

ROUTE HIJACKING AND BGP SECURITY

Dr. George Y. Wu¹, Aravind Anbalagan²

Professor, Dept. of TCOM, George Mason University, Fairfax, VA, United States¹
Graduate Student, Dept. of TCOM, George Mason University, Fairfax, VA, United States²

ABSTRACT: Border Gateway Protocol (BGP) routes are vulnerable to hijack when one attacker falsely modifies the route and advertises it to the source. The attacker modifies the route so that they can add malicious routes and gain advantage of the data that is being routed. This paper discusses route hijacking in detail and about the various counter methods to prevent it. There are various cases when BGP route had been hijacked which has been discussed. There are other major security concerns to BGP in addition to route hijacking.

KEYWORDS: Route hijacking, Border Gateway Protocol

I. INTRODUCTION

BGP is an inter-domain routing protocol which enables exchange of routing information as “reachability” information between different networks on the internet. These different networks in a BGP domain is referred as an autonomous system. So mainly BGP is applied to enable communication between different autonomous systems which may run different routing protocols within themselves. It uses a path vector algorithm to find the most efficient path to the destination. It is important to note that BGP doesn’t transfer the data to the destination but instead finds the best path to the destination. Thus, whenever a network advertises its prefix to the neighboring autonomous system that runs BGP, it is called as BGP peering. Mainly BGP is used to find path to route data between ISP. Moreover, BGP remains the choice for core Internet interconnectivity.

BGP was designed based on implicit trust between all the participants and does not feature security mechanism to validate the routing updates exchanged. There have been several cases where security has been compromised in a BGP router core and poses a threat even today. The vulnerable nature of this protocol itself posed a threat in the form of route hijacks for the past two decades. This leads to a many scalability issues on the network such as for black-hole traffic attackers, DDoS, spamming and man-in-the-middle attacks.

II. ROUTE HIJACKING

Exploiting the implicit trust nature of the protocol, any autonomous system can be able to inject any random route into the routing system. Thus, whenever one network falsely advertises a set of prefixes to the other requesting for reachability, a route is hijacked. This is generally referred as route hijack and referred as IP hijack, BGP hijack and prefix hijack too. At the internet level this is carried out by configuring a malicious edge route that would peer to other BGP peers and

introduce a bogus route into the overall internet. This leads to steering traffic to the attacker's desire and moreover attacker can gain potential information from the data that is being routed. The routing information based (RIB) gets flooded with bogus information and this poisoned information would be shared to its peers as well. Propagation of these routes would affect the broader internet community with ease at no matter of time.

Attackers generally target unused prefixes at a regular interval of time for hijacking to avoid any attention from the legitimate owner. It is said that 20% of the whole of IPv4 address space is presently allocated but not above-board are announced. The unused space is the ideal thing for hijackers to exploit and carry out such malicious activities. Pictorial representation of BGP route hijack is explained as below:

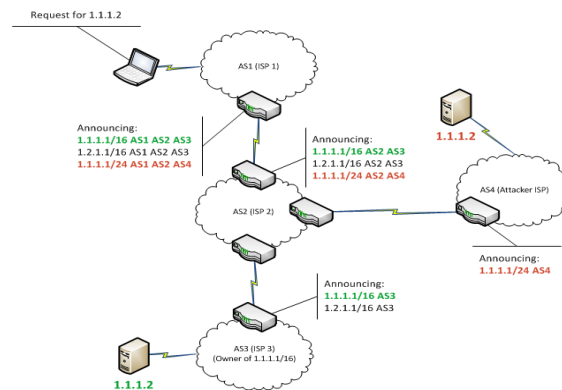


Figure 1: Route hijack in BGP

From the figure the Autonomous system (AS1) of ISP 1 requests a route to 1.1.1.2 with the help of its edge BGP router. The peer BGP router in AS2 (ISP2) propagates this information to the neighboring AS3 and AS4 with the help of its edge routers. The original route for the requested address is with AS3. But now an attacker in AS4 injects a more specific and newer prefix to AS2 which sends the advertisement to the requester in AS1. The consequence is that the data is steered from AS1-AS2-AS4. The attacker thus claims the information through the compromised advertisement sent. This is an example of how route hijack is performed in BGP.

