SECURITY ENHANCEMENT IN BORDER GATEWAY PROTOCOL

1Arshpreet Kaur, 2Er.Harpreet kaur
1(Student)YCOE Department Punjabi University, 2Asst. prof. YCOE Department Punjabi university
1Computer Science And Engg.
2Punjabi University, Patiala,India

ABSTRACT: BGP is the only inter-autonomous system routing protocol, so it is the protocol that makes internet work. Border Gateway protocol enables internet service providers(ISPs) to establish routing among each other and maintain the global reachability. BGP uses an algorithm which cannot be classified as a pure "Distance Vector", or pure "Link State". It is a path vector routing protocol as it defines a route as a collection of a number of AS that is passes through from source AS to destination AS. This list of ASes are called AS_PATH and is used to avoid eBGP routing loop. The performance of Global Routing System is very important for all the entities operating the autonomous systems, which makes up the internet.

Index Terms:-IPSec,MD5,SHA,DES,HMAC,AES,VOIP,AH,BGP,IP,ESPPRTG,GNS3,IOS

1. INTRODUCTION
Border Gateway Protocol was built on experience gained with Exterior Gateway Protocol[1][2], and its usage in NSFNET Backbone. BGP was not scalable for fast paced internet. Currently BGP version 4[3][4] is in use which became standard on March 1995, with RFC 1771[5], which got obsoleted by RFC 4271 [6] in January 2006. BGP is the only inter-autonomous system routing protocol, so it is the protocol that makes internet work. Border Gateway protocol enables internet service providers(ISPs) to establish routing among each other and maintain the global reachability. BGP uses an algorithm which cannot be classified as a pure "Distance Vector", or pure "Link State". It is a path vector routing protocol[7] as it defines a route as a collection of a number of AS that is passes through from source AS to destination AS. This list of ASes are called AS_PATH and is used to avoid eBGP routing loop. The performance of Global Routing System is very important for all the entities operating the autonomous systems, which makes up the internet.

1.1 Basic IP Routing Algorithm –
Given a destination IP address, 10.1.1.1 alias Dst, and network prefix, 10.1.1.0/30 alias NP :

If ( NP matches a directly connected network address) 
Deliver datagram to dst over the network link;
Else if ( The routing table has a route for NP)
Send datagram to the next-hop address according to the routing table;
Else if ( There is no route for NP, but it has a default route) 
Send datagram to the default route’s next-hop-address;
Else
Send a forwarding ICMP error message to the originator;

1.1.2 Static vs Dynamic Routing:
Routing in IP Networks can be done in either statically or dynamically:

a) Static Routing - In Static routing, network engineer creates, maintains and update a routing table statically. A static route to every network is needed to be configured for full connectivity. It has some advantages like it reduces CPU and memory overhead because it does not share static route information with other routers. It provides a total control over routing, but static routing becomes impractical on large networks, also static routing is not fault-tolerant, it requires network engineer to manually change the route information if some link goes down.

b) Dynamic Routing - In dynamic routing, routing table is created, maintained, and updated by a routing protocol. A routing protocol selects the path from source to destination dynamically. Routing protocols shares routing information with its neighbor routers. This process is done throughout the network and make every router gain the knowledge of the routes by adding the route information in the routing table. Using Routing protocols increases CPU, memory, and bandwidth usage because of route information sharing between neighbor routers, but the best thing about using a routing protocol is its ability to dynamically choose a better path, if there is any change in the routing infrastructure. Also it can provide load balancing between multiple links.

There are two types of dynamic routing protocols in IP based networks:

i) Interior gateway protocols - IGP is used for IP routing with an Autonomous System. It is also known as Intra-AS routing.
Enterprises, service providers use IGP in their internal networks. Various IGPs include Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Intermediate System to Intermediate System (IS-IS).

**ii) Exterior gateway protocols** - EGP is used for routing between autonomous systems. It is also known as Inter-AS routing. Service providers and large enterprises interconnect using EGP. Only protocol that comes under this category is Border Gateway Protocol (BGP). It is also the protocol that makes Internet work or we can say that it is the official protocol of the Internet.

