Proposal for a single presentation for TNC18 in Trondheim

Title: SCIONLab - A Deployment of the SCION Secure Internet Architecture

Presenter's name and affiliation: David Hausheer (OVGU Magdeburg)

Keywords: Network Security, Next-Generation Internet, DDoS Defense, Multipath Communication, PKI

Authors names and affiliations: Kurt Baumann (SWITCH), Alex Gall (SWITCH), David Hausheer (U. Magdeburg), Adrian Perrig (ETH), Matthew Smith (U. Bonn)

Presentation description

The SCION secure Internet architecture [1] has reached a level of maturity, which renders it ready today for large-scale pilot service deployment. SCION enables support for research activities in areas that are difficult to evaluate on the current Internet such as: multipath communication, advanced and highly secure PKI systems, in-network DDoS defenses, next-generation routing architecture policy definitions, path-aware applications, and path-based inter-domain routing architectures.

The multi-faceted SCION architecture provides opportunities for several parties:

- Researchers: Researchers in the area of path-aware networking can so far only study simulated environments. Similarly, DDoS defenses that rely on inter-domain mechanisms can so far only be simulated. As listed above, SCION enables research in numerous areas that are not possible on today's networks.
- End users: Enhanced availability and reliability are the main benefits for applications and end users. Increased bandwidth can be achieved thanks to multi-path operation. Path optimization during a connection can result in increased bandwidth and/or decreased latency.
- NRENs: Better utilization of network resources through multi-path support, potential cost-savings due to fewer leased-line connections.

In this talk, we will present SCIONLab [2], a deployment of the SCION architecture which specifically aims to support Next-Generation Internet (NGI) and security research activities, providing a scalable and reliable platform for future Internet applications, e.g., IoT.

SCIONLab provides a platform for NGI research, enabling real-world research that is otherwise only possible in simulated environments. Furthermore, SCIONLab facilitates the interaction with other deployed SCION networks and services, yet SCIONLab's value proposition compared to Planetlab [3] is distinct in that SCIONLab nodes themselves contribute to the routing within the SCION topology, enabling a broader range of applications by allowing researchers to attach their own computing resources anywhere within the SCIONLab network.

The SCION prototype software is in its 5th generation, and is running in test environments at SWITCH, Swisscom, and ETH Zurich, over the past 18 months. We have already started to put together the SCIONLab administration software, which can be accessed at [2]. Moreover, we have successfully ran a course assignment in a network security course over the prototype SCIONLab environment. In the talk, we will present first results from this setup.

We plan to further extend the SCIONLab administration software. Specifically, we will develop SCIONLab resource monitoring and enforcement mechanisms, as well as tools to help writing SCIONLab applications. We also work on studying the usability of our infrastructure for administrators and end users, in order to improve the usability of our systems.

Initially, our goal is that we can support academic users through SCIONLab, that the functionalities of path-aware networking and hidden paths for secure IoT operation are functional, that the basic resource allocation system is in place for SCIONLab users, and that the control-plane PKI is in place.

Essential for us is to enable multi-path research, with the delivery of a multi-path QUIC socket that applications can make use of. We also enable accurate resource monitoring throughout the SCIONLab environment. For the PKI, we plan to enable the end-to-end PKI system that application developers can rely on to build highly secure TLS applications.

In a next step, we plan to deliver the SIBRA inter-domain resource allocation system, which enables a strong DDoS defense mechanism. The resource monitoring and policing enables detection and mitigation of users that exceed their allocated resources. Last but not least, we improve easy-to-use control- and end-to-end PKI systems.

To increase the scale of the SCIONLab network is for us a real asset. To this end, our idea is to integrate SCIONLab as a pilot service into GEANT, NRENs and associated universities, serving as attachment points for additional SCIONLab users and application developers.

The success metrics that are guiding us in the extension of SCIONLab are based on the following KPIs: Ease-of-use for researchers, network availability and performance (bandwidth and latency), supported features (PKI, DDoS defense mechanisms, path selection support, end host / application support), usability, scalability in terms of network size and amount of usage.

References:

[1] Adrian Perrig, Pawel Szalachowski, Raphael M. Reischuk, Laurent Chuat: SCION: A Secure Internet Architecture - http://scion-architecture.net/pdf/SCION-book.pdf [30.08.2017]

[2] SCIONLab - http://www.scionlab.org/ [30.11.2017]

[3] PlanetLab - https://www.planet-lab.org/ [30.11.2017]

Presenter's biography: David Hausheer is a Professor at the Faculty of Computer Science at Otto-von-Guericke-University Magdeburg since May 2017. He holds a diploma degree in electrical engineering and a Ph.D. degree in technical sciences from ETH Zurich. From 2011 - 2017 he was an assistant professor at TU Darmstadt, Germany. Prior to that he has been employed as a senior researcher and lecturer at University of Zurich, Switzerland from 2005 - 2011, while being on leave as a visiting scholar at EECS, UC Berkeley from October 2009 to April 2011.