The potential problems with route hijacking can be as follows:

- 1) The problem arises with scalability with different operating BGP networks as the data in the routing information bases increases.
- 2) The data can be tapped by any random person who advertises a false prefix which can result in potential damage.
- 3) The data is being rerouted to the attackers favor and has no control from the requester's end.
- 4) Man-in-middle attack can be performed by the attacker.
- 5) Existing methods to prevent prefix hijacks are still facing large-scale and deployment issues.
- 6) Attackers can even take control over cryptocurrency transactions.

III. SECURITY: DETECTING AND PREVENTING ROUTE HIJACKS

There have been several solutions to prevent route hijacks devised from the past, but the vulnerable nature of the protocol itself makes it difficult to endure from such attacks. The route hijacks are to be detected at the earliest to prevent the route from getting populated into the internet RIB (Routing Information Base). The existing approaches had deployment challenges and moreover the infrastructure of every autonomous system makes it lack a central authority. The conventional methods detected anomalies in the routes and monitored the stability of routers. But these methods weren't good to distinguish between this critical security issue from power shutdown events and submarine cable problems. Some of the other detection methods devised in the past were table-based. Taking the routing table of organizations and running the tests to identify prefix hijacks, but the problem was that the organizations weren't ready to provide the routing table.

Prevention mechanisms for prefix hijacks are still facing practicability issues due to large-scale deployment needs. Most of the approaches like S-BGP, Resource Publication Infrastructure (RPKI) are impractical and still needs to be refined to deploy in the internet.

The methods proposed by experts from recent studies to detect prefix hijacks are discussed here. Paper [1] uses two programs, first one is to search for suspicious Autonomous Systems and then passes the results to the second program. This program traces the behavior of routers using through their connectivity. From the behavior, we can be able to find out parameters such as direct and indirect neighbors, number of sender and receiver neighbors for both the victim and hijacker. Thus, two classes of data are separated as benign and malicious. The result of the detection method in finding route hijacks was accurate to 81%.

Method [2] uses an attacker model at the first phase to show the different attacks that BGP is facing now. This model classifies the reason and impact on the global routing table. From this we can assess the impact due to the prefix hijack attack. In the second phase a Hijacking Event Analysis Program (HEAP) is introduced. This is an automated program which acts as an extensive filtering system to figure out the routing attacks. Significant false positives in a set of major hijacking reports were identified.

Paper [3] makes use of a AS hijacking detection system that is used to accurately find events of hijack within a single AS. This tracking is real-time and it enables an alarm notification to the administrator along with the information of the attacker. This experiment could detect AS hijack with high accuracy, low detection latency and this must be implemented in the internet.

IV. MAJOR ROUTE HIJACK REPORTED

As said earlier prefix hijacks in BGP prevails from almost two decades back. There have been major catastrophic events in the past and some of the major ones are listed below:

According the survey done by Dell SecureWorks in 2014, Bitcoin miner's connection was rerouted to a mining pool server. The attackers took control of mining pool server and stole the

cryptocurrency used in transactions. The traffic was rerouted for almost 30 seconds for every session. This attack took place over a two-month period and collected around \$83,000.

One famous case in which the western government got involved was studied in July 2015. This was a result of breach in surveillance software provider Hacking Team which resulted in company's internal emails. From the emails, it was revealed that the Italian government in coalition with an Italian ISP joined with the Hacking Team to conduct BGP hijacks. When Command and Control server of the Hacking Team went down, the malware communicating with the server also went down. Falsely announcing the IP prefixes, Hacking Team gained access to the infected machines.

