Functional Composable Cross-Layer Security

Irfan Simsek, Dirk Hoffstadt, Erwin Rathgeb
Computer Networking Technology Group
University Duisburg-Essen, Germany
{irfan.simsek, dirk.hoffstadt, erwin.rathgeb}@iem.uni-due.de

I. INTRODUCTION

Security in Internet was based on the "fix it as you go"-approach which was the only viable strategy as yet. This resulted in multiple fragmented and complex solution approaches which are obviously inadequate – from a conceptual as well as from an operational perspective. However, the researches on a completely new Future Internet architecture afford defining and evaluating new, much more disruptive ideas on Internet security.

In the context of a global research effort on the Future Internet Security, G-Lab DEEP [1] – where Fraunhofer Fokus, TU Berlin, TU Kaiserslautern and our group cooperate, explores on the one hand a Future Internet architecture based on a service-oriented, dynamic service and network composition (Functional Composition, FC [2]), and on the other hand, Cross-Layer security functionalities which can dynamically be added when required in both infrastructure and the service domains in order to achieve a new level of security combining the strengths of network and service level security approaches, as shown in Figure 1.

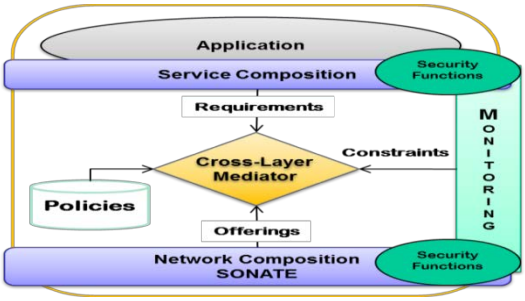

Figure 1. G-Lab DEEP Future Internet Security

In this concept, the G-Lab DEEP FC Framework, SONATE [2] manages, executes and delivers the requested network functions, while the Mediator [3] coordinates Cross-Layer composition between service and network level – based on policies, application requirements, constraints and available Functional Blocks (FB).

In order to analyse the inherent benefits of such an approach on the G-Lab experimental platform, interactive voice and multimedia services have been chosen as a challenging example application. Besides being challenging, these services already exist in today's Internet, and the services as such, their vulnerabilities and possible attack scenarios are already fairly well known [4].

In this presentation, we describe the experiment scenarios and the components developed within the G-Lab DEEP Project providing enhanced security functionality in the service domain – which we group in detection and mitigation functionalities. We will focus on the integration of this functionality into the FC-Framework and, in particular, on the Cross-Layer cooperation aspects to show the benefits of this approach.

II. DETECTION

While general attacks, such as Denial of Service (DoS), can efficiently be detected on the network level, the service specific information is needed for precise deciding on communication anomalies. The combining of detection systems on the network and service level facilitates accurately the detection intrusion.

In the context of G-Lab DEEP, we developed a Distributed Sensor System (DSS) and an Intrusion Correlation and Aggregation Centre (ICAC) – acting on service level and cooperating with the network level components in Cross-Layer manner (see Figure 2). The architecture of the DSS is so designed that a single sensor acts as a FB in the FC Framework and can be activated when required. Via a FC interface, the sensors get the activating impulse and the service specific traffic to be monitored. The activated sensors register at the ICAC and operate rule-based. Sensor rules define how and when sensors should react to service specific traffic to be monitored. By the use of a Honeypot system [5], we analysed the real attacks against voice and multimedia services based on the Session Initiation Protocol (SIP) [6] which evolved de facto standard for such services. Thus, we defined specific sensor rules to detect diverse SIP attacks.

The ICAC is the central point on the service level to correlate, aggregate and exchange detection information via the following interfaces:

- **Service Level Detection Interfaces:** The registered sensors report detected intrusions in Intrusion Detection Message Exchange Format (IDMEF) [7] to the ICAC. Furthermore, the ICAC can update the rules at the registered sensors.
- **Service Level Defence Interfaces:** The ICAC can trigger the Collector Centre for the distributed Filter System on the service level (see chapter III) in IDMEF to filter the service specific traffic for the detected attack source.
- **Cross-Layer Interfaces:** Via this Interfaces, the ICAC gets alerts in IDMEF from network level to service-

specifically analyse the communication traffic. Thus, the rules can accordingly be updated at sensors. Furthermore, the ICAC can trigger network defence components, e.g. distributed firewalls, in IDMEF to filter as closely as possible to attack source detected.

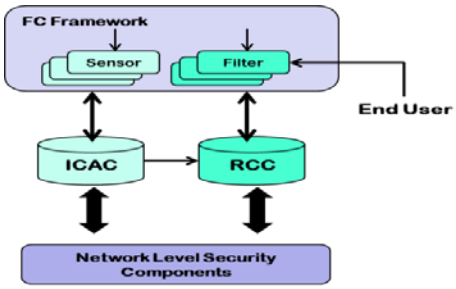

Figure 2. G-Lab DEEP Service Level Security Components and their Interfaces

III. DEFENCE

Defence mechanisms acting on network level can offer effective and efficient protection against attacks; however, these systems can cause serious problems in case of False Positives. Thus, a suitable interaction with end user is of crucial importance. Furthermore, for the protection against service specific attacks, such as Spam over Internet Telephony (SPIT) [8], the interaction with end users is vital.

