Addressing Security in a Cross-Layer Composition Architecture

Martin Becke*, Konrad Campowsky†, Christian Henke†, Dirk Hoffstadt *, Julius Müller †,
Carsten Schmoll ‡, Abbas Ali Siddiqui §, Thomas Magedanz †, Paul Müller §, Erwin Rathgeb * and Tanja Zseby ‡
*Universitt Duisburg - Essen
Ellernstr. 29, D-45326 Essen
Email: martin.becke@uni-due.de, dirk.hoffstadt@iem.uni-due.de, erwin.rathgeb@iem.uni-due.de
†Technical University Berlin
Strae des 17. Juni 135, 10623 Berlin
Email: konrad.campowsky@tu-berlin.de, c.henke@tu-berlin.de, julius.mueller@tu-berlin.de, tm@cs.tu-berlin.de
‡Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Email: carsten.schmoll@fokus.fraunhofer.de, tanja.zseby@fokus.fraunhofer.de
§TU Kaiserslautern
Fachbereich Informatik, Postfach 3049, 67653 Kaiserslautern
siddiqui@informatik.uni-kl.de, pmueller@informatik.uni-kl.de

I. Introduction/Motivation

Clean slate Future Internet approaches are triggered by the realization that there are challenges arising in the current Internet design that may hinder the deployment and development of future applications. New and elevated demands in terms of security, QoS, mobility support, privacy, sustainability and scalability have changed the assumptions of the Internet's early days. The Internet has become complex and ossified, and is proving too inflexible to integrate new functionality. Further cyberspace tussles between users, intellectual property rights, government, over-the top service providers (e.g. youtube) and Internet Service Providers hinder new functionalities to be deployed in the network.

One of these clean state approaches that tries to address the aforementioned challenges is functional composition, which decomposes the network stack in functional building blocks and reorganizes the functionalities in a composition framework. Functional composition architectures can provide solutions for many challenges of the current Internet by 1) customizing the network based on application specific requirements 2) providing means for cross-layer information exchange 3) simplifying the integration of new functionalities through loose coupling of functional blocks 4) ease the management and control through automatic composition and autonomic self-x features 5) enabling network services in the network which can prove a new business model for network providers. Network functional blocks are conceptionally services in a service oriented architecture that can be loosely coupled and composed. Web Services, Next Generation Network Telecommunication Services and Business Process Services follow the same software paradigm but in a different scope. In the project G-Lab DEEP [**?**] we developed an architecture to compose services from both domains by a modularized cross-layer composition approach that uses a mediator to negotiate between applications and the network. In the application layer as well as on the network layer the same questions and problems arise for the composition of functions, for example the semantics, description, the management, discovering and the construction of the optimal function chain for the given conditions. Further we will investigate means to support and secure the service composition by a cross-layer monitoring infrastructure that offers information to the composition engine and can initiate attack mitigation at service and network level. This concept of ad-hoc composition, negotiation and cross-layer monitoring will be demonstrated by the example of voice communication in the Internet. A voice scenario requires a wide spectrum of functional blocks from both layers and it has well-known use cases, with already existing communication and threat challenges. Based on this application scenario we will try to generalize the results for a more broader application domain.

II. Cross-Layer Composition Concept

Todays Internet consists of a dumb network that only offers best-effort packet forwarding for any application. Our functional composition approach offers a network customization based on the application specific requirements and enables the integration of new functionalities also in the core of the network. A functional composition architecture leads to a two-layer architecture - the applications runnings on top at the service layer and the network which is composed based on the application specific requirements. This separation is still valuable because an application designer should not know and

compose the network functional blocks by himself but only state the abstract requirements of the application, e.g. in terms of encryption and QoS (maximum delay, maximum loss). On the service layer a service broker is responsible for composing web services that can be offered by telecommunication or over the top service providers. Each service that requires a network connection will initiate a network customization based on its application specific requirements. A workflow of functional blocks is generated based on the network state and contraints. This workflow is then signaled through the network and executed for the specific flow. In our approach this cross-layer composition is supported by a cross-layer monitor and a mediator. The mediator works as a negotiator between the service and network layer which passes information in both ways and decides in case functionalities are available at both layers (e.g. encryption) where the service should be invoked. This negotiation requires an approach to handle and describe application requirements.

