BGP Prefix Hijacking Attack and its Prevention Methods

Afif Abugharsa
Department of Computer Networks, Misurata University, Libya
Email:afif.abugharsa@gmail.com
Bashir Elkharraz
Department of Computer Networks, Misurata University, Libya
Email: bashir.elkharraz@it.misuratau.edu.ly
Eltohami Elghoul
Department of Computer Networks, Misurata University, Libya
Email: e.elghoul@it.misuratau.edu.ly

ABSTRACT

The Border Gateway Protocol (BGP) is an Internet routing protocol that is widely used. With the introduction and implementation of various security features to prevent attacks and alleviate routing instabilities, BGP remains vulnerable due to the lack of integrity and authentication of BGP messages. BGP operations are highly dependent on its security, and attacks against BGP have a detrimental effect on packet forwarding. Given the importance of BGP security, Two techniques to improve BGP session security have been studied in this project to improve secure Internet routing, this project describes BGP prefix hijacking attack and its cause and the way to prevent it. The project studies BGP prefix filtering and Resource Public Key Infrastructure (RPKI), to prevent BGP from malicious attacks and misconfigurations. BGP prefix filtering is operationally deployable and very effective to improve BGP security problems. RPKI a specialized Public Key Infrastructure (PKI), was developed. It makes use of cryptographically verifiable statements to ensure that Autonomous Systems (ASes) and the owners of Internet resources are certifiably linked to the routing information they generate, resulting in a trusted routing origin..

Keywords –**Border Gateway Protocol, BGP HIjacking, BGP Prefix, RPKI Validation, BGP RPKI.**

Date of Submission: June 30, 2024 Date of Acceptance: July 31, 2024

I. INTRODUCTION

The main protocol for Internet routing is the Border Gateway Protocol (BGP) [17]. Any ISPs or networks on the Internet depend on the BGP protocol. back in 1989 When BGP developed it was not seen in terms of security. The Border Gateway Protocol (BGP) was developed and designed before the Internet environment became subject to attacks, exploits, and routing vulnerabilities. Today, we know that the Internet is a place full of malicious users who try to profit from the break-up of the internet. For malicious users, BGP is an open door. When you access a BGP peering, it is not difficult to borrow another IP space. This is called a BGP Hijacking [16]. Without the BGP protocol, networks of different ISPs and institutions could not communicate with one another in a cost-efficient manner. However, the BGP protocol has not been designed with security in mind. The weakness of security makes it potential to perform BGP hijacks. A BGP prefix hijack can be described as advertising Internet Protocol (IP) prefixes or even Autonomous System Numbers to neighboring routers that won’t belong to the advertiser. The detection of hijacked prefixes and AS numbers has been subject to several research papers and projects. These attacks and errors cause serious effects that propagate through the network resulting in potentially disastrous routing. These attacks may include modifying, deleting, forging, or duplicatingupdate messages, session hijacking, Distributed Denial of Service (DDoS) attacks, or IP spoofing. Malicious attacks alone do not account for all security issue's non-purpose and accidental errors also contribute to network instability known as BGP leaks.

