Measuring the propagation of BGP Hijacks

ALBERT WILLIAMS, University of Massachusetts Amherst
ARJUN SREEDHARAN, University of Massachusetts Amherst

KEYWORDS

Networks, Internet, Border Gateway Protocol, Autonomous System, Security

ACM Reference format:

Ben Trovato, G.K.M. Tobin, Lars Thørväld, Lawrence P. Leipuner, Sean Fogarty, Charles Palmer, John Smith, and Julius P. Kumquat. 1997. SIG Paper in word Format. *ACM J. Comput. Cult. Herit*. 9, 4, Article 39 (March 2010),4 pages.
DOI: 10.1145/1234

ABSTRACT

The Internet at its top level is an interconnection of Autonomous Systems. These Autonomous Systems exchange routing information using an honor system based on the Border Gateway Protocol (BGP). Over the last few years, we have been extensively witnessing misuse of this protocol by hijackers who want to intercept traffic that are not meant for them. It is in this context that we aim to find a way to identify these hijacks, measure them and come up with ways to mitigate them. We designed a data structure to easily record and analyze BGP data and devised a scheme to distinguish hijacks from benign overlaps. After analyzing BGP data over a period of 30 days, we found that 0.48% of all AS announcements 10.07% of overlapping announcements were potential hijacks. We also formulated a reliability score to be assigned to each Autonomous System to identify its propensity to mitigate BGP hijacks.

1 INTRODUCTION

The Internet's architecture relies on trust based peering arrangements between autonomous systems (AS) [1]. This honor system that uses Border Gateway Protocol is vulnerable to exploitation by malicious elements who could announce a range of IP addresses that do not belong to them [2].

In this project, we identify IP addresses/prefixes announced by multiple autonomous systems and try to establish a heuristic to decide which are hijacks. We then study the propagation of these BGP leaks. We also establish which autonomous systems are propagating paths to which conflicting origin, letting us decide which AS can reliably ignore hijackers and which should not be trusted to tell the difference. This is achieved by calculating a reputation metric for each AS. This can help neighboring ASs choose between competing destinations, mitigating the effect of a BGP hijack. In this document,

any two IP address prefixes are said to overlap or conflict if at least one address is contained in both of the prefix sets.

2 BACKGROUND AND RELATED WORK

The Internet is a complex network of networks. Each network here is a unit that is a collection of routers whose IP prefixes and routing policies are under common administrative control. These units are termed as Autonomous Systems. Autonomous systems use a standardized exterior gateway protocol named Border Gateway Protocol (BGP) to exchange routing and reachability information between them. In BGP, routing information is passed on to neighboring peers in the form of network prefix announcements. The AS that owns a range of IP addresses initiate an announcement. Using these announcements, ASs collect routing information from its neighboring ASs and propagate that information further. What routes are announced to what neighbors may depend on the business relationship between them.

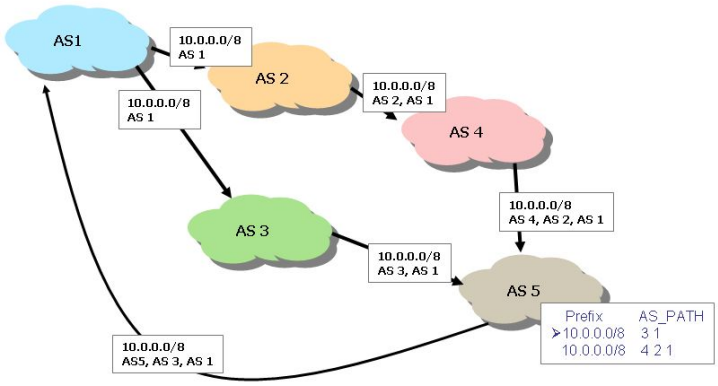

Figure 1. BGP prefix announcement example

To aid operators implement routing policies, BGP announcements carry extra data in addition to the announced IP address prefixes. In the context of this project, the most important piece of additional data is the Autonomous System path (AS path). AS path is the complete path listing which all ASs a packet would have to travel through to reach the AS that (claims to) own the IP prefix. Here's an example of how a typical BGP announcement would look like:

Type: *A (announcement)*
Peer address: *198.32.160.39*
Peer ASN: *9304*
Next hop: *198.32.160.39*
AS-Path: *9304 8928 5391 5391 9146 1299 50010 204170 204170 204170 204170 204170 204170 204170 204170 204170*

Karlin et al. (2006) describes a protocol preserving enhancement to BGP named Pretty Good BGP (PGBGP) that slows the dissemination of bogus routes and provides network operators time to respond before problems escalate into large scale Internet attacks. The key idea presented in this

paper is that routers should be cautious when adopting a route with new information, such as an unfamiliar origin AS [3]. They evaluated this idea on prefix and sub-prefix class of hijacks and showed that it is highly effective at blocking the spread of hijacked routes. It protected 97% of ASs from malicious prefix routes and 85% from bogus sub-prefix routes.

Theodoridis et al. (2013) presents an unsupervised method for detecting BGP hijacks. It puts to use features related to the frequency of appearance and the geographic deviation of each intermediate AS towards a given destination country. Their basis of their technique lies within the basic notion of statistically analysing the BGP activity on a per hosting country basis [4].

A real-time detection system to provide protection against bogus routes is proposed by Qiu et al. [5]. Their system leverages historical BGP routing data to detect suspicious routes comprised of unseen objects. They utilize a directed AS-link topology model to detect routes that violate import -export BGP routing policies. For documented incidents, their system claims to detect bogus routes with almost 100% detection rate and 0.02% false positive rates.

3 METHODOLOGY

We made use of the BGPStream[6] project to access BGP data and announcements over a period of 30 days were studied. In order to easily record and analyze overlapping BGP announcements, we designed a special data structure named *PrefixForest*. At the top level, *PrefixForest* is a list of *PrefixNode* objects. Each *PrefixNode* object contains one *Prefix* object which corresponds to the least specific (the shortest mask) IP address prefix that does not conflict with prefixes of other *PrefixNode* objects in the list.

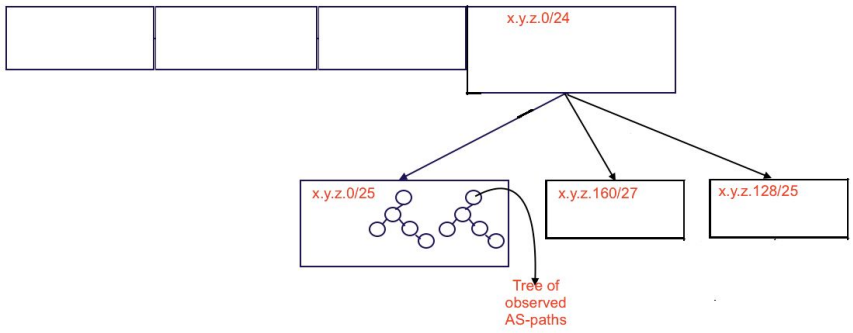

Figure 2. An example *PrefixForest* snapshot

The children of a *PrefixNode* are *Prefix* objects that conflict with it but have more specific IP prefixes. Upon seeing a new announcement, the top level list is checked to see if it conflicts with any of the prefixes already recorded. The information from the new announcement is merged into the existing Prefix object, or appropriately placed as the child of a top-level *PrefixNode*.

Each *Prefix* object contains:

1. The value of the address of the IP prefix (e.g. *178.20.16.0/21*) stored as an unsigned int.

(e.g. 2987659264 for *178.20.16.0*)
2. The length the IP prefix stored as an unsigned int. (e.g. 21 for *178.20.16.0/21*)
3. A list of *ASPathTree* objects (explained below)

An *ASPathTree* is a tree representing the announced AS-paths for a particular prefix originating from a particular AS (which would be placed a at the root of the ASPathTree).

For e.g. if there were 3 announcements received for the prefix *178.20.16.0/21* and they contained the following AS-paths:

701 28 902
321 28 902
239 37 168

Then the list of ASPathTree objects would look like the illustration given in figure 3.