**II. TOOLS AND SIMULATION PARAMETERS**

2.1 Graphic Network Simulator (GNS3) - GNS3 is an alternative software tool to using real computer labs for network engineers, or people studying for Cisco CCNA, CCNP and CCIE as well as Juniper certifications such as JNCIA, JNCIS and JNCIE. It runs the original Cisco IOS and Juniper's JUNOS images which are used in Cisco and Juniper Routers. GNS3, also is widely used to experiment features or to check configurations that needs to be deployed later on real devices. We can also connect GNS3 Labs with real devices. It also includes tools like Wireshark, which can be used as a packet analyzer and Solarwinds Tools which can be used to monitor network performance while capturing packet data on Wireshark. Below Figure 2.1 shows View of Graphic Network Simulation.

2.2 Wireshark (version 2.5) - Wireshark is the world's most popular and advanced network network analyzer. It is the de facto standard across many industries and educational institutions. It has features like "deep inspection of hundreds of protocols, live captures and offline analysis, It has the most powerful display filters in the industry. It works well in conjunction with GNS3. It can read live data from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay and others. It also has decryption support for many protocols that includes IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2. Below Figure 2.2 shows Packet capturing in Wireshark Packet Analyzer.
2.3 PRTG - PRTG Network Monitor (PRTG, successor of Paessler Router Traffic Grapher) is network monitoring software from Paessler AG. PRTG runs on Windows and monitors network availability and network usage using SNMP, Packet Sniffing, WMI, IP SLAs and Netflow and various other protocols. Below Figure 2.3 shows PRTG Network Monitor.

Figure 2.3 - shows PRTG Network Monitor

III. Simulation Parameters

<table>
<thead>
<tr>
<th>Simulator</th>
<th>Graphic Network Simulator (GNS3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Bandwidth</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Link Type</td>
<td>Ethernet</td>
</tr>
<tr>
<td>Routed Protocols</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>Type of traffic</td>
<td>Data and Voice</td>
</tr>
<tr>
<td>Number of Routers</td>
<td>10 GNS3 Virtual Routers + 1 Physical Cisco 2821</td>
</tr>
<tr>
<td>Routers Used</td>
<td>Cisco 2691 and Cisco 2821</td>
</tr>
<tr>
<td>IP Phones</td>
<td>Cisco 7961</td>
</tr>
<tr>
<td>Packet Analyzer</td>
<td>Wireshark</td>
</tr>
<tr>
<td>Monitoring Tool</td>
<td>Paessler Router Traffic Grapher (PRTG)</td>
</tr>
</tbody>
</table>

3.1 Behavior Analysis of BGP routing protocol with IPv4 and IPv6

BGP is the protocol of the internet, since early 1990’s, BGP is the only protocol used to share routes between different autonomous systems. Major priority was always towards the scalability of the Border Gateway Protocol from its starting days. Apart from scalability, other parameters like performance and security are also quite big factors in modern Internet. Bandwidths are increasing day by day, with all the major ISPs around the world like AT&T, Sprint, Verizon, British Telecom etc have their core network connected at 100 Gbps. Even though BGP is made as a slow protocol for a reason, but still there are some implementations like MPLS VPNs where Multi Protocol BGP is used, a good performance[9] is needed between Provider Edge routers that includes fast convergence. Security is the major issue that impacts large number of ISPs around the world like AT&T, Sprint, Verizon, British Telecom etc have their core network connected at 100 Gbps. Even though BGP is made as a slow protocol for a reason, but still there are some implementations like MPLS VPNs where Multi Protocol BGP is used, a good performance[9] is needed between Provider Edge routers that includes fast convergence. Security is the major issue that impacts large number of ISPs everyday, problems like Route Leaking, Plain Traffic over Internet, Distributed Denial of Service Attacks make internet insecure and ISPs faces humongous issues if the design has some problem or security methods not deployed to tackle above issues. In this chapter, problems associated with the BGP and solutions to them are given. Below figure 3.1 is one of the topology used for research work:

