G-LAB DEEP Security

SPONSORED BY THE

Federal Ministry of Education and Research

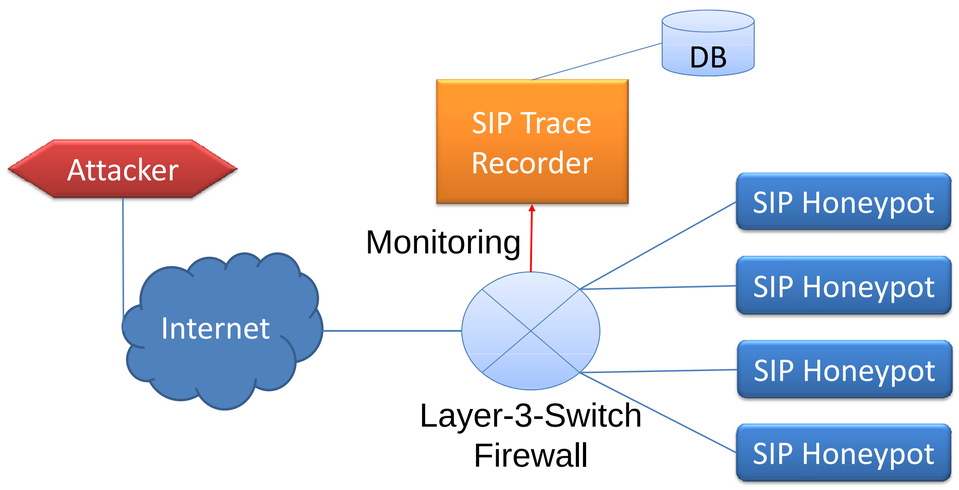
New technologies are always are always exploited for new attacks

Attacks occur on different layers e.g. service layer, network layer

Attack patterns are adapted, e.g. SPAM: Snail Mail/Email/SMS/SPIT

Different attack opportunities for each service/application

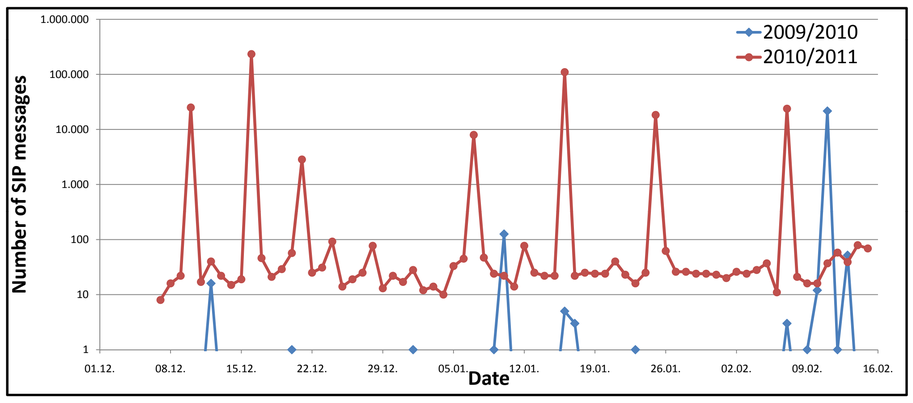
Current situation: SIP VoIP example



Drawbacks

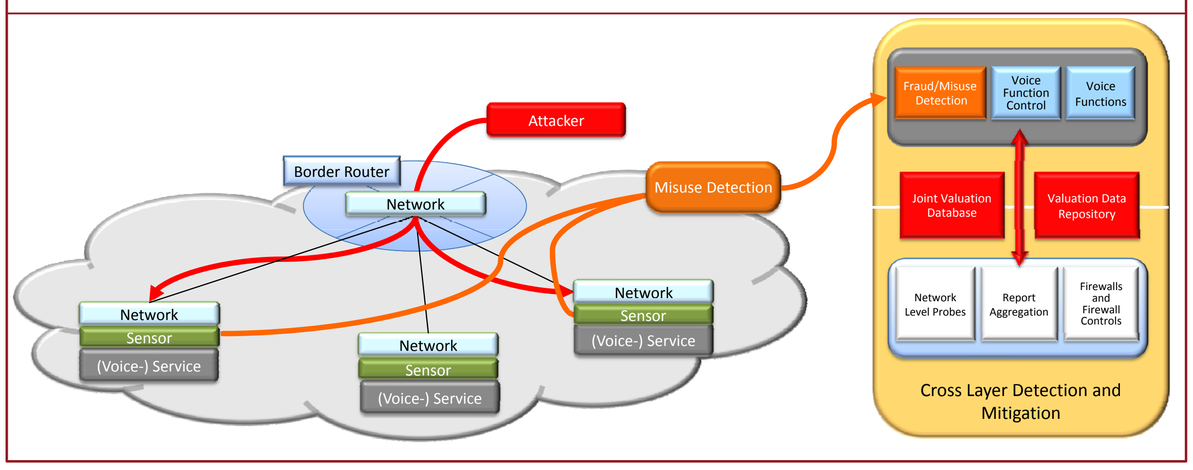
- No real-time reaction
- Limited view
- Only single layer

