Security solutions for future communication networks

Celtic-Plus project SASER

Dr. Eugen Lach, Coordinator
SASER and SASER-SaveNet
Alcatel-Lucent Deutschland AG
eugen.lach@alcatel-lucent.com

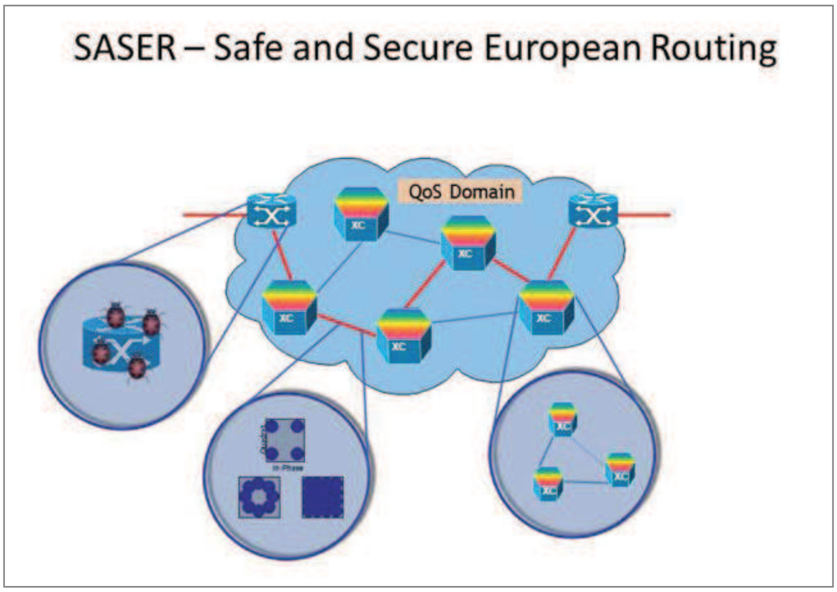
Wolfgang Thomas, Leader
Working Committee 2 “Safe network and node architectures“, SASER-SaveNet
Alcatel-Lucent Deutschland AG
Wolfgang.thomas@alcatel-lucent.com

Iris Adam, Leader WP1-Security, SASER-SIEGFRIED and Working Committee “Security”
Nokia Solutions and Networks Management International GmbH
Iris.Adam@nsn.com

Dr. Marco Hoffmann, Leader
SASER-SIEGFRIED
Nokia Solutions and Networks Management International GmbH
marco.hoffmann@nsn.com

Dr. Ralf-Peter Braun, Leader
Working Committee 4 “Reference Scenarious, test infrastructures and system tests“, SASER
DEUTSCHE TELEKOM AG,
T-Labs
Ralf-Peter.Braun@telekom.de

The SASER project for “Safe and Secure European Routing” has the goal to provide scientific and technical solutions for future secure networks with a sustainable energy- and cost structure. SASER is a multi-national research project within Celtic-Plus, the EUREKA Cluster for a Smart Connected World.



SASER – Safe and Secure European Routing

New SASER Routing Architecture

The SASER-SaveNet subproject is focused on the investigation of new architectures of opto-electrical network elements, which build the layer 0 and layer 1 optical transport network. A key question is how distributed network element architectures can increase the availability and security of optical network elements:

