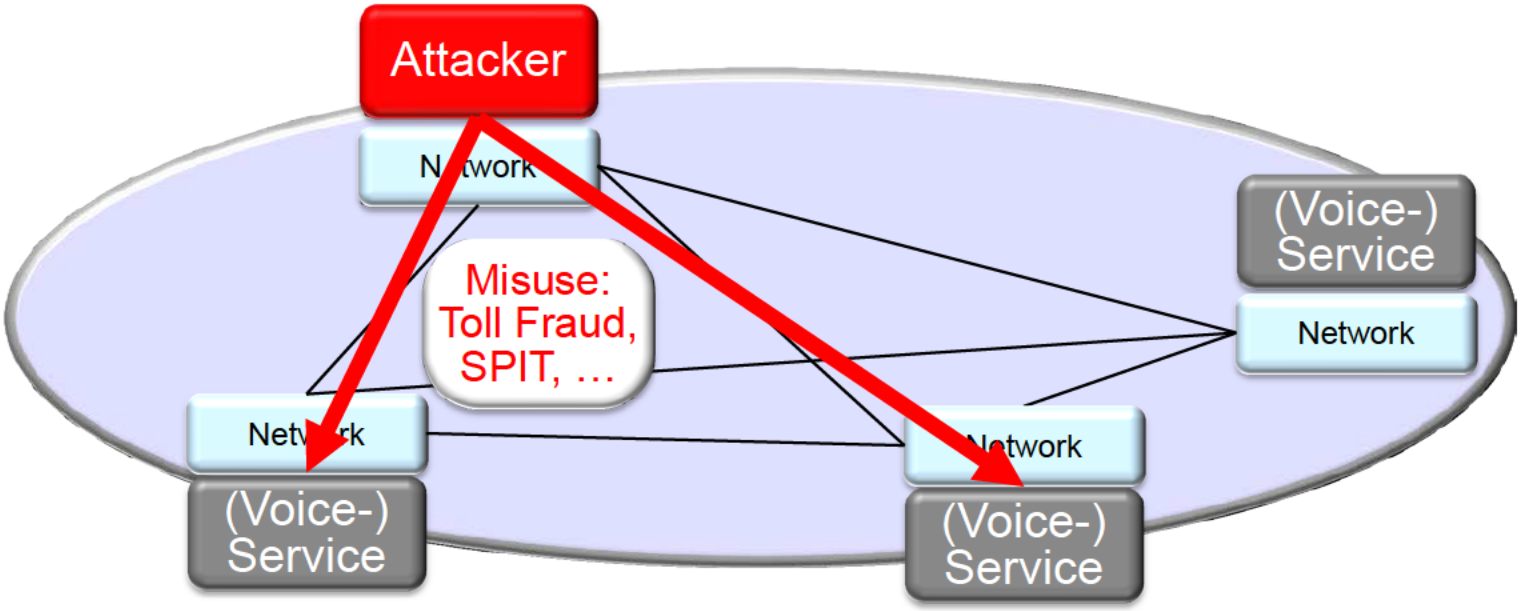
Technische Universität Berlin

Technische Universität Kaiserslautern

Universität Duisburg Essen

G-Lab DEEP

G-Lab DEEP – Cross-Layer Monitoring and Attack Mitigation



Fraunhofer FOKUS

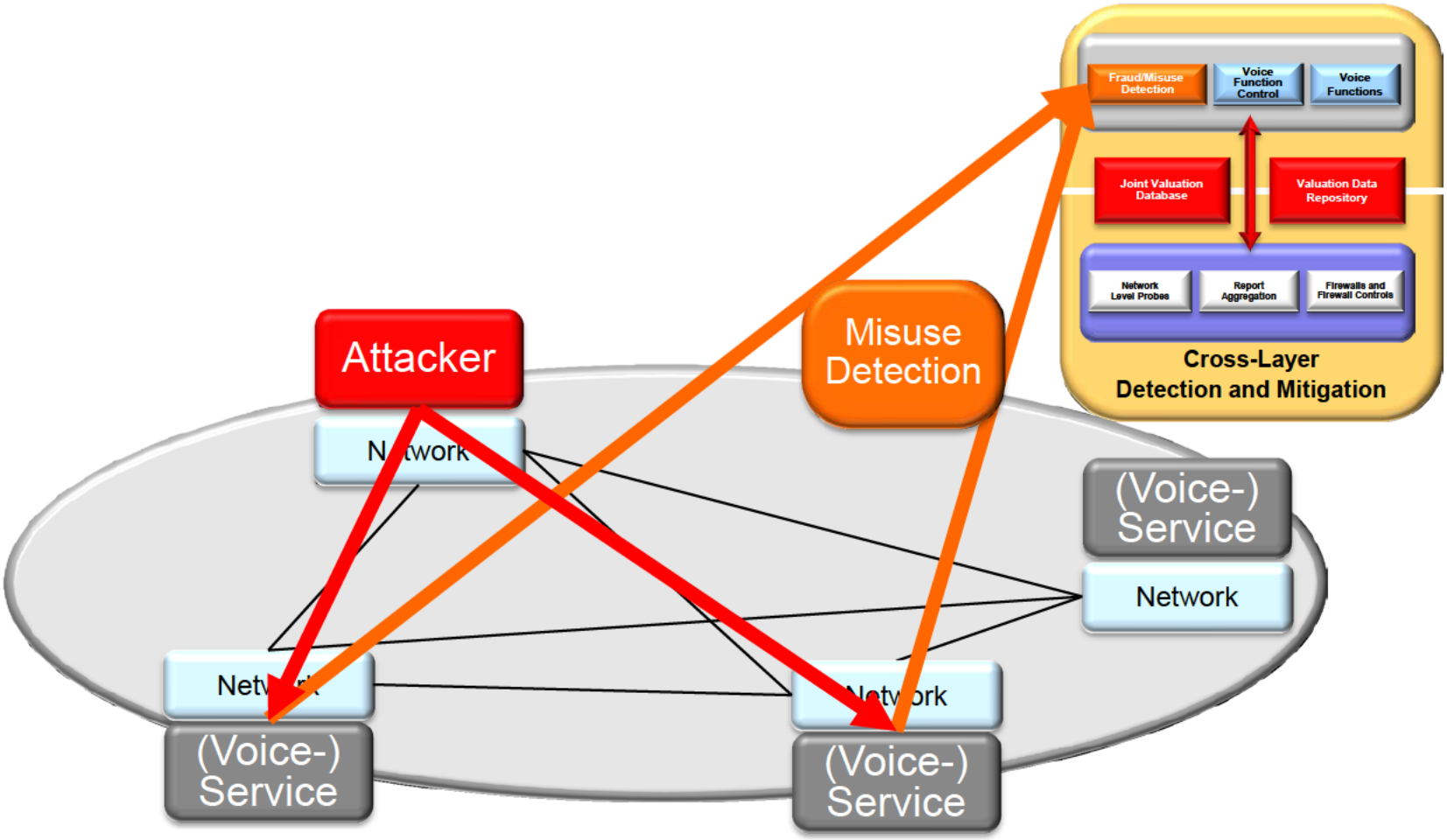
Technische Universität Berlin

Technische Universität Kaiserslautern

Universität Duisburg Essen

G-Lab DEEP

G-Lab DEEP – Cross-Layer Monitoring and Attack Mitigation