II. RELATED WORK

This section highlights various papers that address different aspects of BGP and its security. In the paper [1] which addresses the critical issue of BGP hijacking, where an attacker manipulates BGP routing announcements to redirect traffic to unauthorized destinations. The authors propose an alert system that monitors BGP updates and analyzes routing data to detect anomalous behavior indicative of hijacking. Another research paper referenced as [2] presents a comprehensive resource for understanding and implementing routing protocols. The guide offers valuable insights into various routing protocols, their functionalities, and their application in network environments. The paper cited as [3]. is a comprehensive study guide and lab manual specifically designed for cisco exploration. The book provides a hands-on approach to learning routing protocols and concepts, offering a range of practical lab exercises that reinforce theoretical knowledge. It covers fundamental topics such as routing protocols, subnetting, network design, and troubleshooting. The book [4] provides a foundational guide for understanding the principles and mechanisms of IP routing, focusing specifically on Cisco's routing technologies. It covers essential concepts such as IP addressing, routing protocols, routing tables, and the configuration and operation of Cisco routers. With clear explanations and practical examples, Macfarlane provides readers with a solid understanding of how IP routing works and how to configure and troubleshoot routing within Cisco networks. In the paper referenced as [5], offers a comprehensive introduction to IP routing within Cisco systems. The book serves as a foundational guide for understanding the principles and mechanisms of IP routing, the book cited as [6] serves as an essential resource for understanding routing protocols and concepts, providing in-depth coverage of topics such as routing fundamentals, IP addressing, subnetting, and dynamic routing protocols. The paper [6] is a comprehensive guide that emphasizes a top-down approach to network design. The book provides a holistic perspective on network design, covering various aspects such as business requirements, application requirements, technology choices, and network infrastructure. The study [7] focuses on a case study analysis of BGP and specifically examines the issues of prefix hijacking and transit autonomous system. The research [8] presents a guide on implementing BGP Resource Public Key Infrastructure to enhance the security of the Internet. BGP RPKI is a system that allows Internet Service Providers and organizations to validate the ownership of IP address prefixes, reducing the risk of prefix hijacking and route leaks. The study [9] provides an extensive survey of anomaly detection techniques specifically focused on the BGP. The research [10] focuses on exploring BGP hijacking, a malicious activity where an attacker manipulates BGP routing announcements to redirect network traffic to unauthorized destinations. The paper [11] presents a meta-analysis of BGP threats and security measures, aiming to identify common vulnerabilities and propose new directions for practical BGP security. The study involves an in-depth examination of existing research papers, reports, and industry standards related to BGP security. The paper [12] presents complex peering and transit networks. BGP is a critical routing protocol used to exchange routing information between autonomous systems (ASes) on the Internet. In complex peering and transit networks, where multiple ASes interconnect, BGP security becomes crucial due to the potential for various attacks and vulnerabilities. The paper [13] discusses various risks related to BGP, including route hijacking, route leaks, and misconfigurations. It highlights the potential impact of these risks on network availability, integrity, and confidentiality. The paper [14] focuses on the detection of IP prefix hijack events, which involve the unauthorized rerouting of IP prefixes, potentially leading to security and connectivity issues. This paper [15] studies the circular dependency problem from an evolutionary game theory perspective. We model the strategy evolution of ASes choosing to deploy signing alone, deploy filtering alone, or deploy both signing and filtering. The results show that when the deployment rates of signing and filtering reach a certain range, the evolution can reach an ideal deployment state at a faster speed. The paper [16] proposes to detect anomalies by having the convolutional autoencoder (AE) learn the first-order difference values of time-series data of AS hegemonies under normal conditions. Finally the research [17] analysis BGP convergence based on keepalive and hold timers. In addition, the paper considers the most important interval of route advertisement and update delay.

III. BGP HIJACKING

The BGP is a protocol that allows ASes to communicate routing and reachability information. When routers create a BGP peering relationship, they trust each other by default. As a result, every IP prefix that a router announces is accepted by its neighbors. However, the Internet is not always ideal, an unauthorized network can create IP prefixes that belong to other networks in order to redirect traffic to the unauthorized network. BGP hijacking is the term for this process. There is no prefix or routing information received from an authorized peer that can be verified. Furthermore, there is no guarantee that the routing information received is unaltered. incorrect routing information will travel peer to peer, disrupting the greater network scale BGP does not check whether the prefixes advertised in an update message are owned by the advertiser or permitted by the owner to advertise them by default. Finally, there is no default validation technique for the path attribute of received prefix information. The original prefix advertisement may be disrupted if the BGP path property is changed [10].

IV. BGP PREFIX HIJACKING

Prefix hijacking takes place when an AS falsely claims ownership of a prefix that it does not actually possess. The intention behind this deceptive action is to divert traffic destined for the hijacked prefix towards the AS responsible for the hijacking. This malicious behavior is enabled by the fact that BGP does not require any confirmation of prefix ownership before an AS can advertise its ownership of a particular prefix.

