

# G-Lab Deep: Cross-layer Composition and Security for a flexible Future Internet

Tanja Zseby<sup>1</sup>, Carsten Schmoll<sup>1</sup>, Christian Henke<sup>2</sup>, Dirk Hoffstadt<sup>3</sup>,  
Abbas Ali Siddiqui<sup>4</sup>

<sup>1</sup> Fraunhofer FOKUS Network Research Group  
Kaiserin-Augusta-Allee 31, 10589 Berlin  
{tanja.zseby | carsten.schmoll}@fokus.fraunhofer.de

<sup>2</sup> Technical University Berlin Next-Generation Networks  
Straße des 17. Juni 135, 10623 Berlin  
c.henke@tu-berlin.de

<sup>3</sup> University of Duisburg-Essen, Computer Networking Technology Group  
Ellernstr. 29, 45326 Essen  
dirk.hoffstadt@iem.uni-due.de

<sup>4</sup> University of Kaiserslautern, Integrated Communications Systems Group  
Erwin-Schrödinger-Straße, 67663 Kaiserslautern  
siddiqui@informatik.uni-kl.de

**Abstract.** The Internet enables the way how global businesses and communities communicate today. In the last years, however, new demands have collided with old designs, resulting in a complex agglomerate of protocols and patches. These makeshift solutions are hard to manage, protect, and extend.

The G-Lab DEEP project tries to address these challenges of the Future Internet with an innovative composition approach of network and application level services with a special emphasis on security. One of the main project goals is the dynamically controlled mediation of the requirements of the application layer which results in requirements for the service as well as the network layer. The mediation's goal is to select suitable network function modules and their autonomic combination to support the application's demands. In the application layer as well as on the network layer the same derived questions and problems arise, for example the semantics, description, the management, discovering and the composition of services.

In the G-Lab DEEP work an architecture and framework will be developed and setup in the form of a prototype where applications can state requirements to services and the network, and our solution will combine functional modules to support the desired functionalities. If no requirements are given explicitly by the applications then policies in the network will provide the requirements for a given application.

In our demos the network will be stressed in different scenarios, mostly voice/telephony centered, with background traffic plus emergency calls and/or unsolicited voice calls. Based on cross-layer monitoring and composition policies the network will detect the disturbances, and be secured while still ensuring the reliability of the emergency call(s) using active mitigation strategies which are selected based on the monitoring results.

**Keywords:** Security, Functional Composition, Cross-Layer, Future Internet, Service Composition.

## 1 G-Lab Deep Project Description

In the current IP network design, applications and networks are inherently independent. Based on the separation of layers in the current network architecture applications are not able to instruct the network how to handle the applications' traffic (e.g. cannot request QoS or custom routing). The network only offers best-effort packet transport to the overlying applications. Additionally there is no standard way to tell applications the state of the network, so that applications could react and read the network status. Therefore one goal of a future Internet infrastructure is to support specific demands of applications plus the ability to inform them about the network status. The current paradigm has its roots in the layered OSI model of networking; however this paradigm is partially broken up by some cross-layer techniques and a kludge of ad hoc solutions.

Besides incremental solutions for a future Internet new networking paradigms have been considered that follow a "clean slate" approach, i.e. disruptive technologies that develop the future Internet from scratch. One of these approaches is functional composition, which decomposes the network stack in functional building blocks and reorganizes the functionalities in a compositional framework. Functional composition focuses on the flexibility of the network and therefore targets two improvements to the current Internet

- 1) Ease of management and integration of new functionality
- 2) Application specific network composition and adaptation based on application requirements instead of using "one-size-fits-all" TCP/IP best effort service

The G-Lab DEEP project takes on the challenges of the current architecture with a modularized functional composition approach that 1) passes application specific requirements to the network layer and 2) uses a cross layer composition technique to allow composition of independent service and network functional blocks in one integrated framework based on the requirements and the network status. A modular solution with loose coupling is desirable to (a) achieve a clean separation of the needed functional blocks without strong entanglement of message passing functionalities, and (b) allow loose binding of functional blocks which are needed for a specific service or application request. Further this breaking down into atomic functional blocks allows for the most flexible combination of functions. This is desirable as each combination of services on the application level may require a different combination of network modules to support it.

This concept can be visualized well using the example of voice communication in the Internet. The role of voice communication in the future Internet will grow, especially with mobile voice applications, while in parallel new functions are developed and new application requirements, many of them security-related, are evolving.

Consider for example the situation of an emergency call via a mobile voice terminal. Based on the specific user intent to make an emergency call a workflow of services within the service and network layer must be triggered which together form the emergency call. This workflow may invoke auxiliary services like “get location”, “make a call” and “reserve line” to support the nature of the emergency call. Maybe even a voice recording should be added automatically. Such auxiliary or partial services can be provided by service-enablers within the provider network.

While the emergency call is established functional blocks are invoked, but these must also react on requirements specific to this invocation (e.g. prioritisation). Therefore the services as well as the network connecting them must treat the call accordingly. Within next generation networks (NGN) such requirements can be passed along as policies. On the network layer we want to supply such features by functional composition of network blocks.

To secure a reliable provisioning of all of these network and service components, a management solution spanning those layers is needed, which must also include service monitoring as an integral part. This requires having the monitoring itself available on the service and on the network layer, with configuration and data export using standardized interfaces. The overall solution shall also work in an inter-domain environment. Monitoring can then be effectively used to detect anomalies and to trigger corresponding actions based on policies.

Through the introduction of a cross-layer monitoring system the network status is continuously monitored and made available to other network and application services. Based on this cross-layer monitoring service the composition engine becomes situation aware and can autonomically and automatically compose services based on the network status. In the current IP world network attacks have become a tremendous threat. Besides threats to network elements and end-hosts (e.g. through virus and worms) there also emerged new threats with the development of new applications and services. For example voice over IP has been exploited by adversaries for anonymous mass voice calls for commercial purposes (SPIT) and for passing the bill to other users or companies (toll fraud). Therefore the cross-layer composition and monitoring system needs to incorporate these experiences from the current Internet and address these challenges for future application to enable suitable detection and counter-measures in a secure way.