Cross-Layer Security and Functional Composition for a Future Internet

Michael Kleis*, Abbas Siddiqui†, Irfan Simsek‡, Martin Becke‡, Dirk Hoffstadt‡, Alexander Marold‡, Christian Henke§, Julius Müller§, Cristian Varas*, Thomas Magedanz §, Paul Müller †, Erwin Rathgeb ‡
* Fraunhofer FOKUS, Germany
Email: {michael.kleis, cristian.varas}@fokus.fraunhofer.de
† University of Kaiserslautern, Germany
Email: {siddiqui, pmueller}@informatik.uni-kl.de
‡University Duisburg - Essen, Germany
Email: {martin.becke, irfan.simsek, dirk.hoffstadt, alexander.marold, erwin.rathgeb}@iem.uni-due.de
§Technical University Berlin, Germany
Email: {christian.henke, julius.mueller, thomas.magedanz}@tu-berlin.de

I. Introduction

Today's Internet can be characterised as a global scale packet based network offering best effort transport. The results of intensive network research and standard development in the areas of security, IPv6, Quality-of-Service (QoS) and reliability are most of the time not available for the common end user. In fact security sensitive services becoming more and more popular leading to several security related problems to be addressed for a Future Internet. One example for such a service is Voice-over-IP (VoIP) based on the Session Initiation Protocol (SIP). Among many SIP attack types, Registration Hijacking aiming for a toll fraud is one attractive attack. In a raid in december 2010, people were arrested who caused a damage of about 11 million Euro with such an attack [4]. To address aforementioned issues, the G-Lab DEEP Project [1] investigates in Functional Composition (FC) [3] which allows to introduce and combine network and security functionalities on demand, to establish a data path between communicating devices optimised for their needs. The additional integration of Cross-Layer principles allows services to state requirements to the network and at the same time the network can provide feedback using e.g. a subscription/notification mechanisms for individual connections.

In this paper we describe a demonstrator developed within the G-Lab DEEP project [2] combining Cross-Layer Security and FC principles. The use case we address is the protection of VoIP domains against Registration Hijacking attacks. In the demonstration, is shown how Cross-Layer Security combined with Network and Application Level FC principles can be used in a flexible way to detect, trace back and mitigate such attacks. The combination of Cross-Layer and FC principles allows to assign the resources of network components in a fine-grained and controlled way. Measurement probes for detection and trace back as well as filter modules can be instantiated on demand for selected flows. The whole process is controlled based on predefined FC templates. The prototype has been developed on a G-Lab Testbed.

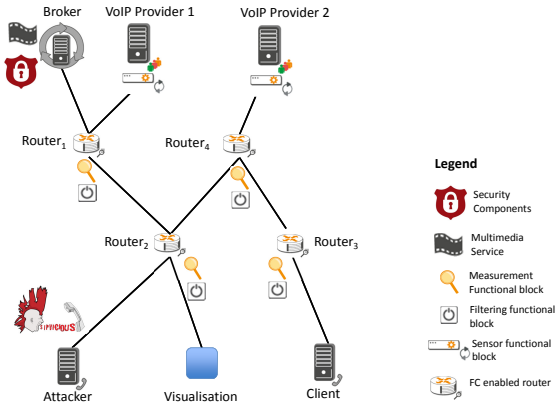

Fig. 1. *Testbed Topology, Demonstrator Components and Functional Blocks*

II. Toll Fraud Scenario and G-Lab DEEP Components

In a typically toll fraud attack, the attacker begins to scan a VoIP domain to discover the SIP Servers and available user accounts. In the next step, the attacker attempts to hack discovered user accounts. To detect and mitigate such attacks we adopt a network level FC framework with security Functional Blocks and Cross-Layer interaction with service level components. As a result we are able to keep the impact of toll fraud attacks within limits (as practically, it cannot be completely avoided). The core components of our demonstration scenario are:

- **VoIP Providers:** For the demonstrator we use two provider instances. One based on the IP Multimedia Subsystem (IMS), the other one based on an Asterisk Server.