In the context of prefix hijacking, the AS executing the attack typically selects the route to the hijacked prefix based on the criterion of having the fewest number of hops. By manipulating the routing information, the attacker aims to attract traffic towards their network and intercept communication intended for the legitimate owner of the prefix.

V. ROUTE ORIGIN AUTHORIZATION (ROA)

The BGP RPKI architecture heavily relies on the concept of Route Origin Authorizations (ROAs). These ROAs serve as objects that enable the verification of whether an Autonomous System (AS) is authorized to originate a specific IP prefix along with its associated subnets. Each ROA consists of four essential components:

1. Prefix: This component represents an IPv4 or IPv6 prefix with a specified length. Typically, it corresponds to a prefix assigned by a Regional Internet Registry (RIR) to a National Internet Registry (NIR), Local Internet Registry (LIR), or Internet Service Provider (ISP).
2. Maximum Mask Length: The maximum mask length specifies the permissible range of IP subnets that can be published from the originating prefix. It determines the level of granularity for the authorized subnets.
3. AS Number: This component identifies the Autonomous System (AS) that has been granted permission to originate the specified IP prefix or any of its permitted subnets. It denotes the AS authorized to announce the routing information.

To ensure the integrity and authenticity of the ROAs, a public/private key system is employed. Digital signature approaches are utilized to create and verify these signatures, thereby providing a secure mechanism for validating the authorization and ownership of IP prefixes within the BGP RPKI architecture.

VI. Preventing IP Prefix Hijacking using RPKI

The RPKI, proposed by the IETF, serves as a framework for enhancing the security of the inter-domain routing system. It employs three key security techniques, namely PKI, signatures, and positive attestations, to safeguard BGP and mitigate IP prefix hijacking. Within this system, ASes are capable of generating their own private and public keys through the PKI. These keys are then used for signing ASes, IP prefixes, and performing route verification. Positive attestations, employed by ARP, are used to validate the Route Origin Authorizations (ROAs) within the RPKI.In practical terms, the RPKI is designed to enhance the security of the hierarchical structure of delegating prefixes and ASes. The primary objective of this approach is to accurately identify the true owner of an IP address, thereby preventing misconfigurations and hijacking attempts. The subsequent subsections delve into the details of the RPKI mechanism and how to effectively defend a specific address space

VII. SIMULATION AND RESULTS

This scenario consists of two main parts. The first part focuses on investigating the BGP Hijacking attack, while the second part involves a study conducted in a simulated environment using PNETLAB to explore security solutions against this attack. The study primarily examines the effectiveness of BGP prefix filtering and RPKI as prevention methods for BGP prefix hijacking, as depicted in Figure 1..

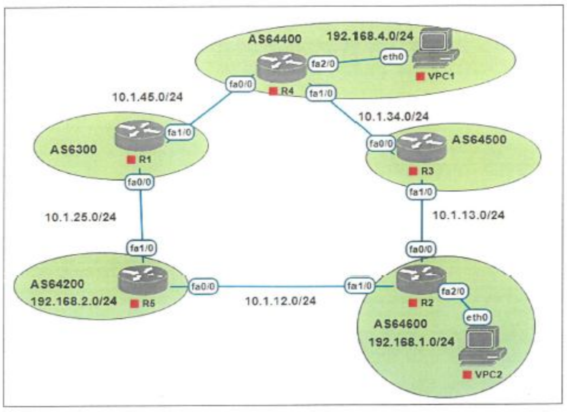

Fig. l. BGP Topology

In the first scenario of BGP hijacking, we set up a network topology using the eBGP protocol with different AS numbers and prefixes. During this setup, when one of the peers announces an IP and prefix that actually belongs to another peer, the hijacking occurs. This happens because the best path selection mechanism directs the packets to the attacker peer. Similarly, hijacking occurs when we announce a more specific prefix compared to the original peer.

In the second scenario, we implemented an AS-path filter to only allow specific path prefixes for advertisement and routing. This configuration ensures that the peer sends and receives data only through a predetermined route path and rejects any announced routes from other neighbors, thereby preventing hijacking.

