Hello everyone

We hope you and your family have experienced Spring in a safe environment and in good health -- with a high-bandwidth and available Internet connection.

These challenging times have reminded us that low-probability events do occur, and it is advisable to prepare for adversarial events.

Much has happened in the networking world over the past months. The resource public-key infrastructure (RPKI) has witnessed a large push, with Cloudflare creating the “is BGP safe yet?” checking tool (https://isbgpsafeyet.com/). As Markus Legner’s article discusses, RPKI is definitely a step in the right direction, but still far from providing a secure routing infrastructure.

Recently, numerous large-scale network outages have occurred. Several of them were due to BGP issues, and would have been prevented in a SCION-based Internet. For instance, the 3-hour long global outage of the IBM cloud, or the major outage at T-Mobile, Verizon, AT&T, and Sprint. Hopefully, these events will further fuel deployment of SCION technology.

On the research front, much progress has happened with the publication of several exciting SCION-related research papers (links are listed at the end of the newsletter). In this issue, we highlight the PISKES paper, which describes the DRKey global key distribution infrastructure, which is the basis for many of the SCION security mechanisms.

David Hausheer reports on the progress of SCION deployment in the GEANT research network, and describes how his team has made SCION available on Android.

As a use case, Christelle Gloor discusses the use of SCION in 5G networks.

Finally, we wanted to ask you to save the date for SCION day on Friday 5th of February, 2021. Due to uncertainties about traveling and holding meetings, we decided to move the date from the originally planned September 29 to February 5, 2021.

RESEARCH

PISKES

Given the increasing prevalence of denial-of-service (DoS) attacks in the Internet and the fact that many of these attacks are enabled or facilitated by the lack of source authentication, our researchers at the Network Security group investigated highly-efficient and scalable systems to perform source-address authentication. This research led to a recent publication of a system called PISKES which will be presented at the AsiaCCS 2020 conference. PISKES enables services to rapidly (within 20ns!) derive a symmetric key for sender authentication. Thus, PISKES enables packet authentication for a wide variety of systems including high-throughput applications.

We have implemented a prototype system that enables a service to authenticate a packet within 85ns, which is over 1500 times faster than a system based on asymmetric cryptography. In addition to the prototype implementation, we fully implemented PISKES in the SCIONlab codebase, giving SCION a leading edge defense mechanism against DoS attacks.

PISKES: Pragmatic Internet-Scale Key-Establishment System.
Rothenberger, Benjamin, Dominik Roos, Markus Legner, and Adrian Perrig.
In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIACCS), 2020.
https://netsec.ethz.ch/publications/papers/piskes_final.pdf

DEPLOYMENT

Why RPKI Won't Save BGP - Markus Legner

The Border Gateway Protocol (BGP) is the mechanism that Internet service providers and other networks use to exchange topology information. At the time when BGP was developed in the 1990s, the Internet's threat landscape was very different from today, and no security mechanisms were integrated into the protocol. It is therefore not surprising that in recent years BGP has been abused on a daily basis for rerouting attacks, referred to as *BGP hijacks*.

Already twenty years ago, researchers started working on better security mechanisms for BPG. While they were designed quite quickly, progress on standardization and adoption was slow and very little changed in actual deployment. In recent years, however, security mechanisms like RPKI and BGPsec have gained traction and seen increasing deployment on the Internet. This sparked the hope of resolving many of the BGP-related security issues in the near future. In a short article, we have summarized and analyzed research that paints a more pessimistic picture of RPKI and BGPsec along multiple dimensions: they (i) cannot solve all current security issues, (ii) have very limited benefits unless they are fully deployed by all networks in the Internet, and (iii) introduce additional security and scalability issues themselves.
We conclude by arguing that to fundamentally secure the routing process of the Internet, we need a more radical change to its architecture. Of course, our proposed solution should not come as a surprise to the reader: SCION.

