SASER – Towards secure European telecommunication networks

Peter Herrmann and Peter Stollenmayer
Celtic Office
herrmann@celticplus.eu
stollenmayer@celticplus.eu

Figure 1: After signing the SASER memorandum of understanding (from left):Dr. Andreas Leven (Site Lead Bell Labs Germany, Alcatel-Lucent), Christoph Glingener (CTO of ADVA), Dr. Georg Schütte (State Secretary, BMBF – German ministry for education and research), Alain Maloberti (Senior VP Network, Orange France), Dr. Hermann Rodler (Managing Director, NSN Germany), Cornelia Rogall-Grothe (State Secretary, BMI – German ministry of the interior), Jacques Magen (Chairman of Celtic-Plus), and Wilhelm Dresselhaus (CEO of Alcatel-Lucent Germany). (copyright: hannibal/BMBF)

The Internet has developed into a crucial infrastructure. We have reached the point where a reliable Internet is seen as a normal part of citizens' lives. Not to forget the enormous economic impact of the Internet on all kinds of sectors. For the future telecommunications infrastructure, safety and security are amongst the most important factors. The Celtic-Plus flagship project SASER (Safe and Secure European Routing) aims at mitigating security vulnerabilities of today's IP networks and will propose a new architecture for energy- and cost-efficient networks for the time frame 2020.

The project works on the two main challenges in today's communication networks:
The new SASER system will allow more security in the network that will become less vulnerable to unauthorized procurement of information.
The new technology will provide an increased bandwidth of existing networks and will help to cope with the increasing use of the Internet that doubles its capacity every two years.
In June 2014, SASER held a high-level conference in Berlin to show their interim results, and the big potential impacts the project will have on the European telecommunications landscape.

Agreement for secure European network communications

Within and beyond the SASER project for "Safe and Secure European Routing", Alcatel-Lucent, Nokia Siemens Networks, ADVA Optical Networking, Orange and Deutsche Telekom Laboratories agreed in a memorandum of understanding (MoU) to coordinate their joint R&D efforts over the next five years for a secure, robust, and reliable network.

World premiere: demo of configurable network

Eugen Lach, Alcatel-Lucent
eugen.lach@alcatel-lucent.com

Software Defined Transport Networks (T-SDN), i.e. the programmability of optical transport networks, is set to revolutionize how optical networks are operated. T-SDN enables that networks can quickly be configured and adapted to changing traffic demands via network operator or customer applications. This is an important step into the virtualization and automation of future networks.

Alcatel-Lucent, coordinator of the SASER-SaveNet sub-project, exhibited a joint live demonstrator with component partners in the SASER conference exhibition in June 2014 in Berlin. It was a world premiere: for the first time a reconfigurable network was shown which consists of configurable flexible optical nodes and software defined adaptive transponders that incorporate electronic as well as optoelectronic components from the horizontal project partners Fujitsu and Finisar. In this demonstrator a central SDN controller utilizes the standardized OpenFlow protocol for packet networks with extensions towards the lower transport layers (Transport-SDN) to steer the programmable hardware like optical switches and transponders. These extensions to the OpenFlow protocol were developed by the researchers of Alcatel-Lucent within the project.

The demonstrator consists of flexible optical nodes comprising wavelength selective switches (WSS) in combination with flexible transmitters and coherent receivers. To enable an agile transport network the transmitters can adjust their wavelength, modulation format, their baud rate and thus the spectral bandwidth of the transmitted optical channels.

The demonstrator permitted the realization of different real network scenarios. For example, the network operator can adjust the bandwidth or the modulation format of the signal to achieve, e.g., either the longest possible transmission distance or transmit a higher data volume on a shorter range. Set up of a new optical lightpaths and shut down of others is possible as well as re-allocating WDM traffic to other spectral channels.

With the introduction of network virtualization, e.g. slicing of physical resources, applications can modify their own logical network. Software-defined solutions allow partitioning of the network and enable to route critical data within predetermined boundaries, a concept called network slicing. This measure can significantly increase resource utilization and enhance safety and network security.

If protocol encryption is applied in Transport-SDN additionally, e.g. by using a protocol engineering suite developed by Alcatel-Lucent within SASER, which simplifies creation and deployment of secure protocols, a further important step towards secure networking can be made.

Figure 2: Demo at the SASER Event in Berlin, June 2014 (copyright: hannibal/BMBF)

Detecting known and novel attacks by analyzing SDN user and the control traffic

Iris Adam, Nokia
iris.adam@nsn.com

Today safety and security are addressed through diverse security actions, such as encryption, software-enabled security functions, backdoor and anomaly detection, and many others. The SASER project will bring these bits and pieces together, towards the definition of a suitable security scenario that is an important step towards secure communications in Europe and in the world.

SASER's main objective is the development of secure and energy-efficient network architectures for upcoming technologies such as Software Defined Networking (SDN) and Network Function Virtualization (NFV). These new technologies are key-enablers in the future telecommunication environment but also include new security challenges. Within the project we focus on analysing and designing mechanisms to ensure secure deployment of SDN and virtualization in a Telco Cloud environment.

After a thorough analysis of the SDN architecture in a Telco Cloud environment, the threats were identified and countermeasures have been defined. This comprises mainly authentication and authorization measures as well as integrity and confidentiality protection between all involved entities (Applications, SDN Controllers, Network Hypervisors and SDN Switches). Additionally encryption techniques on the transport layer enable secret communication by protecting the confidentiality and the privacy of the transmitted user data on the network.

While today's and even more future communication networks are able to transport high volumes of data, there is a tendency that large portions of the bandwidth are misused for dubious purposes, e.g. recently there has been a dramatic growth in high volume Denial-of-Service attacks. In SASER we provide techniques to detect known and novel attacks by analysing the SDN user traffic as well as the SDN control traffic. Rapidly detecting and classifying malicious activity contained within a large amount of network traffic is a challenging task. As network operators are overwhelmed with data from the network monitoring tools, we provide visualization methods to facilitate and promote situational awareness taking maximum advantage of the fact that the human mind is capable of fast visual processing.

Software backdoors pose an extremely dangerous attack vector. It is important to employ various techniques to explicitly search for potential backdoors, to make them easier to detect and to make their insertion harder. In SASER we design and implement software architectures to prevent authentication backdoors in server applications (proactive approach). Furthermore, we design and implement an analysis tool for mostly automated detection of specific backdoors in server applications (reactive approach).

risks. To achieve this we need joint efforts in Europe. SASER is a sparkling example of how we can improve digital sovereignty through joint efforts."

About SASER

SASER (Safe and Secure European Routing) is an 80 million euro public-private partnership project comprising 61 companies, research organisations, and universities from Germany, France, Finland, Denmark, and the UK. The project runs from August 2012 to September 2015 under Celtic-Plus, the EUREKA Cluster for a Smart Connected World, and is partly publicly funded by the research ministries / agencies BMBF (Germany), DGCIS (France), and TEKES (Finland).

■ Further information
SASER Project Website:
http://saser.eu/
SASER Event news release:
http://www.celticplus.eu/Events/SASER-Event-Berlin/ReportEvent.asp
SASER information video:
https://www.youtube.com/watch?v=MD1tkNMzq6Y
SASER Demo in IEEE:
http://goo.gl/sYDkcK