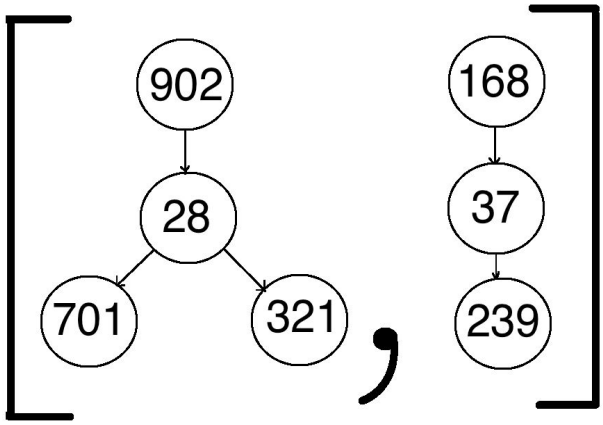

Fig 3. An example list of ASPathTree objects

With the *ASPathTree* in place, we'll be able to tell whose announcement each AS propagated for the same IP prefix. In the above example, *178.20.16.0/21* was announced originally by both AS 902 and AS 168. AS 37 propagated the AS path with AS 168 as the origin while AS 28 chose AS 902.

Our method to distinguish a BGP hijack is inspired by the basic idea embodied in *Pretty good BGP* [3]. In there, the system is wary of adopting a route with new information, such as an unfamiliar origin AS. On the same lines, we group overlapping BGP announcements using the *PrefixForest* data structure and collect all ASs from which they originate within a particular group. From this we spot outliers. We classify any AS that announces a majority of the overlapping prefixes as the legitimate origin, and any others as potential hijackers. We classify no ASs as hijackers if there is no AS appearing as the majority in the list of collected origins.

The next part of our work was to come up with a way with which downstream ASs could assess the reliability of upstream ASs. To that part, we devised a metric named *reliability score*. ASs are scored based on if they propagated the announcement of the hijacker or that of the original AS owning the prefix. In the *ASTree* data structure, all descendants of a hijacker AS would be penalized because they were responsible for propagating the hijack. If an AS has a reliability score of 1, it means the AS has never propagated a hijacker's announcement. A score of 0 means, it has never propagated the legitimate origin when presented with a conflict. This score reflects the trustworthiness of an AS from the perspective of downstream ASs.

4 RESULTS AND DATA ANALYSIS

BGP data between Aug 25 and Sep 24, 2017 were analyzed. Of all the AS announcements in this time period, we found that 0.48% of announcements were potential hijacks. Of just the overlaps detected during this time frame, 10.07% were found to be potential hijacks.

The large prevalence of BGP hijacks stresses the importance of having a reputation system based on which ASs can make better BGP routing decisions.

With the recorded data, after distinguishing between potential hijacks and benign overlaps origin nodes were tagged with this information and the *reliability score* metric (as defined in Section 3) was calculated for all Autonomous Systems. The cumulative distribution of reliability score is shown in figure 5.

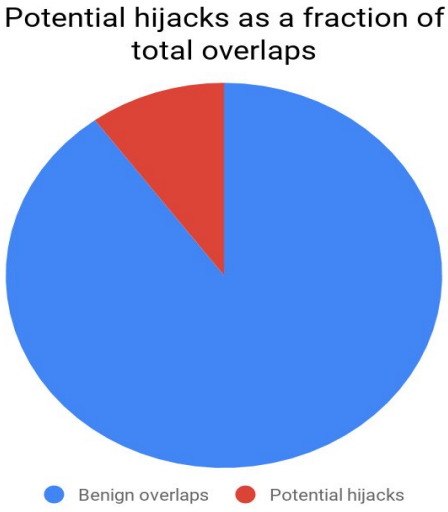

Fig 4. Potential hijacks Vs. Total overlaps

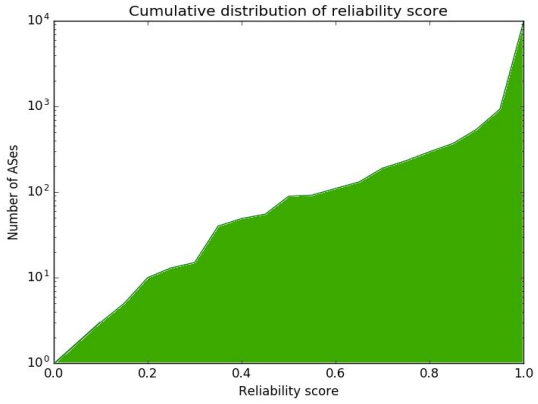

Fig 5. Cumulative distribution of reliability score

It was found that 99% of ASs had a reliability score of above 0.5 and 90% of ASs scored above 0.9 under this metric. 0.001% of ASs scored under a score of 0.2.