Deployment of SCION across GEANT - David Hausheer

Following up on our earlier report in the summer 2019 newsletter about the first deployment of SCION across the European-wide GÉANT research network, we are proud to announce the second deployment, which now connects further sites natively through GÉANT. The new deployment, which was designed and implemented by Fin Christensen and Johannes Wünsche at OVGU Magdeburg, now includes besides SWITCH also the German National Research and Education Network (DFN) and SIDN, the operator of the .nl country-code top-level domain. Furthermore, the French large-scale testbed Grid5000 has been connected as well. Each of those networks is now connected to the GÉANT Testbeds Service (GTS) in an entirely BGP-free manner via two separate L2VLANs, which will enable researchers to run experiments exploiting a multitude of path opportunities both from within and across those networks through native SCION connections at up to 10G speeds for certain paths.

Running an entire SCION AS on Android - David Hausheer

The team of Elias Kuiter and Tom Heimbrodt at OVGU Magdeburg have released a new version of the SCION app for Android which now enables to run an entire SCION AS on an Android smartphone. Besides, the new app also made the setup and configuration of a SCION AS on Android very easy. In its current release, the app supports pinging other SCION ASes and reading data from a SCION sensorserver. We welcome both feedback and contributions to the app, for which the source code is available here.

USE CASE

5G - Christelle Gloor

The rapid technological advancement of the last decades have increasingly connected us. Now that cell phones are widely adopted, a large portion of growth of connected systems is driven by the Internet of Things (IoT). We increasingly rely on automated data gathering—for real-time applications or to make our systems learn and adapt to our needs. Examples include driverless cars; smart homes and factories; or general sensors, e.g., to detect and quickly report wildfires. Many new applications will be connected via the cellular network due to their mobile nature or remote location.

Connecting many IoT devices comes with a set of challenges. Due to a plethora of vulnerabilities, IoT device vendors have earned a questionable reputation. Examples include systems with easy-to-crack default passwords that do not force the user to change them and undisclosed backdoors that can be exploited by hackers.

On the user's end, many people do not regularly patch their systems. Barely noticed IoT devices, e.g., in the context of a smart home, will most likely receive even less care. The problem is exacerbated by the remote nature of some devices such as sensors, and the lack of convenient user interfaces, constituting another hurdle for keeping our systems up to date and secure.

With this in mind, the 5G community is currently considering what properties are desirable for networks handling massive IoT deployments—and how SCION could be used in the protocol stack to make them a reality.

The most promising concept discussed to mitigate the impact of unsafe IoT is *network virtualization.* A system is envisioned to create application-specific "zones" spanning the network towards the participating entities. The goal is to ensure isolation between different applications to protect against network-wide threats outside of the zone. SCION already provides control plane isolation between the different isolation domains. Additionally, recent research on SCION-based network virtualization (SVLAN [Kwon et al. 2020]) is being considered as a basis for the zoning mechanism. A global quality-of-service (QoS) system is to be added on top to guarantee service-level objectives through the zone, even during a distributed denial-of-service (DDoS) attack. Here again, SCION researchers have paved the way with the Colibri System, formerly known as SIBRA, which will soon become available in SCIONLab.

Another goal is to lower the attack surface for DDoS attacks by authenticating the source of a packet. Various mechanisms are being investigated including cooperative firewalls and the PISKES system [Rothenberger et al. 2020] based on SCION—this eliminates DDoS amplification through open domain name service resolvers and will facilitate tracing and blocking of malicious traffic.

SCION provides valuable benefits in the realms of security and QoS—stay tuned for news on how SCION will integrate into our future cellular networks!

RECENT RESEARCH RESULTS

PISKES: Pragmatic Internet-Scale Key-Establishment System.
Rothenberger, Benjamin, Dominik Roos, Markus Legner, and Adrian Perrig.
In Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS), 2020.
https://netsec.ethz.ch/publications/papers/piskes_final.pdf

SoK: Delegation and Revocation, the Missing Links in the Web's Chain of Trust. Laurent Chuat, AbdelRahman Abdou, Ralf Sasse, Christoph Sprenger, David Basin and Adrian Perrig.
In Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P) 2020.
https://netsec.ethz.ch/publications/papers/sok-delegation-revocation.pdf

The Value of Information in Selfish Routing.
Simon Scherrer, Adrian Perrig and Stefan Schmid.
In Proceedings of the International Colloquium on Structural Information and Communication Complexity (SIROCCO) 2020.
https://netsec.ethz.ch/publications/papers/scherrer_value_2020.pdf

Thanks for your support and stay tuned for further updates!

The SCION team