We developed a distributed SIP Call Filter System (DCFS) with a Rating Collector Centre (RCC) on service level (see Figure 2). As well as the sensors, the filters can act as FB in the FC Framework and can be activated via a FC interface when required. The filters perform on the basis of caller ratings. By the use of defining multiple rating levels, the filter reaction is defined for coming calls. Via a suitable interface, an end user can interact with the filter and can rate herself coming calls. According to achieved rating level, predefined events are performed for a call, e.g. directly putting through, solving CAPTCHAs, or completely filtering.

The RCC is the central point on the service level to correlate, aggregate and exchange rating information via the following interfaces:

- **Service Level Defence Interfaces:** If a new caller is rated or the rating level for an existing caller changed at a filter, the filter reports the caller rating to RCC via Remote Procedure Call (RPC) [9]. For each coming report in RCC, the global caller ratings are correlated and distributed to each filter via RPC.
- **Cross-Layer Interfaces:** Via this Interfaces, the RCC can exchange rating information by using the IPFIX protocol [10] with the network level defence components.

IV. EXPERIMENT SCENARIOS ON THE G-LAB TESTBED

With the help of the Honeypot results, we defined divers SIP attack scenarios in order to evaluate the components described in this paper. VoIP/Asterisk server integration on the standard boot image at the G-Lab testbed allowed us to effectively set up the scenarios on the testbed.

The first scenario is a SPIT attack scenario. An attacker tool – developed on the basis of the Honeypot analysis, performs SPIT calls. The Distributed Context-Aware Firewall (D-Caf) – developed in the context of G-Lab DEEP, is a network level security component which is able to react to overload situations. Thus, the D-Caf can detect the traffic overload caused by the SPIT calls. The source of the detected overload is reported to the RCC which distributes an inferior rating for the caller to the filters. Thus, the caller has to solve CAPTCHAs or is directly rated by the end user as SPIT call. The RCC gets the new rating from the filters and reports this to D-Caf which can block the SIP traffic from the attacker.

The second scenario have been successfully demonstrated at EuroView2011 [11].

In the third scenario, we have the same attack scenario as in the second scenario. However, the security components on the network and service level cooperate directly via the described interfaces. Furthermore, we developed a tool to replay the real SIP attack messages traced by the Honeypot system. This tool – which is initialised on a G-Lab node, and G-Lab testbed environment allowed us to evaluate our components with real world terms. In this scenario, we have achieved the same evaluation results as in the second scenario.

V. ACKNOWLEDGEMENTS

This work is funded by the German Federal Ministry of Education and Research within the scope of the G-LAB DEEP project as part of the G-Lab project.

[1] BMBF Funded Project, G-Lab DEEP, [online] (last access 25.05.2012) http://www.g-lab-deep.de

[2] Paul Mueller, Bernd Reuther. Future Internet Architecture - A Service Oriented Approach, it - Information Technology, Jahrgang 50 (2008)

[3] Abbas Siddiqui, Daniel Günther, Paul Mueller. Mediation between Service and Network Composition, 10th Würzburg Workshop on IP: Joint ITG, ITC, and Euro-NF Workshop "Visions of Future Generation Networks" EuroView, (2010), Würzburg, Germany

[4] Sandro, 11 million Euro loss in VoIP fraud .. and my VoIP logs, [online] (last access 09.06.2011) http://blog.sipvicious.org/2010/12/11-million-euro-loss-in-voip-fraud-and.html

[5] Dirk Hoffstadt, Alexander Marold, Erwin P. Rathgeb. Analysis of SIP-Based Threats Using a VoIP Honeynet System. The 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, June 2012, Liverpool, United Kingdom

[6] J. Rosenberg et al. RFC 3261-SIP: Sessio7n initiation protocol, 2002.

[7] H. Debar, D. Curry, and B. Feinstein. RFC 4765 - The Intrusion Detection Message Exchange Format. IETF, 2007

[8] Jonathan Rosenberg, Cullen Jennings, Jon Peterson. The Session Initiation Protocol (SIP) and Spam, SIPPING Internet-Draft, 17 July 2005

[9] R. Thurlow. RFC 5531 - RPC: Remote Procedure Call Protocol Specification Version 2. IETF, May 2009

[10] J. Quittek, T. Zseby, B. Claise, and S. Zander. RFC 3917 - Requirements for IP Flow Information Export (IPFIX). IETF, October 2004

[11] Michael Kleis, Christian Varas, Abbas Siddiqui, Paul Müller, Irfan Simsek, Martin Becke, Dirk Hoffstadt, Alexander Marold, Erwin Rathgeb, Christian Henke, Julius Müller, Thomas Magedanz. Cross-Layer Security and Functional Composition for a Future Internet. 11th Würzburg Workshop on IP: Joint ITG and Euro-NF Workshop "Visions of Future Generation Networks" (EuroView2011), Aug. 2011, Germany