Furthermore, we employed the "Filter Own Prefixes" approach, which involves accepting only specific prefixes with a length of /24 and discarding all other announced prefixes to protect against BGP path hijacking. Additionally, we implemented a filter to block all traffic originating from a particular AS number, which serves as a preventive measure against potentially malicious peers on the internet.

VIII. BGP HIJACKING TEST SCENARIO

The study considers the first scenario, where we configured network topology using eBGP protocol with a different AS numbers & prefixes, when one of the peers announces the same IP and prefix that belongs to another peer the hijacking accrues based on best path selection and the packets go to the attacker peer, this also happens when we announce the more specific prefix than the original peer can rely on RPKI to drop invalid announcements, though it acknowledges the possibility of misconfigurations still occurring.In the second scenario, we used an AS-path filter to allow only specific path prefixes to advertise and route, which makes the peer only sending and receiving from a specific route path and denies any Hijacking announced routes from other neighbors Also, we used Filter Own Prefixes and Accept only specific Prefixes with Length /24 and drop all other prefixes announced to hijack the BGP path, the last type of filter is blocking all traffic from specific AS number that might prevent malicious peers on the internet. Finally, we Implementation RPKI Scenario. In this scenario, we installed and configured RPKI and Routinator server. then we connected the server whit the network topology using an RTR session to validate BGP routes using RPKI, which makes routers read all registered addresses and AS numbers up to date from the RPKI server also RPKI gives routers validation details for each path in the BGP table protecting them from any invalid routes or unknown routes, we did announce valid, invalid and unknown routes in the scenario and all of them readed from the RPKI server immediately as the same validation state. The results can be observed from Table 1 which shows RPKI validation states based on prefixes that announced from BGP neighbors as their status.

Table 1 RPKI validation status

Router name	prefixes	Origin AS	RPKI status ROA	Action
R1	61.45.248.0/24	135533	Valid	Pass
R2	61.45.249.0/24	135534	Valid	Pass
R5	61.45.255.0/24	135540	Invalid	Drop
R5	203.0.113.0/24	135540	NotFound	Drop

IX. CONCLUSION AND FUTURE WORK

The study primarily focuses on addressing the issue of BGP prefix hijacking and explores preventive measures to mitigate this problem. The case study employs a small-scale simulation lab topology to illustrate how the hijacking occurs and subsequently implements solutions to counteract it. To prevent BGP prefix hijacking, it is crucial for network engineers in each ISP to implement prefix filtering, both on ingress and egress. This filtering ensures that only the expected prefixes are received from and advertised to BGP peers. However, this solution may face scalability challenges due to the need for implementation on every router running BGP. Additionally, the study investigates the effectiveness of Resource Public Key Infrastructure (RPKI) as a prevention method against BGP prefix hijacking. The analysis demonstrates that RPKI has shown significant success, particularly as the quality of data has improved over the years of its use. The study suggests that operators can rely on RPKI to drop invalid announcements, though it acknowledges the possibility of misconfigurations still occurring.

In the future, the research aims to achieve two main objectives. Firstly, it seeks to extend the previous study to explore other prevention methods against BGP prefix hijacking attacks, encompassing various types and technologies. Secondly, the research intends to examine other types of attacks targeting the BGP protocol, such as Distributed Denial of Service (DDoS) attacks.

.

REFERENCES

[1]. J. Schutrup, B. Borch.” BGP Hijack Alert System" Universiteit van Amsterdam System and Network Engineering, Holland, 7 February 2016.

[2]. Routing Protocols Companion Guide,cisco press, Jun 1, 2011.

[3]. A.Johnson. " Routing Protocols and Concepts CCNA Exploration Labs and Study Guide Instructor Edition" Cisco Press, Jun 1, 2011.

[4]. J.Macfarlane." Network Routing Basics Understanding IP Routing in Cisco Systems" Wiley Publishing, Inc., Indianapolis, Indiana,April 21, 2006.

[5]. R.Graziani, A.Johnson.” Routing Protocols and Concepts CCNA Exploration Companion Guide" Cisco Press, Dec 6, 2007..