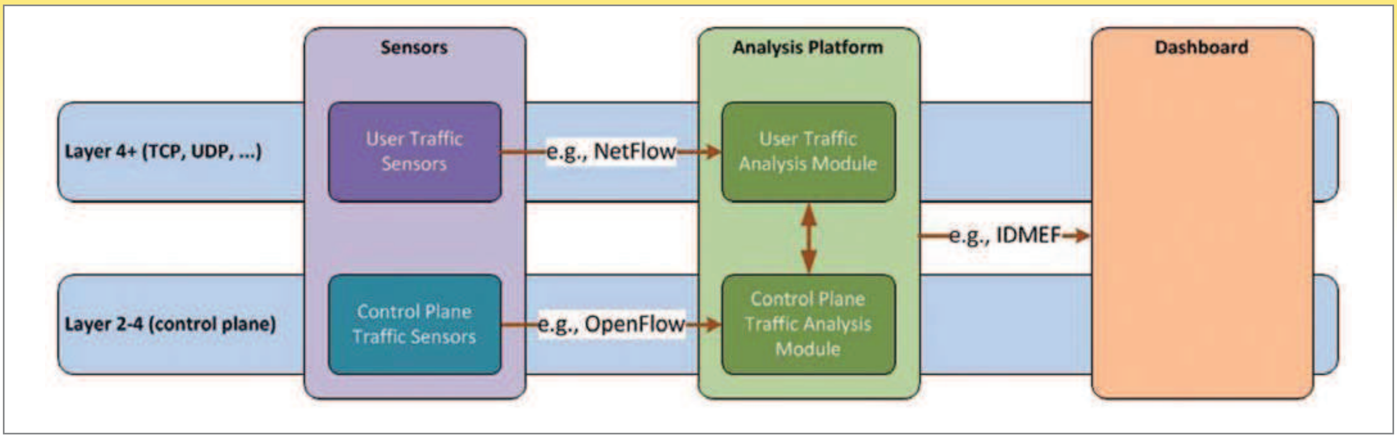
The sub-project SASER-SIEGFRIED has the aim to increase the safety and cyber security capability of communication networks. The partners of the work package “Security” in SASER-SIEGFRIED consist of telecommunication vendors, universities and research facilities from Germany and Finland. They focus on the development of methods to protect networks against external and internal attacks. Their activities include the evaluation of a security concept for a new network architecture based on virtualization, cloudification and software defined networking. Anomaly detection, backdoor detection and visualization technologies are investigated to detect cyber-crime hidden inside massive data.

SASER-SaveNet

The concept of virtualization, which is known from computing, can also be applied to transport networks. In computing virtual computers are established on top of a trusted computing platforms, which controls the virtual machines and makes sure that they are separated from each other, so that a failure on one virtual machine cannot bring down the service of the other virtual machines. Analog to this concept physical transport links can be separated into virtual communication channels and can be operated separately from each other. By guaranteeing bandwidth for each virtual channel, the channels cannot influence each other, which guarantees the availability and achieves high quality of service. Denial-of-service attacks, which aim to overload virtual channels, cannot impair other virtual channels.

Another virtualization concept is to split large network elements into several smaller distributed network elements, which behave like one big (virtual) network element. This increases the overall network security as failed or attacked parts of the virtual network element can be isolated and circumvented. This may reduce or limit the services and bandwidth of the virtual node, but does not bring down the virtual node as a whole.

One security risk of distributed systems is the fact that they expose internal communication interfaces to attackers, as for example two parts of the network element are interconnected via standard Ethernet cabling. This is not only a problem of distributed telecommunication systems, but a general problem of machine-to-machine interfaces. In the mechanical engineering industry, for example, construction engines are more and more integrated with IT systems and also there the communication interfaces of the machines must be secured. Although it is in principle known how to implement encryption and authentification in embedded systems, interfaces are often inadequately secured due to a lack of development time, incomplete protocol specification, incapable implementation, insufficient testing and the like. What is required are software tools, which support development engineers to specify and rapidly deploy secure protocols.


Sensors
Analysis Platform
Dashboard
Layer 4+ (TCP, UDP, ...)
User Traffic Sensors
e.g., NetFlow
User Traffic Analysis Module
e.g., IDMEF
Layer 2-4 (control plane)
Control Plane Traffic Sensors
e.g., OpenFlow
Control Plane Traffic Analysis Module

Scalable Sensor and Analysis Platform

In SASER-SaveNet the software defined networking (SDN) approach is seen as a crucial concept to increase network security and reliability. SDN has gained a lot of attraction recently and allows to rapidly develop and deploy new applications and services to packet networks. Originally invented to control switches and routers in data networks, SDN can be extended to transport networks. This allows to dynamically provide connectivity between router ports through the optical network. By providing virtual links between routers, through-traffic in the routers can be reduced. This reduces the power consumption of the network and increases the network security and reliability, as the optical light paths are much harder to manipulate than IP packet streams.

