SASER-SIEGFRIED – architecture and technologies for secure future networks

Objectives:

Within the SASER-SIEGFRIED project, all partners jointly designed an architecture and technologies for secure future networks. The target was to correct security deficits of today's Layer 3 networks. The following activities were accomplished for this objective:

- Firstly, data transmission was downscaled as far as possible to lower network layers (Layer 1 and 2), to reduce the need of IP-routers, which had to be considered as critical to security. This was realized by adopting technologies of network virtualization, SDN (software defined networking) and efficient redundancy, based on flexible and highly available optical systems.

- Secondly, mechanisms of security for future networks were designed, based on an analysis of remaining security problems in Layer 3 (for example: Backdoor and Anomaly detection).

Consortium:

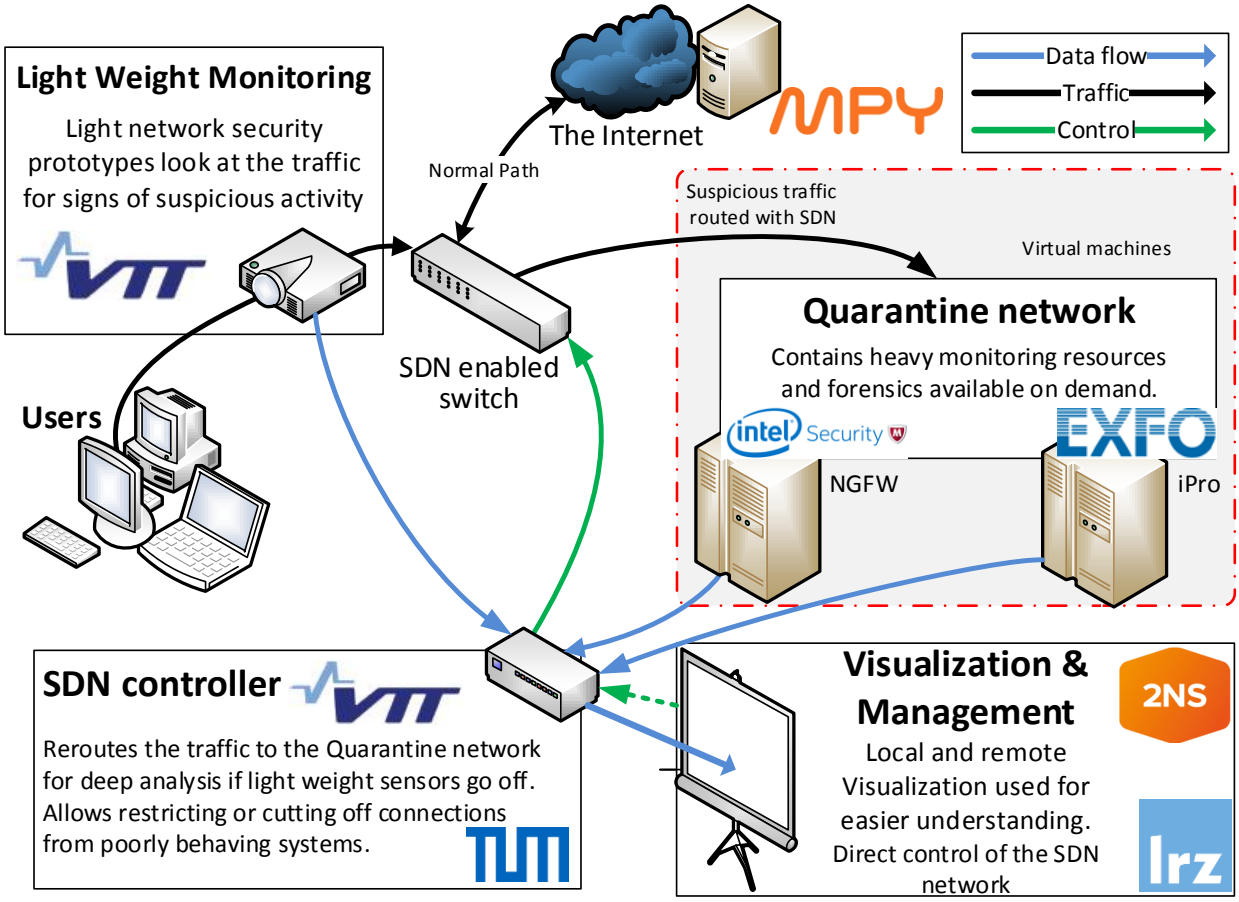
The project ran from August 2012 until December 2015 and involved 26 partners from Germany (15), Finland (5), France (5) and Denmark (1) from industry, research institutes and academia. As a Celtic-Plus project it was carried out under the umbrella of EUREKA and received public funding from the German Ministry for Education and Research (BMBF), the Finnish Funding Agency for Innovation (TEKES) and the French DG Entreprises (DGE) for parts of their effort.