[6]. P.Oppenheimer ."Top-Down Network Design Third Edition" Cisco Press, Aug 24, 2010.

[7]. R.Hakimi, Y.Saputra, B.Nugraha. "Case Study Analysis on BGP: Prefix Hijacking and Transit AS" IEEE International Conference on Telecommunication Systems Services and Applications (TSSA’16)At: Bali, Denpasar, Indonesia, 6-7 Oct. 2016.

[8]. F.Luciam, T.Tofoni, " For a safer Internet BGP RPKI: instructions for use" 27 CTO of Namex (Roma IXP), Manrs, Mar.2020.

[9]. B. Musawi, P. Branch. G,Armitage. " BGP Anomaly Detection Techniques: A Survey" IEEE Communications Surveys & Tutorials, IEE,, October 2016.

[10]. BORDER GATEWAY PROTOCOL Lab 13: BGP Hijacking ,http://ce.sc.edu/cyberinfra/workshops/Material/BGP/Lab%2013.pdf, 03-DEC-2020.

[11]. T.ROSSUM.” BGP security and the future: A meta-analysis of BGP threats and security to provide a new direction for practical BGP security" Delft University of Technology, Holland, 2020-OCT-15.

[12]. M.Khalid, Q.Nazir. "Security Issues of BGP in Complex Peering and Transit Networks" Halmstad University, Halmstad, Sweden, Dec 2008.

[13]. Risks and mitigation options of the Border Gateway Protocol (BGPJ,https://www.ria.ee/sites/default/files/ria ohuhinnang bgp en.pdf, June 2020.

[14]. H. Alshamrani, Hameed. " Detecting IP prefix hijack events using BGP activity and AS connectivity analysis" University of Plymouth,UK, February 2017.

[15]. M. Zeng, X. Huang, P. Zhang, D. Li and K. Xie, "Improving Prefix Hijacking Defense of RPKI from an Evolutionary Game Perspective," in *IEEE Transactions on Dependable and Secure Computing*, doi: 10.1109/TDSC.2024.3371644.

[16]. K. Nakashima, M. Harayama and M. Mishima, "Detection of BGP Hijacking based on AS Hegemony," *2024 International Conference on Electronics, Information, and Communication (ICEIC)*, Taipei, Taiwan, 2024, pp. 1-4, doi: 10.1109/ICEIC61013.2024.10457231.

[17]. A. Abaid, M. Hraib, A. B. Ghazzi and S. Sati, "Convergence Time Analysis of Border Gateway Protocol Using GNS3," *2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA*, Tripoli, Libya, 2021, pp. 689-694, doi: 10.1109/MI-STA52233.2021.9464522.

Authors Biography

Afif Abugharsa: Afif Abugharsa is an accomplished author and academic specializing in information technology. He holds a BSc degree (2007) and an MSc degree (2012). With a strong passion for technology and research, Afif has made significant contributions to the academic community, including presenting his work at the prestigious IEEE conference, MI-STA, held in Libya in 2024. In addition to his research, Afif serves as a dedicated Teaching Staff member at Misurata University's Faculty of Information Technology, where he mentors and guides students in their IT education..

Bashir Elkharraz Elkharraz is an accomplished author and academic specializing in information technology. With a BSc degree in 2003 and an MSc degree in 2011, he has consistently shown a passion for technology and a dedication to advancing knowledge in the field.

As an esteemed member of the Teaching Staff at Misurata University's Faculty of Information Technology, Elkharraz has made significant contributions to the academic community through his research and publications. His expertise and commitment to education have positively influenced the development of aspiring IT professionals.

Eltohami Elghoul: Elghoul is a highly skilled author and academic who specializes in the field of information technology. Having obtained a BSc degree in 2003 and an MSc degree in 2011, he has consistently shown a deep passion for technology and research during his professional journey. As an esteemed member of the Teaching Staff at Misurata University's Faculty of Information Technology, Elghoul holds a pivotal position in shaping the education and development of students within the field. With his extensive expertise and unwavering commitment, he provides invaluable knowledge and mentorship to aspiring IT professionals.