III. Cross-Layer Monitoring

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 autonomously compose services based on the network status. Functional blocks that continuously monitor the congestion of links, availability and cpu load of hosts offer their information to the cross-layer composition engine that can adapt its composition. 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 emerging new threats with the development of new applications and services, e.g. Voice over IP has been exploited by adversaries for anonymous mass voice calls for commercial purposes (SPIT). 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 countermeasures in a secure way. Generic cross-layer monitoring and measurement facilities are provided a management platform that provides a range of active and passive monitoring mechanisms to capture and collect a wide variety of metrics from both the network and the service layer. These metrics either serve as the basis for reactions from the service composition engine based on policies or are made available to other entities of the system.

IV. Security Issues

The architecture of G-Lab DEEP integrates service specific and network based anomaly detection with a user evaluation concept. Service misuse detection modules generate user evaluation reports that are send to a common evaluation aggregator based on a user ID with network based evaluation reports. For example a sip user that successfully logged in and used a premium service will receive a positive valuation whereas a user that has repeatedly falsely identified will get a negative valuation. These aggregate user evaluations serve as an input for the compostion engine and for other functional blocks that resolve congestion by firewalling users with the worst evaluations.

V. Example Scenarios

Two example scenarios shall demonstrate the interaction of the composition, monitoring and security infrastructure. In the most basic case user A initiates a (VoIP) phone call to user B. In this case the service broker composes a call service and an authentication service on the service layer. The call service will have requirements like unreliable transport, maximum delay ¡ x, acceptable loss rate ¡ y. The composition engine has been informed by the cross-layer monitor that the network link to the destination has large losses. The network will be composed based on the network state and the application requirements an unreliable transport functional block will be chosen and composed with an extra FEC block that will make up for the loss on the path or if FEC is not available in the network the mediator can also ask the application to use a more loss tolerant voice codec. In the second scenario we assume that the machine from which User A wants to make an emergency call is infected by some malicious software that generates malicious traffic. Based on the cross-layer monitor the user will get a bad valuation. Knowing that this compromised host generates unwanted and regular traffic the composition framework will now include a deep packet inspection and filtering module in the workflow chain for all traffic from that host to differentiate between normal and malicious traffic. Further the service broker composition will include an authentication service for the emergency call for this compromised host to make sure a legitimate user and not a bot is trying to call the emergency centre.

VI. Resource Federation

Several initiatives and projects worldwide currently investigate federation mechanisms. Among those are several well-known projects from the GENI and FIRE initiatives. A full overview has been published before [**?**]. The work presented here shall contribute to the discussion around heterogeneous resource federation models, strategies, and implementation scenarios. From the authors point of view, overcoming heterogeneity is the most challenging issue where not only the resources but also the federation mechanisms and implementations themselves are heterogeneous when federating across the boundaries of administrative domains. Federation might take place on several abstraction layers where in the end different federations might agree to federate on yet another overarching level. This will ultimately lead towards a massive federated resource pool where users can assemble desired functionality across layers and administrative boundaries upon demand in a seamless manner. This vision is driving our work. A separate contribution has been prepared for EuroView2010 covering more details regarding generic resource federation (Wahle and Magedanz, Generic Resource Federation - Mechanisms and Prototypes Serving the FIRE and FI PPP Visions).

ACKNOWLEDGMENT

The project G-Lab Deep is funded by the Federal Ministry of Education and Research (BMBF).

REFERENCES

[1] G-Lab Deep - Deepening G-Lab for Cross-Layer Composition, http://www.g-lab-deep.de/, 2009

[2] T. Magedanz and S. Wahle. Control Framework Design for Future Internet Testbeds. e & i Elektrotechnik und Informationstechnik, 126(07/08):274-279, July 2009. ISSN: 0932-383X (print) ISSN: 1613-7620 (online).