Systematic SIP attacks already existing, intensity is increasing significantly

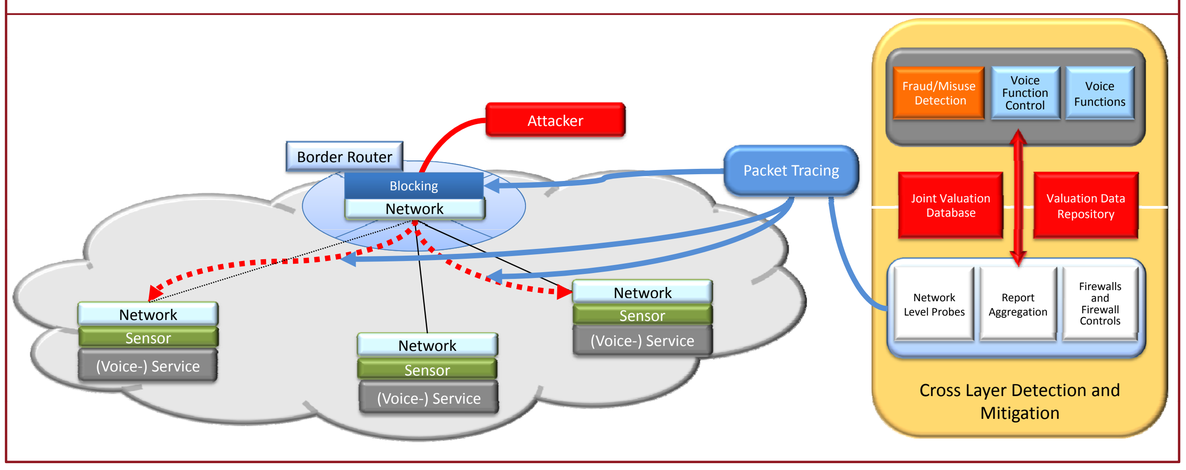


GLAB DEEP: Cross-layer distributed detection & mitigation

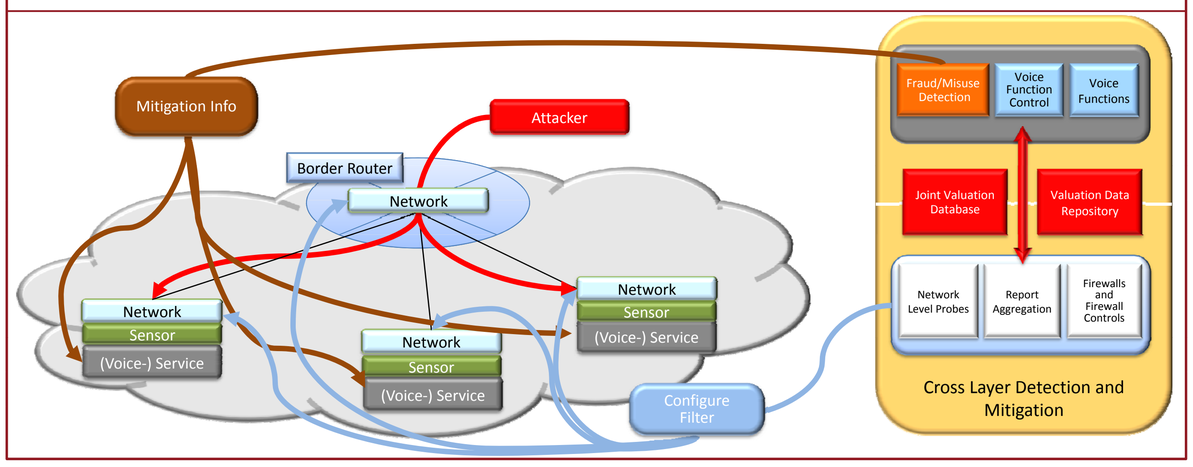
Detection view



Blocking view



Mitigation view



- Attacker tracing to border router
- Real-time adaption due cross layer composition
- Distributed detection & mitigation
- Cross layer communication

Challenges for Future Internet security research

- Benefit from new architectures without introducing new vulnerabilities, e.g. service oriented approach/functional composition
- Algorithms for real-time, distributed, cross-layer cooperation
- 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