Results:

During the project, many excellent results were achieved. Three major highlights to mention were joint implementations of partners from different countries and work packages realized as proof of concepts or as a field trial:

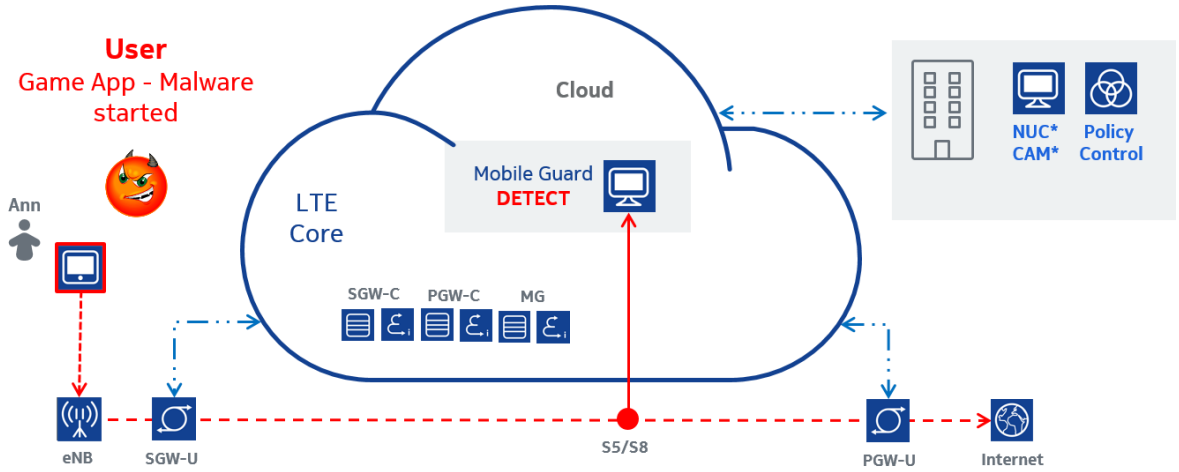
- **Adaptive Monitoring and Management of Security Events with SDN**
  In a live operator network the user traffic to the Internet is monitored by a "light weight" monitoring system. This system analyzes the traffic regarding "man in the middle attacks". If an "anomaly" is detected, the monitoring application triggers the SDN controller to reconfigure the SDN switches with the aim to reroute the suspicious traffic to a quarantine network where enhanced analysis is executed. In case of false positives, the traffic is routed back and the monitoring application is informed to adapt the thresholds. Additionally there are two interfaces from the monitoring application to a management system. The first one is

used to steadily send Netflow data, which is aggregated and visualized in the management system for the purpose of continuous monitoring the security state of the network and to complement the automatic analysis (detection of false positives and false negatives). The other connection is bidirectional to exchange alarm messages in case of security incidents. The demo was setup by all Finnish partners, TU Munich, Leibniz Supercomputing Center and Nokia.



- **SDN-Based Security Enforcement in Mobile Networks using VNFs**

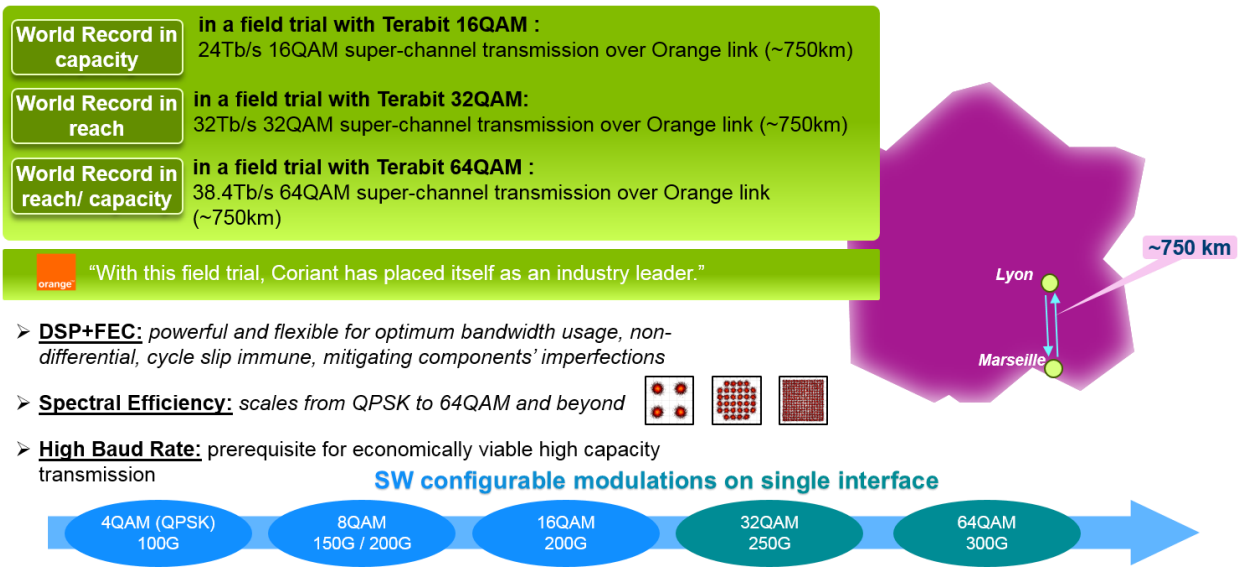
The demonstration shows Nokia's Mobile Guard security appliance, which detects malware infections using its user plane agent located between mobile Serving Gateways (SGW) and Packet Data Network Gateways (PGW). Typically, at this point the Mobile Guard would issue a warning to the user via SMS or email. However, this would allow the malware to have Internet access until the user reacts to the notification and removes it from the device, which bears the risk of spreading further or in the worst case disrupting network operation.



