# IP Prefix Hijacking and Available Solutions

Prashant D. Londhe
Department of Computer Science,
Gogate Jogalekar college,
Ratangiri

Sanil C. Savale
Department of Computer Science,
Gogate Jogalekar college,
Ratangiri

Ketan G. Jogalekar
Department of Computer Science,
Gogate Jogalekar college,
Ratangiri

## ABSTRACT

IP prefix Hijacking is an issue regarding to Computer Network. IP Prefix Hijacking can be defines as illegitimate takeover of groups of IP addresses by corrupting Internet routing tables. Prefix hijacking is a type of network attack that can give malicious parties access to untraceable IP addresses. The IP Prefix identifies the number of significant bits used to identify a network. IP Prefix defines how many bits are reserved to represent network and how many bits are reserved to represent host. IP hijacking is the illegitimate takeover of groups of IP addresses by corrupting Internet routing tables. It is also known as BGP hijacking, Prefix hijacking or route hijacking. This paper gives demonstration of IP Prefix Hijacking and Discusses on Solutions available. This paper discusses on Types of IP prefix Hijacking.

**General Terms and Keywords**: IP Prefix, AS, BGP.

## 1. INTRODUCTION

In Today's Life, Internet is treated as best medium for Communication. Internet can be defined as Networks of Network. Network is formed by connecting two or more machines with each other. As they are now connected, so they can make communication with each other. For Communication they should identify each other in a secure way. For identification purpose each node should possess unique identity. This unique identity is referred as IP Address i.e. Internet Protocol Address. E.g.192.100.1.1/24. An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.[1].This unique IP address remains same until network is reset. So one node i.e. Sender node can identify its required node i.e. Destination node with the help of IP address. The designers of the Internet Protocol defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. However, due to the enormous growth of the Internet and the predicted depletion of available addresses, a new addressing system (IPv6), using 128 bits for the address, was developed in 1995,standardized as RFC 2460 in 1998,and is being deployed worldwide since the mid-2000s.[1].IP addresses are binary numbers, but they are usually stored in text files and displayed in human-readable notations, such as 172.16.254.1 (for IPv4), and 2001:db8:0:1234:0:567:8:1 (for IPv6).[1]

## 2. IP PREFIX INTRODUCTION

We can give IP address example as 192.100.1.1/24. In this example 192.100.1.1 is address for defined node and 24 is known as IP Prefix. IP address and IP prefix are separated by "/". The IP Prefix identifies the number of significant bits used to identify a network. IP Prefix defines how many bits are reserved to represent network and how many bits are reserved to represent host.[2] Prefix hijacking is a type of network attack that can give malicious parties access to untraceable IP addresses. On the internet, networks under control of a single entity constitute an Anonymous System (AS), each of which has a unique numerical ID assigned to it by its Regional Internet Registry. [2] Each AS has one or more routers on the edge of its network which routes traffic to its entire peer ASs. ASs then communicates routing information and establishes peering relationships using the Border Gateway Protocol (BGP).This is all done in an effort to allow each AS to make announcements about the IP address space it controls.[2] IP space is allocated and announced in blocks, so if an AS controls all IP addresses between 3.0.0.0 and 3.255.255.255, then it could announce the block 3.0.0.0/8.

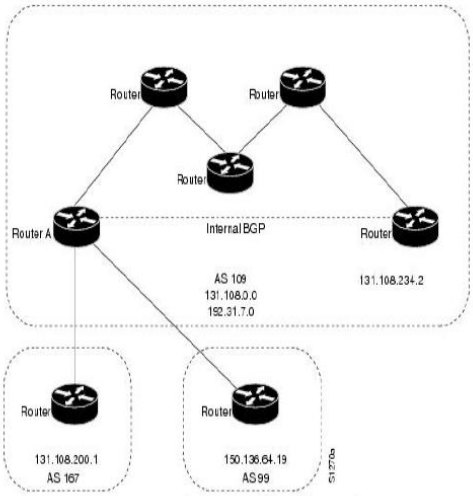


Fig 1: Example Of IP Prefix

The numbers before the slash indicate the IP address mask, and the number after the slash is how many bits of the mask should be considered important. Lower numbers indicate larger blocks - 3.0.0.0/8 contains 16 million IP addresses, while 3.1.2.0/24 contains only 256. ASs that exchange BGP information directly - "Peering ASs" - are assumed to be friendly with each other, so BGP implements no security against receiving bad or invalid routing info from other routers. [2]

