A Brief Introduction to BGP Hijacking and Countermeasures

Peder Grundvold

May 25, 2021

1 Introduction

Today's Internet is not one single network but rather a network of networks. In a more formal definition can it be described as a collection of several autonomous systems (ASs). An AS is a group of networks with a unified routing policy, typically controlled by an Internet Service Provider (ISP) or a large organization such as a university or government agency. Technically is an AS defined as a collection of IP prefixes operated by the same entity. Each AS is managed with interior routing protocols, for instance, Open Shortest Path First (OSPF), but the different ASs also need to be connected. This is where Border Gateway Protocol (BGP) comes in.

BGP enables routing between different ASs; for instance, it enables a user in Japan to connect to a US-hosted server by finding a route encompassing several different ISPs. Furthermore, because the structure of the Internet is constantly changing ASs need to be kept up to date with information on new and obsolete routes. This is performed by each AS having a TCP connection, using port 179, to neighbouring ASs where BGP messages are exchanged.

The Border Gateway Protocol is largely based on trust, meaning enterprises believe that their ISPs are choosing the safest and most efficient path for their data. This was also the case for most protocols developed in the early days of the Internet when it was constrained to a handful of government and military institutions. However, unlike other protocols, and even with a large amount of research going into this, security has never been added to the official protocol specification. So despite its critical role in today's Internet, is the protocol not designed to provide any form of security guarantees[7]. This leads to several vulnerabilities, like hijacking attacks and route leaks.

In this article we will first discuss some known BGP attacks, using real-life examples. We will then look into countermeasure techniques that could hinder these earlier discussed attacks.

2 Problem Discussion

The two incidents discussed in this article are based on BGP hijacking. This attack is caused by ISPs (or other owners of ASs) lacking proper filtering of received prefix announcements before sending them to others. By using an ISP like this, a potential attacker can advertise any prefix to the ISP's peers. If the malicious announcement is more specific than the existing one or claims to have a shorter path, the traffic may be directed to the attacker.

2.1 Stealing Cryptocurrency using BGP Hijacking

First, we will discuss an attack where the adversary compromised an entire ISP by gaining access to edge routers, and in this way, we're able to send malicious BGP messages. In 2014 the Dell SecureWorks Counter Threat Unit™ (CTU) discovered an unknown entity repeatedly hijacking traffic using an attack based on BGP[6].

The victim was doing cryptocurrency "mining", which is the process of using large amounts of computational power to perform tasks to validate the transactions of other users. Completing these tasks will generate more of the given cryptocurrency, and this will be rewarded to the miner. However, in this case, when the victim went to the pool to find a new task the traffic was rerouted to a malicious pool maintained by the attacker. This meant that the victim continued to solve tasks without noticing any difference but the rewarded cryptocurrency went to the attacker.

Figure 1 shows a simple demonstration of the attack scenario. On the bottom right AS2 sends a legitimate BGP message saying that it owns prefix 1.1.1.1/16. On the bottom left AS3, which is controlled by the attacker, also sends a BGP message claiming to own the prefix 1.1.1.1/24. These two massages will then propagate further and reach AS1, and because the prefix from AS3 is more specific this will be prioritized by AS1 when routing to 1.1.1.2. This attack, according to CTU, successfully earned the adversaries an estimated $83,000, generated in the span of four months.

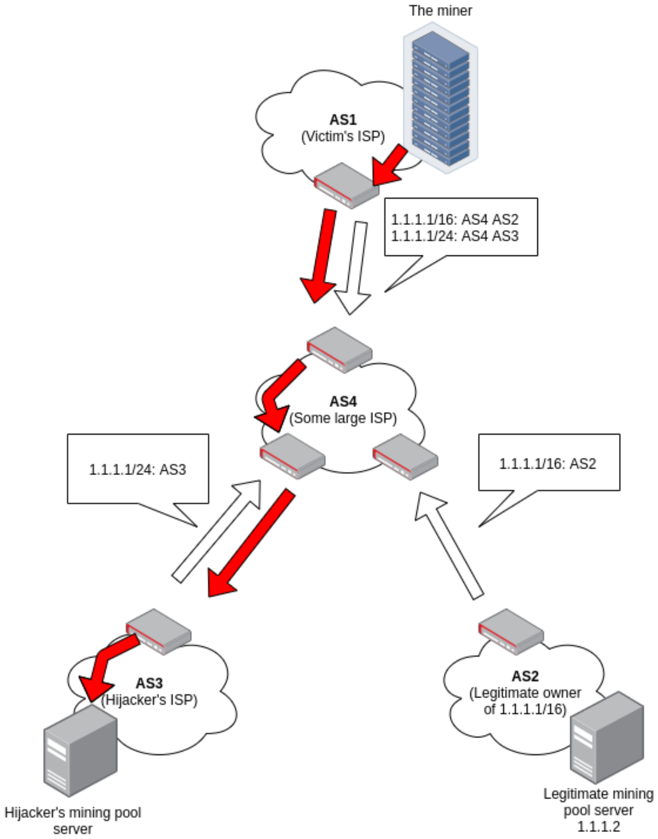

Figure 1: A BGP Hijacking Attack Scenario

2.2 Attack to Obtain Bogus Certificates from Top Certificate Authorities

Public Key Infrastructure (PKI) is a hugely important cryptographic mechanism for today's Internet. This provides confidentiality and integrity for users on the web by allowing domains to be publicly vetted (as indicated by the small padlock icon in front of an URL). On the Internet are Certificate Authorities (CAs) responsible for doing this vetting process, as well as issuing PKI certificates. However, in the paper "Bamboozling Certificate Authorities with BGP" researchers from Princeton University demonstrated how an adversary can use BGP to hijack traffic and trick a CA into issuing a bogus certificate to the adversary's domain[1].