Fraunhofer FOKUS

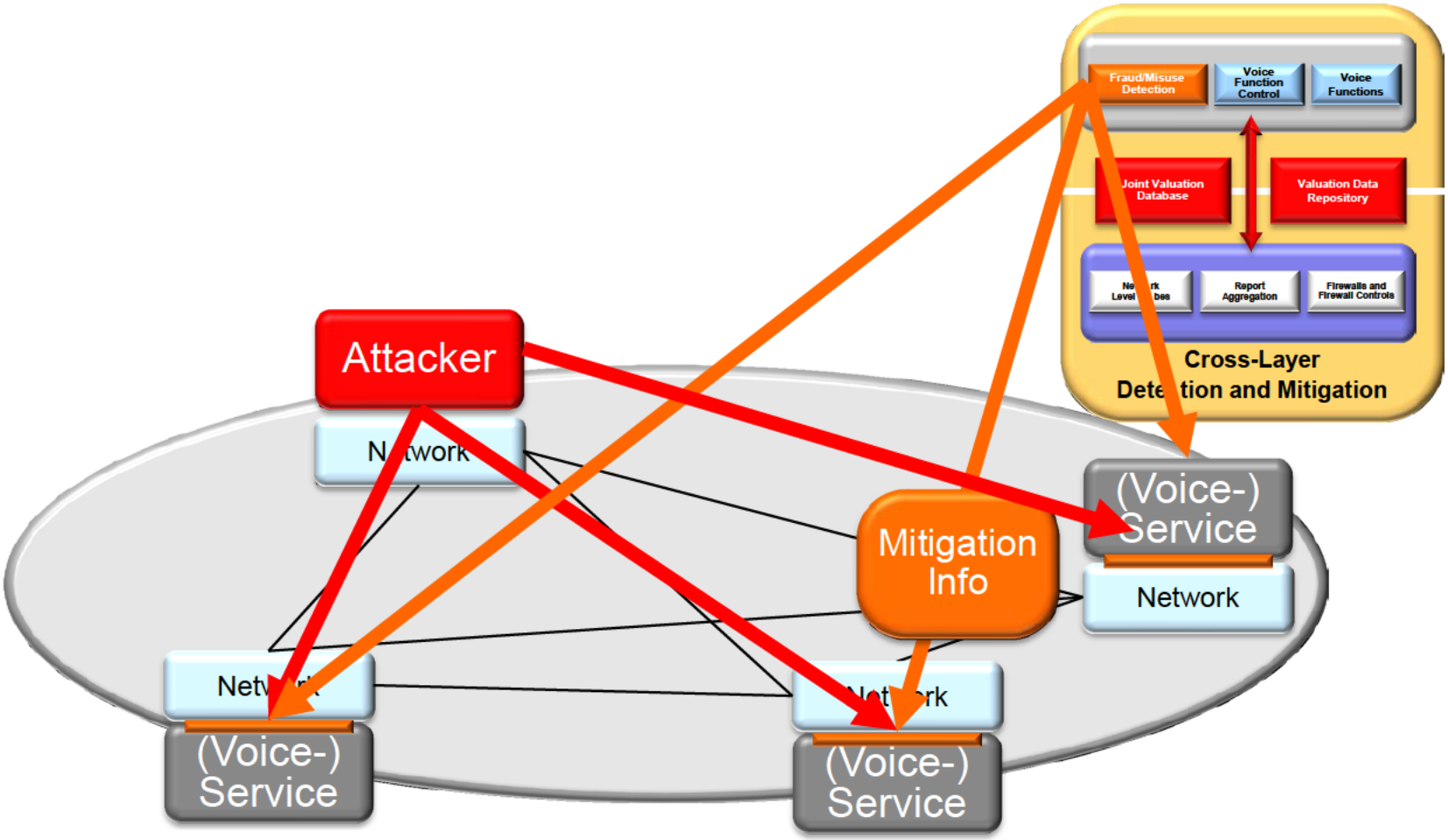
Technische Universität Berlin

Technische Universität Kaiserslautern

Universität Duisburg Essen

G-Lab DEEP

G-Lab DEEP – Cross-Layer Monitoring and Attack Mitigation



Fraunhofer FOKUS

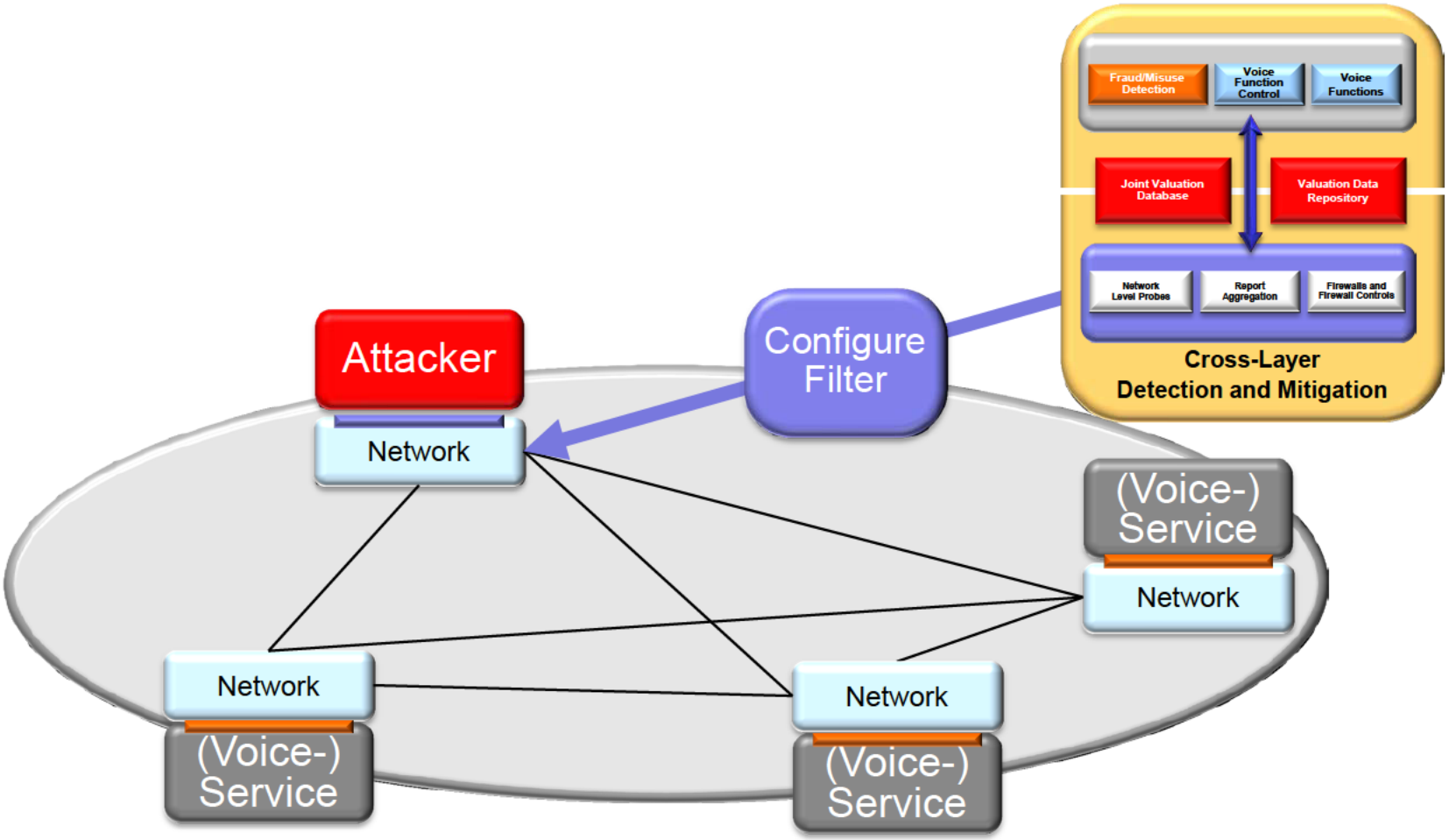
Technische Universität Berlin

Technische Universität Kaiserslautern

Universität Duisburg Essen

G-Lab DEEP

G-Lab DEEP – Cross-Layer Monitoring and Attack Mitigation



Fraunhofer FOKUS

Technische Universität Berlin

Technische Universität Kaiserslautern

Universität Duisburg Essen

G-Lab DEEP

Network and service security – Major issues and challenges

Strong authentication and encryption –
Applicability and limitations in dynamic, open environments

Authentication versus trust –
Tradeoff between control and anonymity/privacy

Generic and service specific misuse and attack patterns –
Proactive approach to detection and mitigation

DoS is different from other threats (and very popular) –
No acceptable solution concepts known yet

Distibuted, cross-layer security functions –
Definition of function split and cooperation algorithms

New paradigms, architectures and functions –
Assessment and mitigation of vulnerability/misuse potential