Ph.D. Proposal: Improving the Security of BGP

October 31, 2023

1 Summary

- **Position:** Ph.D. student
- **Location:** Grenoble, France
- **Hosting university:** Université Grenoble Alpes
- **Hosting laboratory:** Laboratoire d'Informatique de Grenoble (LIG), DRAKKAR team
- **Supervision:** Martin Heusse, Andrzej Duda
- **Application deadline:** Nov. 30, 2023
- **Duration:** 3 years
- **Start day:** ASAP

2 Context

The Internet uses the Border Gateway Protocol (BGP) for global connectivity. BGP propagates prefix announcements between Autonomous Systemes (ASes) so that any host on the Internet can reach any other hosts. The important assumption in its operation is that all BGP speakers trust each other and consider all BGP announcements as valid. However, this assumption leads to attacks such as **prefix hijacking** or **route leaks** [1, 2, 3, 4, 5].

A route leak is "the propagation of routing announcement(s) beyond their intended scope".[1] RFC 7908 describes this type of events, covering both intentional and accidental injections of erroneous routing information. One of the well known hijacking incidents was the YouTube route leak by Pakistan Telecom in 2008,[2] which resulted in Internet-wide traffic diversions.

[1] RFC 7908 provides a complete taxonomy of route leaks.

[2] Pakistan Telecom was ordered to block YouTube so it originated its prefix for the YouTube IP address block, which leaked to the global Internet. As a result, the YouTube traffic was temporarily diverted to Pakistan.

Hijacking attacks have an important impact on availability and confidentiality of communications and network operators consider them as a common and persistent threat to the global Internet [6]. There are many reasons of the incidents—they can result from configuration errors (fat fingers), software bugs, or active malicious attacks, but all have their roots in the lack of authorization checks built into the BGP protocol.

Resource Public Key Infrastructure (RPKI) origin validation is the most advanced effort for protecting origins against prefix hijacking. RPKI associates public keys with IP prefixes.[3] ASes certify their IP prefixes through a binding with AS numbers: they cryptographically sign and publish authorizations in publication servers (also called publication points) using Route Origin Authorization (ROA) objects. A ROA is an RPKI object that certifies the authorization of an AS to originate a set of IP prefixes. An AS can query the ROAs in the public repositories and filter bogus BGP advertisments based on Route Origin Validation (ROV).

A resilient routing solution would require the validation of the full AS path and there are several approaches to achieve this goal. Seo et al. proposed Secure BGP (sBGP) that digitally signs both the prefixes and AS paths included in BGP messages [7]. Secure BGP is CPU intensive on border routers and requires modifications to the BGP protocol. BGPsec is an evolution of Secure BGP.[4] Similarly, it presents the same drawbacks as sBGP—it is CPU intensive on routers and requires modifications to BGP [8].

Gill et al. [9] revealed that the majority of network operators do not prioritize the use of secure routes in their routing policies. Taking this into account, Lychev et al. [9] showed that a secure BGP solution such as S-BGP and BGPsec has only meager benefits in partial deployment in contrast to the standardized solution, RPKI. Even worse, the need for a coexistence of plain and secure BGP implementation creates new attack vectors. On the one hand, malicious ASes may intentionally disable the use of the secure BGP for some routes, known as downgrade attack, and, thus, render the deployment of secure BGP useless for groups of ASes. On the other hand, the lack of consensus amongst ASes on where to place the security in the routing policy may cause the existence of multiple stable BGP states. Lychev et al. also showed that Tier-2 ASes initially adopting the secure protocol will provide better security than Tier-1 ASes.

A possible approach to **achieving trustful global routing** is to take advantage of advanced features of DNS (DNSSEC and DANE) to provide lightweight validation of BGP announcements. The goal of the PhD thesis is to analyze the existing solutions and explore a new scheme based on DANE/TLSA for signing BGP advertisements.

This thesis will tackle the problem using a four-step approach:

- Identify: you will read papers and current specifications (RFCs) to identify security threats.

[3] M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing", February 2012, RFC6480.

[4] M. Lepinski and K. Sriram, "BGPsec Protocol Specification", September 2017, RFC8205.

- Design: you will propose new approaches to improve the current state of the art by exploring the possibilities of DNS as a directory of public information.
- Prototype: you will develop prototypes to validate the proposed ideas.
- Evaluate: you will evaluate their performance and useability.

The Ph.D. program will take place within the framework of a collaboration with the Huawei Research Center, Paris.

3 Your profile

- Master's degree or equivalent in IT/CS/Telecom with the specialization in Networking
- Excellent knowledge of TCP/IP networking
- Good programming skills
- Proficiency in Debian/Ubuntu or other Unix-like operating systems
- Excellent written and spoken English
- Research experience is a plus
- Industry experience is a plus

4 What we offer

- The research team with a strong background in computer networking.
- Cutting-edge research topics.
- Collaboration with a top industry player.
- Publications at top conferences (e.g., Infocom, Internet Measurement Conference).
- Strong supervision.
- International and very dynamic team.

LIG laboratory is located in Grenoble, the capital of the Alps. It is a major French scientific and industrial center for computer science and applied mathematics. The city lies amidst three mountain ranges and offers an exceptional quality of life, with efficient public transportation and dedicated bikeways.

5 How to apply

Applicants should send a detailed CV along with a motivation letter, last diploma, transcripts of undergraduate and graduate studies to duda@imag.fr. Email subject must start with "[Ph.D. Application: Improving the Security of BGP]". References or letters of recommendation are appreciated.

References

[1] Pierre-Antoine Vervier, Olivier Thonnard, and Marc Dacier. Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks. In *22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2015*, 2015.

[2] Pavlos Sermpezis, Vasileios Kotronis, Petros Gigis, Xenofontas A. Dimitropoulos, Danilo Cicalese, Alistair King, and Alberto Dainotti. ARTEMIS: Neutralizing BGP Hijacking Within a Minute. *IEEE/ACM Trans. Netw.*, 26(6):2471–2486, 2018.

[3] Pavlos Sermpezis, Vasileios Kotronis, Konstantinos Arakadakis, and Athena Vakali. Estimating the Impact of BGP Prefix Hijacking. In *IFIP Networking Conference, IFIP Networking 2021, Espoo and Helsinki, Finland, June 21-24, 2021*, pages 1–10. IEEE, 2021.

[4] G. Huston. A Survey on Securing Inter-Domain Routing: Part 1. APNIC Blog, 2021.

[5] G. Huston. A Survey on Securing Inter-Domain Routing: Part 2. APNIC Blog, 2021.

[6] Pavlos Sermpezis, Vasileios Kotronis, Alberto Dainotti, and Xenofontas A. Dimitropoulos. A Survey among Network Operators on BGP Prefix Hijacking. *Comput. Commun. Rev.*, 48(1):64–69, 2018.

[7] Stephen T. Kent, Charles Lynn, and Karen Seo. Secure Border Gateway Protocol (S-BGP). *IEEE J. Sel. Areas Commun.*, 18(4):582–592, 2000.

[8] Qi Li, Jiajia Liu, Yih-Chun Hu, Mingwei Xu, and Jianping Wu. BGP with BGPsec: Attacks and Countermeasures. *IEEE Netw.*, 33(4):194–200, 2019.

[9] Phillipa Gill, Michael Schapira, and Sharon Goldberg. A Survey of Interdomain Routing Policies. *Comput. Commun. Rev.*, 44(1):28–34, 2014.