Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. Laurent Vanbever
Networked Systems Group

BGP Verification without Specification

Semester Thesis Proposal

One of the biggest security problems of the Internet is BGP. It builds solely on trust and has no safety checks built-in whatsoever. Hence, issues, such as route leaks and hijacks, happen frequently [4] and can have devastating consequences [1, 5, 8]. These leaks are usually caused by simple misconfigurations or intentionally by malicious operators.

Over the years different approaches and BGP extensions (e.g., RPKI [2], BGPsec [7], DISCO [6]) have been proposed to prevent such attacks or weaken their impact on the global routing system. However, these proposals see very low adoption as they require global coordination and infrastructure. Also, they are only useful if a majority of the Internet's ASes participate.

In addition, there are well known best practices and guidelines for network operators that protect the local AS and prevent configuration mistakes of neighboring networks to propagate any further. Unfortunately, as recent incidents show, even large networks fail to have these basic mechanisms in place [8].

In this thesis, we aim to create a system that protects a single AS from accepting wrong, unusual, and unintended routes and prevents it from propagating them any further. To cause minimal disruption to the network operators' daily work, we intend to design the system in way such that the BGP configuration of the AS only has to be minimally changed. This is done by introducing a middle-man on every BGP session of the AS that intercepts BGP messages, analyzes them, and if necessary holds them back or discards them.

To this end, the system learns a statistical model of what a benign, usual announcement looks like (both incoming and outgoing). The model can rely on different announcement specific features (e.g., the announced prefix and its prefix length, the AS path and its length, the route origin, and the attached communities) and on network specific features (e.g., the egress location, the number of egresses, and the traffic statistics).

Based on the devised model and historical data, the system learns what announcements the AS usually receives and what it usually sends out to its neighbors. Hence, it can detect announcements that deviate from the norm (e.g., longer prefixes, different egress, or unusual origin).

When the system detects an unusual announcement, it has to decide what to do with the announcement: (i) let the announcement pass, (ii) drop it, or (iii) notify the network administrator.

Milestones

- Start by refreshing your BGP knowledge and getting familiar with current BGP security initiatives (RPKI [2], BGPsec [7], DISCO [6]), their shortcomings and best practices [8];
- Familiarize yourself with BGPStream [3], RIS Live [3] and Route Monitoring [9] and investigate the variability of announcements and their features over time;
- Based on the gained insights, devise a statistical model to classify usual and unusual announcements;
- Validate and evaluate your model.

Contact

- Rüdiger Birkner, rbirkner@ethz.ch
- Prof. Dr. Laurent Vanbever, lvanbever@ethz.ch

References

[1] BGPmon Network Solutions Inc. Massive route leak causes Internet slowdown. https://bgpmon.net/massive-route-leak-cause-internet-slowdown/.

[2] R. Bush, R. Austein, K. Patel, H. Gredler, and M. Waehlisch. Resource Public Key Infrastructure (RPKI) Router Implementation Report. RFC 7128, February 2014.

[3] CAIDA. BGPStream. https://bgpstream.caida.org/.

[4] Cisco. BGPStream - BGPMON. https://bgpstream.com/.

[5] CNET - CBS INTERACTIVE INC. How Pakistan knocked YouTube offline (and how to make sure it never happens again). https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/.

[6] Y. Gilad, T. Hlavacek, A. Herzberg, M. Schapira, and H. Shulman. Perfect is the Enemy of Good: Setting Realistic Goals for BGP Security. In *ACM Hotnets*, Redmond, WA, USA, 2018.

[7] M. Lepinski and K. Sriram. BGPsec Protocol Specification. RFC 8205, September 2017.

[8] The Cloudflare Blog. How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today. https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-internet-offline-today/.

[9] University of Oregon. Route Views Project. www.routeviews.org/.