5 DISCUSSION

Our results throw light on the fact that a large number of hijacks happen in the Internet on a regular basis. Even though the limitations and vulnerabilities of BGP as an exterior gateway is well known in

the academic community, it is evident that not much has been done to mitigate attacks and prevent hijacks in the real world. There are about 40,000 ASs in the world today and to analyze announcements by all of them over a significant period take a mammoth effort. This is the reason for one of the notable limitations of our work. Our figures are derived from analyzing BGP data over 30 days. This may be deemed insufficient to draw strong conclusion about the nature of BGP hijacks in the Internet today. It was during our period of study that a large chunk of Japan's Internet went dark because of a routing error made by Google [7]. It is probable that such incidents affected the outcome of our study.

Notwithstanding the limitations, our results show that in the larger scheme of things BGP must be enhanced to empower ASs take better routing decisions, and *reliability score* could serve this purpose well.

6 CONCLUSION AND FUTURE WORK

We have found that BGP hijacks are widespread and one of the main reasons they propagate is because downstream Autonomous Systems do not have the ability to make good judgment. This paper provides a measurement of BGP hijacks occurring in the Internet and introduces a metric called *reliability score* that can be used by downstream ASs to assess the reliability of announcements received from upstream ASs.

We detect hijacks by finding outliers among AS origins of overlapping BGP announcements. This detection mechanism could be extended in the future by taking into account the relationship between ASs. See figure 6. If two ASs announcing overlapping IP prefixes are peers or have a provider-customer relationship, it is highly probable that this is merely traffic engineering in action. But it these two ASs in question have no relationship with each other, it could be a potential hijack.

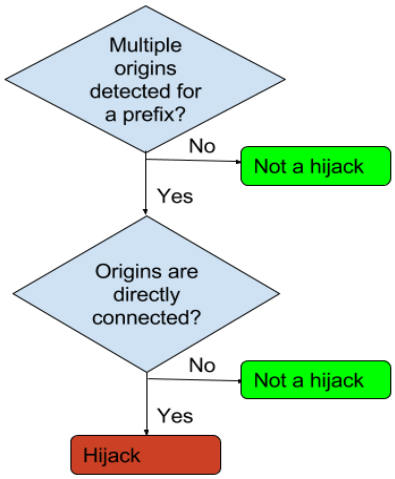

Fig 6. Detection of hijack using AS relationships

REFERENCES

[1] E. Zmijewski. The end of undetected BGP route hijacking. http://www.renesys.com/wp-content/uploads/2014/05/Linx851.pdf, May 2014.

[2] S. Goldberg. Why is it taking so long to secure internet routing? Communications of the ACM: ACM Queue, 57(10):56–63, 2014.

[3] J. Karlin, S. Forrest, J. Rexford, Pretty good BGP: improving BGP by cautiously adopting routes, in: Proceedings of IEEE ICNP, 2006.

[4] G. Theodoridis, O. Tsigkas, and D. Tzovaras, “A Novel Unsupervised Method for Securing BGP Against Routing Hijacks,” in Computer and Information Sciences III, E. Gelenbe and R. Lent, Eds. Springer London, 2013, pp. 21–29.

[5] J. Qiu, L. Gao, S. Ranjan, and A. Nucci. Detecting Bogus BGP Route Information: Going Beyond Prefix Hijacking. In Proc. SECURECOMM, 2007.

[6] C. Orsini, A. King, D. Giordano, V. Giotsas, and A. Dainotti. 2016. BGPStream: a software framework for live and historical BGP data analysis.

[7] “Google routing blunder sent Japan's Internet dark on Friday”. Richard Chirgwin, The Register. 27 Aug 2017. https://www.theregister.co.uk/2017/08/27/google_routing_blunder_sent_japans_internet_dark/