- **Client:** Based on the MyMONSTER client, a Softphone for voice and video over IP.
- **Attacker:** Based on the commonly used SIPVicious tool to start the attacks in the demonstration scenario.
- **SONATE:** The G-Lab DEEP FC Framework [3] used to manage, execute and deliver the requested network functions.
- **Cross-layer Mediator:** The Mediator [6] coordinates cross-layer composition based on policies, application requirements, constraints and available FC functional blocks.
- **Broker:** The broker selects and composes the required application level services necessary to satisfy the user request. The corresponding network related requirements are signalled to the Mediator.
- **Intrusion alert Correlation and Aggregation Center (ICAC):** To correlated and aggregate intrusion alerts.
- **Packet Tracking Collector**: To correlated and aggregate network measurements.

The FC functional blocks developed to be used in the demonstration with SONATE are:

- **Packet Tracking Probes:** Measurement probes for the traceback of attacks.
- **Filtering:** A functional block for filtering of attack flows.
- **SIP Intrusion Detection Sensor System:** Distributed sensors for the detection of SIP intrusions.

The G-Lab network setup with the described components is shown in Fig. 1. To show also the possible damage of registration Hijacking attacks, the demonstration is based on the following steps:

1) Registration Hijacking Attack to an unprotected SIP domain.
2) Hacked user account is used at a VoIP Server to establish a video call to a premium number. The legitimate user would have to pay the call.
3) Network is set to defence condition: Sensors are activated to detect Registration Hijacking attacks. Network level FC templates contain sensor, trace back and filter functional blocks.

In the following we describe the demo flow for the last step.

III. Defence Condition

After starting the attacker, the interactions from detecting until blocking the attack are as follows:

1) Sensor functional blocks detect the intrusion based on predefined attack patterns.
2) Sensors report intrusion alerts in Intrusion Detection Message Exchange Format (IDMEF) [5] to the ICAC.
3) Correlating and aggregating the alerts. The ICAC triggers the Broker and reports attack source IP-Address and attacked SIP Extensions to the Broker.
4) Broker triggers SONATE to activate the Packet Tracking components via the Mediator.
5) Trace back of the attack traffic to the last G-Lab node with filtering functional block.

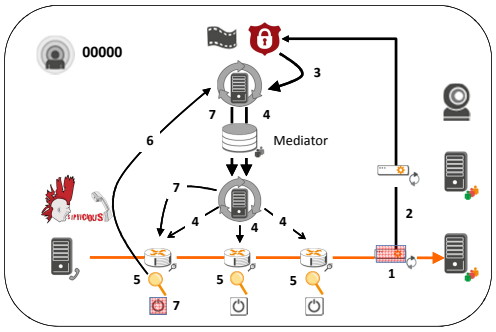

Fig. 2. *Attack Mitigation on Real-Time Display*

6) The Packet Tracking Collector informs the Broker about the G-Lab node close to the source of the attack.
7) The Broker triggers the SONATE to activate the filtering functional block at the reported G-Lab node via Cross-Layer Mediator.

To be able to illustrate these steps, the demonstrator has two network related visualisation displays. The first one is based on netview [7] to visualise the actual network flows in the demonstrator testbed, as well as the trace back for attack mitigation. The second one is a real-time display, showing the components, activated functional blocks and the high level message flows between components. In Fig. 2 the current version of the real-time display is shown while displaying the interactions of demonstrator components in defence condition. In the actual demonstration the interaction between components is visualised sequentially.

IV. Acknowledgements

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

References

[1] BMBF Funded Project, G-Lab, [online] (last access 09.06.2011) http://www.german-lab.de
[2] BMBF Funded Project, G-Lab DEEP, [online] (last access 09.06.2011) http://www.g-lab-deep.de
[3] Paul Mueller, Bernd Reuther. Future Internet Architecture - A Service Oriented Approach, it - Information Technology, Jahrgang 50 (2008)
[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] H. Debar, D. Curry, and B. Feinstein. RFC 4765 - The Intrusion Detection Message Exchange Format. IETF, (2007)
[6] Abbas Siddiqui, Daniel Günther, Paul Mueller. Mediation between Service and Network Composition, 10th Wrzburg Workshop on IP: Joint ITG, ITC, and Euro-NF Workshop "Visions of Future Generation Networks" EuroView, (2010), Würzburg, Germany
[7] Santos, Tacio, Henke Christian, Schmoll Carsten, Zseby Tanja, Multi-hop packet tracking for experimental facilities, Proceedings of the ACM SIGCOMM conference (2010), New Delhi, India