The researchers show five different BGP hijacking attacks that were all successful in tricking real-life CAs. The simplest of these, named the traditional sub-prefix attack, is equal to the one discussed above. However, the final attack methodology they propose is very interesting, and it differs from the others in that it does not break the data-plane connectivity to the victim's domain. This makes it much harder to detect for both the victim and their ISP. Simply put, this attack does not say that your AS is the victim's AS. Instead, it announces that the fastest way to the victim is through your AS.

However, no matter which of these BGP hijacking methods are used, the process of tricking a CA is the same. An adversary sends a certificate signing request for a victim's domain to a CA. Then the CA will ask for proof that you are the legitimate owner of the victim's domain, typically by asking you to add a specific file to the server hosting that domain. After this, the CA wants to verify this by sending an HTTP GET request for let's say www.example.com/verify-file.html. Now the BGP attack is initiated and this request is routed to the adversary instead. This means that the request is sent to a server the adversary actually owns, and after answering the request a certificate is obtained stating that the attacker is the legitimate owner of the victim's domain.

2.3 Multiple Vantage Point Verification

The above-mentioned paper also lists Multiple Vantage Point Verification as a possible countermeasure to prevent BGP hijacking attacks. This method, and how it was deployed by the major CA Let's Encrypt, is further described in another paper by the same authors[2]. The idea is quite simple; because it is highly unlikely that an adversary has control of multiple ASs, the CA will use multiple vantage points in several different ASs when performing the domain verification process. The researchers also presented multiVA; the first real-world deployment of the multi-vantage-point countermeasure. This solution includes an algorithm to strategically select vantage points to maximize security and a method for complying with the CA/Browser Forum Baseline Requirements[3].

2.4 RPKI

Another promising countermeasure is Resource Public Key Infrastructure (RPKI), defined in RFC6480[5]. This framework, made by the IETF, cryptographically signs records to associate a BGP route announcement with the correct originating AS number[8]. Notice that, as with the aforementioned vetting of domains, this solution is also based on PKI.
How it works is similar as well; using RPKI all BGP update messages are signed and routers are therefore able to verify incoming messages using a Route Origin Authorization (similar to a CA in domain verification). A situation where a malicious update message is rejected by an ISP using RPKI is shown in Figure 2.

There has been interesting development around RPKI in recent years. In February of 2020 a group called Mutually Agreed Norms for Routing Security (MANRS) announced a task force specifically made to help content delivery networks and other cloud services implement security checks to harden BGP. RPKI is one of the main mechanisms they promote.

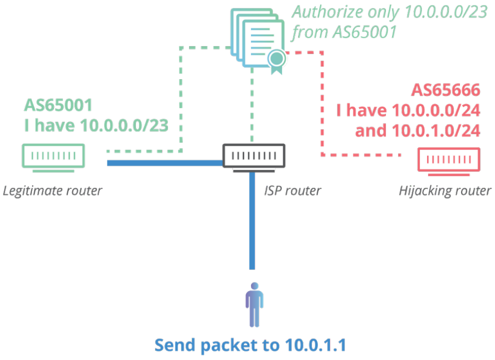

Figure 2: RPKI in Action[4]

3 Conclusion

The Border Gateway Protocol is of vital importance to the internet, and with this also important for most people's everyday life. Yet, almost no one has any idea of its existence. The two attacks earlier discussed highlights how vulnerable this protocol is, and how dire the consequences of such attacks can be. However, unlike other areas of internet security, there is nothing the average consumers can do to mitigate this risk. This is because BGP only operates between different ISPs and other large organizations. Fortunately, an increasing number of the word's ASs are implementing security countermeasures such as those discussed in this paper. But there is still a large part of ASs that are vulnerable, and we as consumers are responsible for holding our ISPs accountable. To facilitate this, Cloudflare, a major web infrastructure company, have developed a tool where users can test the BGP security of their ISP. It is as simple as going to https://isbgpsafeyet.com/ and clicking "Test your ISP". This is a very helpful step to increase the awareness around such an important mechanism of the Internet.

My ISP is secure, is yours?

References

[1] Henry Birge-Lee et al. “Bamboozling certificate authorities with {BGP}”. In: *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 2018, pp. 833–849.

[2] Henry Birge-Lee et al. “Experiences Deploying Multi-Vantage-Point Domain Validation at Let’s Encrypt”. In: ().

[3] CA/Browser Forum. *Baseline requirements for the issuance and management of publicly-trusted certificates*. Tech. rep. Aug. 2020.

[4] Jérôme Fleury and Louis Poinsignon. *RPKI and BGP: our path to securing Internet Routing*. `https://blog.cloudflare.com/rpki-details/`. Accessed: 2021-4-15. Sept. 2018.

[5] Matt Lepinski and Stephen Kent. “An infrastructure to support secure internet routing”. In: (2012).

[6] Pat Litke and Joe Stewart, Dell SecureWorks Counter Threat Unit. *BGP Hijacking for Cryptocurrency Profit*. `https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit`. Accessed: 2021-4-14. Aug. 2014.

[7] Asya Mitseva, Andriy Panchenko, and Thomas Engel. “The state of affairs in BGP security: A survey of attacks and defenses”. In: *Comput. Commun.* 124 (2018), pp. 45–60.

[8] Matthias Wählisch, Olaf Maennel, and Thomas C Schmidt. “Towards detecting BGP route hijacking using the RPKI”. en. In: *Comput. Commun. Rev.* 42.4 (2012), pp. 103–104.