An SDN-based approach to enhance BGP security

Regivaldo Costa, Fernando M. V. Ramos
LaSIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal
rcosta@lasige.di.fc.ul.pt, fvramos@ciencias.ulisboa.pt

BGP, the glue that holds the Internet together, is vulnerable to a series of attacks. Several incidents demonstrate their recent materialization in the form of prefix hijacks and route leaks [1]. The networking community is well aware of the problem, with many solutions having been proposed in the past two decades [2].

Motivation. Unfortunately, the most effective solutions for BGP security remain largely undeployed [1]. This is fundamentally due to one (or more) of the following reasons. First, they use cryptographic techniques that are *too computationally expensive* for current routers. Second, they require *changes to BGP* which, due to its widespread adoption and the lack of a centralized authority to mandate such change, makes migration difficult. This problem could be overcome if network operators were given *the right incentives* to migrate to a secure solution. But this is also hard, particularly as several solutions are not effective until there is wide adoption, while others offer benefits to the Internet as a whole, but not to its adopters.

Contribution. The separation of the routing control problem from routers as advocated by Software-Defined Networking (SDN) has been proposed as a solution for BGP problems [3]. We posit this to be key to address BGP security. As such, in this abstract we propose an SDN architecture for secure routing.

Our solution — BGPSecX — is based on a Software-Defined Internet Exchange (as SDX [4], an SDN-based architecture targeting IXPs). Our design further includes secure channels between the BGPSecX of different IXPs that want to collaborate. The L2 nature of IXPs make them a good fit for SDN, and its growing importance (they number more than 350 today, and some carry as much traffic as global Tier-1 ISPs [5]) turns them into a compelling target. Recently, IXPs have started offering value-added services to their members — such as Route Server services — as a successful incentive to join. We see BGPSecX as an additional value-added service.

BGPSecX will include four security defenses against prefix hijacks. First, detection by means of ROA verification using a RPKI infrastructure. The RPKI provides a trusted mapping from allocated IP prefixes to ASes, and can thus be used to create a whitelist mechanism to filter hijacked routes. One problem of the RPKI is coverage, which is still small (less than 5% of all prefixes are mapped). This motivates the next techniques. Second, we include prefix filtering, another whitelist technique used to filter bogus announcements. The idea is for an AS to keep a list of prefixes announced by its customers (which is usually possible) and discard announcements of prefixes not on the list. The main challenge of this technique is the lack of incentives, as this technique does not protect an AS itself, but instead it protects the Internet from attacks by its own customers [1]. However, the secure channel will allow IXPs to communicate, and enable the creation of white lists of clusters of IXPs, which can be seen as a more attractive solution. Third, queries between IXPs will be used for validation of routing information (inspired by [6]). Fourth, we will explore the use of well-know anomaly detection mechanisms [2] and use them at an inter-IXP scale.

We believe our proposal to be capable of addressing the three fundamental problems mentioned in the beginning. First, by offloading control logic to the SDN controller we remove the computational burden from routers. Second, our solution does not require changes to the protocol as the techniques only require BGP messages to be intercepted. Finally, by offering BGPSecX as an additional value-added service from an IXP, we grant incentives for organizations to secure their interdomain routing. As IXP members use the service, positive network effects may be created increasing adoption by other members. Also, techniques that offer little value to the AS that implements them, such as prefix filtering, can gain further relevance at the scale of clusters of IXPs.

Implementation. We implemented a first prototype that mitigates prefix hijacking using a RPKI infrastructure, as a network application for both Floodlight and

ONOS. We are now in the process of validating our initial solution with the use of real BGP traces.

Acknowledgments

References

[1] S. Goldberg. *Why is it taking so long to secure internet routing?*, Commun. ACM (Sept. 2014).

[2] K. Butler et al. *A survey of bgp security issues and solutions.*, Proceedings of the IEEE (Jan. 2010).

[3] V. Koltronis et al. *Outsourcing the routing control logic: Better internet routing based on sdn principles.*, In HotNets'12.

[4] Arpit Gupta et al. *SDX: A software defined internet exchange.*, In SIGCOMM'14.

[5] B. Ager et al. *Anatomy of a large european ixp.*, In SIGCOMM'12.

[6] G. Goodel et al. *Working around bgp: An incremental approach to improving security and accuracy of interdomain routing.*, In NDSS'13.