Prefix-hijacking occurs when a malicious or misconfigured AS announces to its peers that a block of IP-address space belongs to them, when, in fact, it does not. After a short delay,

routes based on this bad announcement propagate through the internet at large and the malicious AS may be able to send and receive traffic using addresses it does not own.[2]

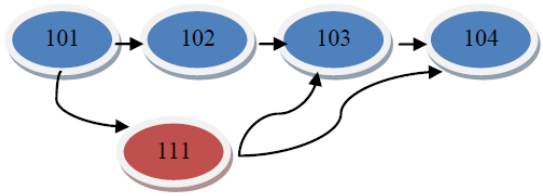



Fig. 2: AS Tree With attacking scenario

## 3. TYPES OF IP PREFIX HIJACKING

### 3.1 Hijack a Prefix

The most direct way to hijack a prefix is to announce the ownership of IP prefixes that belong to some victim ASes. The BGP neighbors subsequently propagate the route, if it is selected as the best path.

### 3.2 Hijack a Prefix and its AS

Stealthy attackers can avoid MOAS by advertising a route to the stolen prefix with an AS path that traverses its own AS to reach the victim AS. It is conceivable that the attacker uses a compromised router to pretend to be the victim AS X by advertising the route with AS path {X}. However, by default many BGP routers can reject routes with AS paths not starting with the AS number of their neighbor router in the BGP session. To ensure reachability, attackers in AS Y can instead advertise a route traversing its own AS reaching the victim AS X, i.e., with AS path {Y,X} for stolen prefixes owned by AS X.

### 3.3 Hijack a subnet of Prefix.

This is combination of first and second attack. Because of longest prefix matching, attackers can exclusively receive traffic destined to the hijacked prefix.

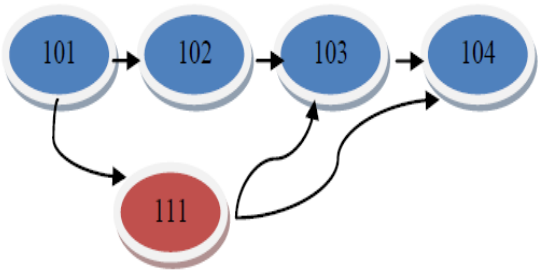
### 3.4 Hijack a legitimate Path

In the first four attack types, attackers attempt to announce an attractive route, so that routers in different networks on the Internet, even given alternative routes, will still select the hijacking route as the best route. One of the steps in route selection process is preferring routes with the shortest AS path Note that given the shortest AS path preference, networks topologically close to the victim AS are less likely impacted as they tend to choose the correct routes which are usually shorter than the hijacking routes. Based on the same reasoning, routing tables of networks close to the attacker's AS announcing the hijacking route are more likely polluted. For the fifth attack type, the attacker does not need to announce a new route but merely violate the rule of forwarding traffic. We do not focus on this attack type, but our techniques can also identify it by simply performing trace route-like probing to show that traffic stops within the malicious network.[7][8][9]

Fig 2.1 Types Of IP Prefix Hijacking

## 4. AVAILABLE SOLUTIONS AND RELATED WORK

No Doubt, IP Prefix Hijacking is an dangerous issue regarding to network communication. But Lots of researchers, Scientist have done their work for solving these types of Hijacking.




Consider an Example of Network having 4 nodes viz. 101, 102, 103, 104. Network is using IPv4 Technology for sending and receiving data packets. Take a scenario Node 101 wants to communicate with 104. So respective path for communication will be

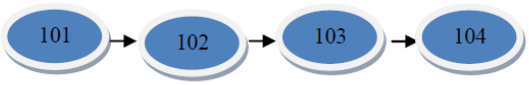



Fig 3:- Node Communication from 101 to 104.

Consider a Malicious node 111 wants to attack on pre-described network. So for IPv4 we have 16 bits for identification and routing purpose i.e. IP prefix. Node 111 will try to modify these 16 bits and will try to insert its identity maliciously, so node 111 is able to hijack a data and in other way we can say 111 can listen data transferring

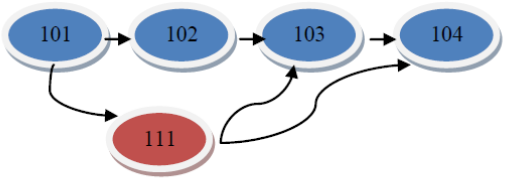



Fig 4 :- AS Tree With attacking scenario.

