Why RPKI Won't Save BGP

Markus Legner*

June 8, 2020

As the initial protocols at the core of the Internet are not sufficiently secure for the scope and threat landscape it has reached since, ever new security patches are being applied. But, as there's a saying, "if you always do what you always did, you will always get what you always got." SCION provides the radical change to the Internet that is needed to fundamentally solve its security issues.

The Internet's fundamental routing protocol BGP and current efforts to fix its security issues

The Internet is not a centrally managed network but rather a federated system of many smaller, independently managed networks, so called autonomous systems (ASes). As there is no central authority, these ASes need to exchange information among each other about where addresses are located, which connections exist, etc. For more than 30 years, this information has been exchanged via the Border Gateway Protocol (BGP). For an IP address range, a so-called *IP prefix*, BGP UPDATE messages exchanged by ASes contain the owner and the full AS-level path through which it can be reached.

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. Over the past decade, however, the lack of authentication in BGP caused the prevalence of routing attacks, in particular BGP hijacks, where a malicious AS announces IP prefixes, which it does not actually own. These attacks cause data in the Internet to be rerouted to the attacker instead of the legitimate recipient and can have devastating consequences, including privacy leaks, outages, and censorship. Suspicious announcements occur on a daily basis, even though it is not always obvious in practice whether these are due to mistakes or malicious actions.

The issues arising from the lack of security mechanisms were recognized early and researchers already started working on security improvements to BPG in the late 1990s and early 2000s. The fundamental idea of the later standardized Resource Public Key Infrastructure (RPKI) and BGPsec, a security-enhanced version of BGP, was to cryptographically certify ownership of IP addresses and authenticate the BGP messages. While change was very slow initially (RPKI and BGPsec were only standardized in 2012

*markus.legner@inf.ethz.ch

and 2017, respectively), there was a substantial increase in RPKI deployment in recent years, which rekindled the hope that the Internet can actually be secured in the near future.

As we will describe in this article, this hope may be premature and a more radical change to the Internet architecture will be necessary to fundamentally fix its security issues.

The latest routing evolutions are still insufficient

RPKI and Route Origin Attestations

By itself, RPKI provides keys to ASes and certificates for the IP addresses they own and are therefore allowed to announce through BGP, so-called route origin attestations (ROAs). This process is done through multiple steps following the delegation of IP addresses starting from the Internet Corporation for Assigned Names and Numbers (ICANN) and regional Internet registries down to individual ASes. When an AS announces that it owns a particular IP prefix through BGP, other ASes can check if it has a valid ROA; if not, the recipient of this announcement can conclude that it is fraudulent and reject it.

Unfortunately, ROAs only prevent the simplest form of BGP hijacks. A malicious AS trying to hijack a particular IP prefix can still send a BGP UPDATE message claiming that it is directly connected to its legitimate owner. Recipients of such an announcement would accept it as the legitimate owner of the addresses is noted as the last AS in the BGP message and would then start sending traffic to those IP addresses to the attacker, who can then inspect, reroute, or drop it.

BGPsec doesn't work well in partial deployment

BGPsec was designed to solve this and more sophisticated types of hijacks by cryptographically authenticating the whole path in BGP messages. However, BGPsec was only standardized three years ago and it will likely take many years until it reaches global deployment. Unfortunately, a detailed analysis of the protocol has shown that it performs very poorly unless *all* ASes use and enforce BGPsec. In a partial deployment (i.e., when some ASes still use "normal" BGP), BGPsec can cause instabilities, is prone to so-called downgrade attacks (in which an attacker causes other ASes to accept standard BGP messages even if a BGPsec-secured path exists), and generally provides very little benefits unless ASes assign highest priority to security.

Problems of BGPsec in full deployment

But even if all ASes in the world were to deploy BGPsec, many issues remain. The paper "Even Rockets Cannot Make Pigs Fly Sustainably: Can BGP be Secured with BGPsec?" shows that attackers would still be able to create wormholes or cause forwarding loops. Even more worrying is the fact that the use of RPKI and BGPsec may introduce circular

dependencies, where communication depends on cryptographic keys and certificates, which in turn require existing communication paths to be exchanged.

RPKI and BGPsec also cause issues for network sovereignty. As very few organizations are at the root of the RPKI hierarchy, these organizations have the power to create or revoke certificates. Depending on the jurisdiction, local courts of some countries may gain the power to shut down parts of the Internet (with the obvious possibility of abuse), which makes some ISPs reluctant to deploy RPKI.

Finally, BGPsec further exacerbates BGP's scalability issues. To provide global connectivity, every one of the currently about 68000 ASes in the world needs to know how to reach every other AS. This requires a large number of BGP UPDATE messages, the processing of which requires much more resources in BGPsec due to the additional cryptographic checks. Furthermore, *prefix aggregation*, which is used to combine multiple IP prefixes to reduce the number of routes and announcements, no longer works in BGPsec. This is particularly cumbersome as the increasing fragmentation of the IP address space and the trend towards announcing ever smaller IP address ranges have caused a strong growth of the number of paths that Internet routers need to store and exchange.

SCION: routing security through a clean-slate design

Parallel to efforts trying to fix the existing Internet, researchers started working on fundamentally new protocols. The new Internet architecture SCION has been researched and developed over the past ten years by many collaborators from research institutes, led by ETH Zurich, and from Anapaya. By recognizing security, reliability, and scalability as core design goals, we fundamentally solve many of the issues of today's Internet.

SCION groups ASes into *isolation domains* according to common jurisdictions or other criteria and thus addresses both scalability and network sovereignty: Instead of discovering paths between any pair of ASes, the routing process is hierarchically separated into an intra-ISD (discovering paths within an ISD) and an inter-ISD process (discovering paths between ISDs). This means that fewer paths need to be discovered and accordingly fewer routing messages are required.

Furthermore, each ISD can define its own roots of trust (instead of relying on a single global entity such as ICANN), which makes its public-key infrastructure (PKI), which provides keys and certificates to the ASes, independent of misbehavior of external entities. All routing messages in SCION are cryptographically authenticated based on this flexible PKI, which prevents hijacking attacks. Finally, by integrating the distribution of certificates with the routing process, no cyclic dependencies between the PKI and the routing process can arise.

The SCION book describes the architecture in much further detail and analyzes how it defends against various attacks that are prevalent in today's Internet. In addition, what was only a research project several years ago is now real: Anapaya's SCION-based public network now spans 12 countries with more than 50 connection points for enterprises and service providers located in major datacenters in Europe and Asia. By fundamentally solving security issues instead of applying ad-hoc fixes, SCION can actually deliver a secure Internet of the future.