A case study done in 2013 by [4] about a case in Bulgaria that happened in December 2012. An actor named Mallory was incriminated on involvement with prefix hijacks and his intent was malicious. Symantec scanned spam network prefixes from Mallory. But there was a strong correlation between Mallory and Alice. Alice's sub-prefixes were intentionally sent by Mallory and this was claimed to be a spam. But later, scanning and investigation revealed that it was Mallory that did these route hijacks but the reason for it was not disclosed.

Another famous case happened in February 24, 2014. It was YouTube which was affected by Pakistan hijackers. The attempt to block the server and content within their nation reflected to shut traffic to the site globally.

V. BGP SECURITY

Cryptographic techniques for BGP security include pairwise keying, which is a method where the parties involved in routing data, exchange the keys for communication well in advance. Hash functions like Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1) are used to compute a fixed-length hash value from an input text. Message authentication codes are tags that is applied to messages for authenticity and integrity reasons. MAC is generated by taking a secret and message data and computing a tag. Diffie-Hellman key negotiation allows parties that doesn't even know about each other to share secret key. Public Key Infrastructure is a method where same key is shared between two routers exchanging data. This is not a safe solution and has certain flaws in it. Public Key Cryptography which is also called as asymmetric cryptography is a different key sharing between the speakers exchanging data.

Recent studies and research [5] on the security aspects of BGP have come up with architectures for BGP security. Flexibility provided to each user is increased and afforded to each user by S-BGP, soBGP and IRV which are currently under consideration by the IETF.

Secure BGP is referred as S-BGP, which is the first routing security solution for BGP. This solution validates the data routed between two autonomous systems using public key certificates. It supports a pair of PKI, where one PKI is used to authenticate addresses that are allocated and second PKI is used to bind AS numbers to organizations. These two PKIs are used to validate all information exchanged. Address attestations are provided to the prefixes and Route attestations are distributed within the information.

Secure Origin BGP which is referred as soBGP, allows flexibility between the security and the protocol overhead. This solution also provides a PKI for ensuring authorization and authentication between organizations. This holds three types of PKIs, one which is used to bind a public key to every router. The other two PKIs are used to provide policy and address attestations respectively.

Interdomain Route Validation (IRV) service is a least centralized solution for securing BGP. This is designed to be an independent operation from the routing protocol. Every data in the AS is queried and the storage and processing costs are eliminated. The UPDATE messages which are validated are chosen to an AS.

VI. REFERENCES

- [1] Hussain Alshamrani, Bogdan Ghita, Plymouth University, UK, “IP Prefix Hijack Detection Using BGP Connectivity Monitoring”, IEEE, ISBN: 978-1-4799-8950-8, Aug. 2016.
- [2] Johann Schlamp, Ralph Holz, Quentin Jacquemart, Georg Carle, and Ernst W. Biersack, “HEAP: Reliable Assessment of BGP Hijacking Attacks”, IEEE Journal, Vol. 34, No. 6, June 2016.
- [3] Chunxiu Li, Yujie Ma, Ke Li, Xin Li, Jiangang Zhou, Shanzhi Chen, “Detecting AS Hijacking in One Administrative Domain”, *ICCT*, 2013.
- [4] Pierre-Antoine Vervier, Quentin Jacquemart, Johann Schlamp, Olivier Thonnard, Georg Carle, Guillaume Urvoy-Keller, Ernst Biersack, Marc Dacier, “Malicious BGP Hijacks: Appearances Can Be Deceiving”, ISBN: 978-1-4799-2003-7, Aug. 2014.
- [5] Kevin Butler, Toni Farley, Patrick McDaniel, and Jennifer Rexford, “A Survey of BGP Security Issues and Solutions”, Aug. 2008.
- [6] <https://www.bishopfox.com/blog/2015/08/an-overview-of-bgp-hijacking/>
- [7] <https://blog.team-cymru.org/2016/01/bgp-route-hijacking-an-overview/>
- [8] https://en.wikipedia.org/wiki/IP_hijacking