Fig 3 shows Fake route and defeating problems. To defeat those methods, Christian McArthur and Mina S. Guirguis have created a tool, “fake route” that intercepts trace route requests and falsifies its replies. Before the attacker hijacks a prefix, it does a trace route to the intended victim to learn about the ASes, routers and timing information along the legitimate path. Fake route uses this information to respond with the IP addresses (via spoofing the source IPs) and round-trip times (via adding the appropriate delay) of the legitimate routers, after the hijacking occurs. Responses from fakeroute could not be differentiated from legitimate responses.

Table 1: Traceroute & BGP Paths

| Status | BGP path to the Victim |
|---|---|
| Before Attack | 101-102-103-104 |
| After Attack | 101-111-103-104 |
| Trace Route Paths to the Victim | |
| Before Attack | 101-102-103-104 |
| After Attack | 101-111-103-104 |
| Falsifying Hop Count | 101-111-111-104 |
| Falsifying Entire Path | 101-102-103-104 |
| Trace Route Paths to the Reference Point | |
| Before Attack | 101-102-103-104 |
| After Attack | 101-102-103-104 |

In above table it is clearly shown that node 111 (Attacking node) is working as falsy node. So every possible communication from node 101 goes from falsy node 111. So in other words we can say node 111 is able to hear all communication from node 101.

## 4.1 Traceroute Path Disagreement

The authors also provide a detection method that relies on comparing a possible route to the victim with another route to a reference point. The reference point is chosen to be as close as possible to the victim, yet outside the victim‟s prefix. For example, in Figure 4, if a monitor was located in AS 101, a trace route to Texas State, AS 104 would go through the attacker‟s AS. However, a trace route to an IP in AS 103 would take a very different path. This can be seen in Table 1. Thus, all scenarios in Figure 4 will raise an alarm. Once again, through the use of fake route, the entire path can be falsified as indicated by “Falsifying Entire Path” in Table 1.

In order to avoid having discrepancies between the hijacked path and the BGP route, the attacker must provide a trace route path in which the IPs of the routers translates into AS numbers that match the BGP route. The path “Falsifying Hop Count” shown in Table 1 illustrates an AS trace route version matching the BGP announcement. However, if this route is compared to the route to the reference point there will be discrepancies suggesting a possible hijacking. If the attacker uses fake route to respond with a path that would match the route to the reference point, the AS trace route path would then disagree with the BGP announcement. Therefore, by combining these two methods, path disagreement with a reference point and mapping the IP trace route to the BGP route, stealthy prefix hijacking attacks are detected.

Author [3] has suggested another method of detecting IP Prefix hijacking which is based on TCP Idles can Technique. Let us assume a typical hijacking scenario where AS1 has a large prefix P1, e.g., 195.6.0.0/16. AS2 is malicious and hijacks subnet P2 of P1, e.g., 195.6.203.0/24. Suggested probing technique works as follows:-

Find a live host (H2 or H2‟ e.g., 195.6.203.3) in the hijacked prefix P2 with predictable IP ID values (e.g., increment by 1) and has little outgoing traffic. Later relax this requirement, but for ease of explanation let's assume the host has no outgoing traffic.

Find a live host (H1, e.g., 195.6.216.26) with IP in P1 but not in P2. More generally H1 can be any live host in any prefix except P2 originated by AS1.

Assume that due to hijacking, there exists a host H‟2 in attacker's network AS2 and a host H2 in the victim's network AS1 with the same IP 195.6.203.3. Since H1 and H2 are in the same AS, packets from H1 to 195.6.203.3 is routed using IGP, e.g., OSPF and reach the correct host H2. In contrast, if probing packets are sent from outside of AS1, they are routed using the polluted BGP routes and reach H‟2 instead, since P2 is more specific than P1.

Send probe packets to 195.6.203.3 and record its current IP ID value. Remember because our probing comes from outside of AS1, in the case of hijacking, traffic is routed to the potentially hijacked prefix and the IP ID value is that of attacker's machine, i.e., H‟2.

Send a SYN packet to an open port of H1 (195.6.216.26) with a spoofed source IP of H2 (195.6.203.3). H1 should reply with SYN/ACK to the spoofed source. Because IP address of H1 195.6.216.26 and 195.6.203.3 are inside the same AS, the response should reach H2 in AS1. After receiving this unsolicited SYN/ACK, H2 sends back a RST and increases its IP ID value by one.