Therefore, within the SASER-SIEGFRIED project, Nokia and BISDN leverage SDN's northbound API to notify the PGW SDN controller of the attack and redirect all traffic coming from the device towards a Nokia appliance in the cloud, which offers a SuperClean app for the tablet to be cleaned. After the user has downloaded the app and used it to remove the malware from the tablet, the Mobile Guard will instruct the PGW SDN controller to forward its traffic normally again. The PGW-C application running in parallel on the controller and thus, the normal operation of the mobile network is unaffected by this.

Different versions of this demonstrator were shown during the midterm and final review, the Mobile World Congress 2014, SIGCOMM 2014 and Glocecom 2015.
Besides Nokia and BISDN, Fraunhofer AISEC contributed to the SDN security and T-Labs provided their cloud environment.

- **World Record Flexi-rate Field Trial**
  In a field trial in the Orange optical transport network between Lyon and Marseille in France four world records were broken.



In this field trial, advanced technology engineers from Orange, Coriant, Ekinops, Keopsys, and Socionext successfully demonstrated the highest ever C-band transmission capacity using 24 x 1 Tbps/DP-16QAM (i.e. 24 Tbps), 32 x 1 Tbps/DP-32QAM (i.e. 32 Tbps), and 32 x 1.2 Tbps/DP-64QAM (i.e. 38.4 Tbps) modulation formats in a "live" networking environment. The companies also achieved a record-setting transmission reach of 762 kilometers in the same live environment, more than twice the distance of any previous field records for 32QAM, and the first ever regional transmission for 64QAM. These achievements represent an important milestone in the research and development of highly scalable, spectrally-efficient optical networking technologies optimized for future network growth.

In addition to these major highlights a very high number of more than 250 scientific presentations, journals, and conference contributions (80 – 90 % of those related to highly technical levels and with peer-review selection processes for contributions) proved the quality of the project results. 7 standardization contributions were submitted, 24 IPRs generated and 6 press releases (incl. 1 interview) published.

- "Record-breaking Transmission Field Trial of 38.4 Tbps over 762 kilometers Lyon-Marseille-Lyon Fiber Optic Link" (Coriant, Orange, Ekinops, Keopsys, Socionext): https://www.celticplus.eu/saser-siegfried-record-breaking-transmission-field-trial/
- "Coriant and Orange Set World Records for Optical Transmission Capacity and Distance Using State-of-the-Art Modulation Technology in Multi-Terabit Field Trial": http://www.coriant.com/company/press_release.asp?id=1233
- "Socionext takes part in Record-breaking Transmission Field Trial of 38.4Tbps over 762 kilometers": http://www.socionext.com/en/pr/sn_pr20150630_01e.pdf
- "Ekinops Enables Orange to Set Record in Optical Transmission": http://www.ekinops.net/en/press-releases/ekinops-enables-orange-to-set-record-in-optical-transmission
- http://www.keopsys.com/index.php/news/47/112/Record-in-Optical-Transmission.html

- “Geschwindigkeitsrekorde im Rückgrat des Internets“: On field trial Lyon-Marseille-Lyon (Deutschlandfunk) : http://www.deutschlandfunk.de/glasfaser-technik-geschwindigkeitsrekorde-im-rueckgrat-des.684.de.html?dram:article_id=324503

The implementation of 34 different demonstrators influenced the development / improvement of 9 products and showed the high business impact by transferring the results to business lines of the industry partners. On the other side, the academia supervised 57 master and PhD thesis that contributed to the great research results.

Additionally the first time in such a project 4 open source software contributions were developed and are available on different webpages:

- POCO: Framework for Pareto-Optimal Controller Placement: https://github.com/lsinfo3/poco
- OFCProbe: OpenFlow Controller Benchmark: https://github.com/lsinfo3/ofcprobe
- TableVisor: https://github.com/lsinfo3/TableVisor
- xdpd: eXtensible OpenFlow datapath daemon http://xdpd.org/