SASER-SIEGFRIED

As a starting point in SASER-SIEGFRIED, a comprehensive threat and risk analysis for an optical network as deployed today was carried out that identified 39 different threats. An assessment based on the methods suggested by ISO 27005 resulted in each threat being classified as either "minor" (applied to 20 threats), "intermediate" (15), "major" (4) or "critical" (0). In particular, the assessment showed that the most critical attack surface of an optical network seems to be the management plane, so securing this part of the network and applying secure operational procedures should be the highest priority of optical network operators when securing their networks.

Future telecom operator services are characterized by global delivery of high-performance applications over high-capacity network infrastructures. As current applications evolve, it is not feasible for telecom operators to set up and configure a dedicated network for each application. Therefore, a key challenge for operators is the deployment and operation of dynamic and scalable network infrastructures capable of supporting all application types. In SASER-SIEGFRIED, we address this issue using Software Defined Networking (SDN) and network virtualization. An integral part of SDN is the separation of data and control plane, leading to increased programmability and flexibility in a network, whereas network virtualization makes a physical infrastructure more easily shareable. However, the introduction of new technologies in the telecommunications environment introduces new security challenges which may demand innovative solutions. Within the project we focus on analysing and designing mechanisms that ensure secure deployment of SDN and network virtualization in a Telco environment. Furthermore we are actively developing an efficient and scalable sensor- and analysis platform for control and data plane monitoring. The approach of the analysis platform is based on the idea shown in the figure below.

The new management flexibility and increased network bandwidth have the potential to open new attack surfaces against the network and can broaden the existing threats against the users. Our security monitoring provides a thorough approach for the task to detect anomalies in control and user traffic. These anomalies could either stem from traditional threats, such as DDoS or botnet activity, but could also be new threats induced through the SDN architecture.

However, the use of anomaly detection in practices is hampered by a high rate of false alarms. Security dashboards can be used to solve the information overload problem and support the analytic tasks to verify that attack alerts are valid attacks. In a first step in SASER-SIEGFRIED, tools for anomaly detection are reviewed for functionality that exists today. This study is accompanied by workshops and interviews with security analysts to understand their complex needs.

As part of SASER-SIEGFRIED we deal with techniques to investigate backdoors in software systems. Our focus is on binary code to build tools and algorithms applicable even if there is no source code available and also to cover malicious functionality injected during or after code generation, e.g., by the compiler tool chain or during operation. As a first approach, methods are developed to foster semi-automated backdoor analysis and detection, intending to discover relevant attack patterns. As a second technique, backdoors are mitigated by preventive, constructive means, in order to minimize the attack surface for malicious code manipulations. In addition, based on state of the art technology and executable backdoor samples, a „Learning Environment" is developed, providing a Linux and Cloud based tool box and teaching material for software analysts, enabling them to quickly understand and apply the techniques examined and developed in SASER-SIEGFRIED.

SASER-Horizontal

In the horizontal activity "Reference Scenarious, test infrastructures and system tests" of the EUREKA/Celtic-plus SASER project the concepts, results and prototypes developed in SASER will be tested and evaluated in a testbed with real Telecom environmental conditions provided for testing the developed advanced optics and packet functionalities and solutions. The feasibility of new functionalities as well as their fitting in existing network infrastructures can be evaluated and demonstrated.

Further information:
SASER website: http://www.SASER.eu
Description and leaflets: http://www.celtic-initiative.org/Projects/Celtic-Plus-Projects/2011/SASER/saser-default.asp