Reprobe 195.6.203.3 and obtain the current IP ID value of H2 or H‟2 (depending on whether there is a hijacking attack). If the IP ID value in the reply is only increased by 1, it has not sent any packets. Very likely it did not receive H1's SYN/ACK packet.

# 5. POSSIBLE SOLUTIONS

## 5.1 Implementation of Real-Time Monitoring

One of the most important properties of our system is real-time monitoring. As hijacking sometimes lasts only for a short time period to avoid detection, a real-time detection system is essential to defend against malicious attacks in a timely manner, reduce the damage incurred, and identify the culprit. We demonstrate next how we achieve the real-time capability in our prototype system.

### *5.1.1 System architecture*

Consider a prototype system aimed at online detection of anomalous BGP routing updates and selective lightweight active probing to gather data-plane fingerprints for identifying hijacking attacks. It consists of three modules.

1. Monitor Module processes BGP updates in real time to identify potential IP hijacking. The classifier in this module classifies each update into two types: valid and anomalous. For the latter case, it groups them into four hijacking types described in x3. Then both the type and the update information (i.e., prefix and AS path) are fed into the Probing Module for further analysis.
2. Probing Module takes input from the Monitor Module and selects corresponding probing techniques. It chooses the appropriate probing locations and launches probing (e.g., OS detection, IP ID reflect scan) to the target prefix. Probe results are sent to the Detection Module.
3. Detection Module analyzes and compares the probe results to identify suspicious updates.

## 5.2 Neighbour Search

The first need to evaluating NLRI (Network Layer Reach-ability Information) is that its Neighbour must be reachable (or resolvable). Another way of saying the Neighbour must be reachable is that there must be an active route, already in the main routing table of the router, to the prefix in which the Neighbour address is located. Neighbour is most important factor in BGP. The various techniques are applicable to do

this. But we are focusing on attendance method. Consider the Fig.3 in which node 102 have the neighbours 101 and 103. Now after some delay 102 enquires the neighbours i.e. attendance, in pre-attack situation both the neighbour node gives attendance as present, after getting Ack. by this both nodes, node 102 will check routing table for cross-check.

If the routing table is exactly the same as the current neighbour situation then there is no problem. But if routing table and current neighbour's situation does not matching (After Attack – fig 4) then nod102 may take following actions.

1. Sends alert to router and neighbour BGPs
2. New neighbour search: node 102 will tries to find new neighbour excepts node 111.
3. If new neighbour found then nod 102 will send data to that node (Here also a possibility that , new node is also a attacker's node).
4. It will destroy data if that suspicious neighbour is next to it.

## 6. CONCLUSIONS

This paper focuses on IP prefix hijacking as well as focuses on various types of IP prefix hijacking. Faker out,, may help to stop IP prefix hijacking but it will required big amount of system resources to find tracer out and BGP paths. Real-time monitoring slows down the processing seed. Further analysis is also important. We cannot depend on this analysis as system is working in real-time. Analysis may helps to improve the real-time result. In neighbour Search technique detecting the Geneon neighbour is important task. New neighbor may be a hacker's node.

In summary, there is scope to the define technique to improve in IP prefix hijacking techniques. We have demonstrated some methods to stop IP prefix hijacking.

## 7. REFERENCES

[1] DOD,Standard Internet Protocol (1980) – Internet Documentary.

[2] How prevalent is prefix hijacking on the internet?- Internet Documentary by Peter Boothe, James Hiebert.

[3] Probabilistic IP Prefix Authentication (PIPA) for Prefix Hijacking, By Akmal Khan, Ted "Taekyoung" Kwon, Hyunchul Kim, Seoul National University, Korea.

[4] JPractical Defenses Against BGP Prefix Hijacking – by ZhengZhang,Ying Zhang, Y. Charlie Hu, Z. Morley Mao

[5] Accurate Real-time Identification of IP Hijacking – by Xin Hu Z. Morley Mao, University of Michigan.

[6] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[7] Swamp Computing" a.k.a. Cloud Computing".Web Security Journal.2009-12-28[http://security.sys-con.com/node/1231725].

[8] Understanding IP Prefix Hijacking and its Detection by Christian Horn n june 2009

[9] Analysis of IP Prefix Hijacking and Traffic Interception by Khin Thida Latt, Yasuhiro Ohara, Satoshi Uda and Yoichi Shinoda Japan Advanced Insitute of Science and Technology, Ishikawa, 923-1292 Japan-IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.7, July 2010