Poster: Traffic Engineering Security Implications

Renan Paredes Barreto
FURG
Rio Grande, Brazil
renan.barreto@furg.br

Leandro Marcio Bertholdo
UFRGS
Porto Alegre, Brazil
leandro.bertholdo@ufrgs.br

Pedro de Botelho Marcos
FURG
Rio Grande, Brazil
pbmarcos@furg.br

ACM Reference Format:
Renan Paredes Barreto, Leandro Marcio Bertholdo, and Pedro de Botelho Marcos. 2024. Poster: Traffic Engineering Security Implications. In *Proceedings of the 2024 ACM Internet Measurement Conference (IMC '24), November 4–6, 2024, Madrid, Spain.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3646547.3689672

1 Introduction

Traffic delivery is a fundamental aspect of Internet operations today. Internet applications have strict service requirements regarding latency, packet loss, jitter, and bandwidth to deliver the best user experience. Autonomous Systems (ASes) operators rely on expanding their connectivity options and manipulating route announcements using the Border Gateway Protocol (BGP) to achieve this goal.

For the first strategy, ASes connect to multiple transit providers, peer with Content Delivery Networks (CDNs), and interconnect at Internet eXchange Points (IXPs), trying to be as close as possible to ASes responsible for generating/receiving large traffic volumes. For the second strategy, network operators benefit from the multiple connectivity options the AS has to manipulate its prefix announcements to influence the route selection by other ASes. Network operators rely on inbound traffic engineering techniques such as AS-Path Prepend (ASPP), selective announcements, more specific announcements, and BGP action communities.

Each technique explores different criteria ASes use (BGP and IP protocols) to influence the decision of the route an AS will choose. For example, by using ASPP, the network operator will artificially make a route longer and, thus, less likely to be selected by other ASes. By disaggregating a prefix into more specific ones, the operator will benefit from the longest prefix matching (LPM) routers use to select routes. Selectively announcing a prefix to only a subset of the AS´ neighbors will restrict the set of alternatives other ASes have to send traffic to the AS originating the route. At the same time, BGP action communities allow the prefix originator to ask neighboring ASes to perform traffic engineering over that prefix.

While these techniques may achieve the AS´ traffic engineering goal, they may also increase routing security risks, more precisely, the prefix suitability of being hijacked or impacted by a route leak. For example, ASPP makes it easier for an AS to originate a shorter path [2]. Selective announcements reduce route diversity, making it easier for an AS to originate an invalid route. Finally, the prefix length may make it more or less suitable for a hijack due to the longest prefix matching of the IP protocol. Also, it directly impacts the routing table size and the overall complexity of route management.

We aim to investigate the security implications of each inbound traffic engineering technique and the AS´connectivity. We use the PEERING Testbed [4] combined with data and control plane measurements to offer systematical analyses of these aspects to achieve our goal. Our preliminary evaluation indicates that the AS´ connectivity and ASPP can directly impact security by increasing the likelihood and impact of a hijack.

2 Methodology

To evaluate the security implications of the traffic engineering techniques, we rely on the PEERING Testbed and control plane data from the RIS Live platform [3]. The testbed allows us to perform actual BGP announcements to its peers through different points of presence in research institutions and IXPs. Our experiments emulate a prefix-hijacking scenario and work as follows.

Experiment steps. Each round consists of emulating an AS originating a prefix, with or without using an inbound traffic engineering technique and with different connectivity levels, and another AS, with various connectivity levels, trying to hijack the prefix originated by the first AS. We start the experiment with the first AS originating the prefix. We call this step as the *regular announcement*. We then wait for 15 minutes for our announcement to propagate. During this time, we are using the RIPE RIS Live platform to monitor the propagation of our announcement. After the propagation period, for 40 minutes, we perform a series of ping measurements targeting various ASes/prefixes across the Internet while still collecting data from RIS Live. We also wait 2 minutes after the ping measurements to give time for any late ping reply. We aim to understand routing behavior when only the *regular announcement* is in place. Then, the second AS announces the same prefix using a different ASN as the originator. We call this step the *hijacking announcement*. We then repeat the same control and data plane measurements to understand the effectiveness of the hijacking attempt. Finally, the first AS performs a *mitigation announcement* (i.e., a more specific version of the prefix) to try to reduce the impacts of the prefix hijacking. Again, we collect control and data plane measurements similar to those in the previous steps.

Announcement criteria. For each scenario, we will announce the prefix using (or not) a given inbound traffic engineering technique and varying the connectivity level of the prefix originator and the attacker. When using ASPP, we will analyze the impacts considering different prepend sizes (i.e., 1, 2, 3). When using more specific announcements, we will investigate how the prefix length interferes with the success of the hijacking event. For the selective announcement case, we will restrict the prefix announcement to a subset of the existing AS connections. We also plan to evaluate using BGP action communities to limit/modify our announcements

IMC '24, November 4–6, 2024, Madrid, Spain

ACM ISBN 979-8-4007-0592-2/24/11
https://doi.org/10.1145/3646547.3689672

Table 1: Preliminary results for the control and data plane measurements.

Experiment configuration			Control plane monitors			Data plane targets		
Originator	Attacker	Prepend size	Total	Hijacked	Recovered	Total	Hijacked	Recovered
Amsterdam	GRNET	0	395	85 (21.52%)	75 (88.24%)	1682677	356119 (21.16%)	356119 (100%)
		1	397	142 (35.77%)	132 (92.96%)	1679636	762282 (45.38%)	762282 (100%)
		2	397	255 (64.23%)	244 (95.69%)	1678404	1282353 (76.40%)	1282353 (100%)
		3	396	381 (96.21%)	368 (96.59%)	1680564	1680564 (100%)	1680564 (100%)
GRNET	Amsterdam	0	381	320 (83.99%)	296 (92.50%)	1646449	1228879 (74.64%)	1228879 (100%)
		1	382	328 (85.86%)	305 (92.99%)	1635977	1313934 (80.31%)	1313934 (100%)
		2	382	329 (86.13%)	305 (92.71%)	1653106	1321587 (79.95%)	1321587 (100%)
		3	381	330 (86.61%)	306 (92.73%)	1664218	1333532 (80.13%)	1333532 (100%)

whenever available. For the connectivity level, we will analyze the impacts considering the number of upstream providers, presence at IXPs, peering sessions with CDNs, and distance to tier-1 providers.

Targets. We derive our target list from the latest version of the ANT IP Hitlist [1]. After probing it, we built a new list with approximately 2M replying addresses across 40K ASes.

Protocols. We perform our measurements using ICMP, TCP, and UDP to understand if the protocol impacts.

Identifying the ingress ports. On the PEERING testbed, it is possible to identify the ingress port of a packet by the interface MAC address. This allows us to identify whether a target has been hijacked as the legit´s and the hijacker´s ingress MACs are different. Thus, we capture all packets associated with our prefix during our experiments for analyses.

Measuring the security implications. In each round, we collect data and control plane information. We rely on data from the RIS Live platform for the control plane. We estimate our metric by analyzing the number of RIS monitors that changed their best route from the *regular announcement* to the *hijacking announcement*. We also measure the number of monitors that changed to the *hijacking announcement* and were "recovered" by the *mitigation announcement*. Analogously, we use the same principle to analyze the data plane impacts based on the responses to our ping measurements.

Ethics. None of our prefix announcements will interfere with actual traffic from real users, as the PEERING testbed has no clients. We will also add our contact information to our ping measurements to allow ASes to indicate that they do not want to be probed and rate-limit the number of requests per second so as not to cause overheads in our VPs or the target ASes.

3 Preliminary evaluation and next steps

We performed initial measurements using the ASPP technique and an IPv4 prefix to validate our methodology and gain preliminary insights. We used the Amsterdam and GRNET PEERING muxes because they were the more responsive ones in a previous round of evaluation. Using them, we emulated scenarios where the *regular announcement* has 0, 1, 2, or 3 prepends and considered the cases where each mux is the originator of the *regular announcement* or the attacker. Table 1 shows the preliminary control and data plane measurement results using ICMP. For our analyses, we considered only monitors/targets that were responsive in all steps of each experiment.

When we originate the prefix in Amsterdam, we observe that the prepend size directly relates to the impact of the prefix hijacking in the data and control plane measurements. When we originate the prefix at GRNET, there are two important aspects to highlight. First, there is (almost) no difference in the impact independently of the prepend size. This may indicate that Amsterdam already has shorter paths to the monitors/targets than GRNET, thus easing the hijacking process and indicating that connectivity is essential to routing security. Second, we observe approximately 20% of not hijacked monitors/targets, suggesting that these (or someone in the path) are choosing the route likely based on local preference. We plan to investigate these cases further in the future. Finally, announcing more specific prefixes is a suitable mitigation strategy.

Although all ping targets were recovered, not all monitors were, indicating that using control and data planes helps expand our visibility. There are two possible scenarios for this difference. First, there could be ASes hosting BGP monitors that were not targeted by our ping measurements. Second, many ASes have multiple border routers; thus, the hijack could affect parts of these ASes networks while other parts do not. We plan to investigate this further in the next steps of our work.

In the following steps, we plan to evaluate other muxes and investigate the impacts caused by the other traffic engineering techniques, their combination, and the connectivity aspects. We also plan to measure the security impacts for IPv6 prefixes and investigate the connectivity and geographical aspects of the monitors/targets affected (or not) by the attack. Finally, we intend to explore how using RPKI reduces the security impacts in our scenarios.

References

[1] Xun Fan and John Heidemann. 2010. Selecting representative IP addresses for Internet topology studies. In *ACM IMC 2010*. https://doi.org/10.1145/1879141.1879195
[2] Pedro Marcos et al. 2020. AS-Path Prepending: There is No Rose without a Thorn. In *ACM IMC 2020*. https://doi.org/10.1145/3419394.3423642
[3] RIPE NCC. 2024. RIS Live. https://ris-live.ripe.net/
[4] Brandon Schlinker et al. 2019. PEERING: virtualizing BGP at the edge for research. In *ACM CoNEXT 2019*. https://doi.org/10.1145/3359989.3365414