Problem 1 - Plain Internet vs IPsec based Internet

Problem 1 lies in comparing Internet traffic with no security applied and with IPsec used to encrypt traffic. We all know that IPSec[10][11][12] is a suite of security protocols, it is to security, what TCP/IP is for routing. Still it is not used widespread to secure internet traffic by ISP and is mainly used in Virtual Private Networks. In the testing topology shown in Figure 3.1, Bharti Airtel is connected with a Cloud3, which has virtual interface VM Net 1 connected with it, that interface also has Cisco IP Communicator connected with it. Cisco IP Communicator is a soft IP phone by Cisco Systems used in Real World VoIP communications. Below is the graphic of Cisco IP Communicator used:

Figure 3.1 - BGP topology used in GNS3

Problem 1 - Plain Internet vs IPsec based Internet

Problem 1 lies in comparing Internet traffic with no security applied and with IPsec used to encrypt traffic. We all know that IPSec[10][11][12] is a suite of security protocols, it is to security, what TCP/IP is for routing. Still it is not used widespread to secure internet traffic by ISP and is mainly used in Virtual Private Networks. In the testing topology shown in Figure 3.1, Bharti Airtel is connected with a Cloud3, which has virtual interface VM Net 1 connected with it, that interface also has Cisco IP Communicator connected with it. Cisco IP Communicator is a soft IP phone by Cisco Systems used in Real World VoIP communications. Below is the graphic of Cisco IP Communicator used:

Figure 3.2 - Cisco Soft IP Phone

On the other end, Rogers in Canada is connected with a cloud which is using LAN interface of laptop and a physical Cisco Router 2821 is connected with the LAN interface of Laptop, which has further an Cisco 7961 IP Phone connected with it. All the VoIP configuration is done on Cisco 2821 router and is the router that manages the VoIP calls between Bharti and Rogers. VoIP calls can easily be tapped using sniffers like Wireshark as shown below:

Figure 3.3 - Decoding UDP Traffic
As the above figures show, capturing voice traffic is a very easy task and if someone on the internet does a MITM attack over the internet on your company's voice data, then it can be very vulnerable. As VoIP is nothing but voice travelling over Internet Protocol, therefore IPSec can be used to secure the VoIP related data so that it cannot be tapped. IPSec is good, but it can be processor-intensive also, therefore it cannot be implemented for whole internet traffic as it may take the internet down as most of the routers will go down because of the CPU load it takes to encrypt and decrypt packets and routers will get less time to forward the IP packets based on the best path, which is their prime work. Below figure 3.8 is the Rogers router CPU processing capture with no IPsec applied, it shows that only 5% of CPU is utilized:

Above graph taken from Wireshark shows that average delay during the voice call on internet takes an average of 50-60 ms on plain internet with no IPsec applied.

Above graph created from Wireshark shows that average jitter between RTP packets during VoIP call is around 6-7 ms.

BGP Traffic with IPsec applied is compared below with different combinations of Security combinations:

- Combination 1 - SHA - AES 128 - DH5

Above graph shows that CPU Utilization begins to increase one IPsec is applied. In the above graph IPsec is applied between Bharti Airtel and Rogers traffic and the edge routers of both the ISPs have their CPU load begin to increase. In 8 minutes, CPU load increased from 10 percent to 16 percent with the same amount of traffic.

In the below graph, Wireshark capture is shown of ESP packets from Bharti Airtel or Rogers, Canada. As all the traffic is encapsulated within ESP, therefore it is nearly impossible to tap.
the VoIP traffic and then decode the RTP traffic using Wireshark Player.

**Figure 3.11 - IPSec packets captured in Wireshark**

Below figure 3.12 shows cpu utilization rate with combination of AES 128, SHA and DH5 algorithm applied.

**Figure 3.12 - CPU Load on Rogers Router during IPSec combination 1 applied**

**Combination - 2 - SHA - AES 256 - DH5**

**Figure 3.13 - CPU Utilization Rise during combination 2 of IPSec applied between the traffic**

Above is the CPU Load graph from PRTG showing rise in CPU load on Rogers router accepting packets from airtel and other ISPs over the internet and performs encryption and decryption on Cisco Router. It shows that around 14 percent load is increased on CPU over 8 minutes, which is pretty high and if traffic is increased in constant manner then it can reach its full utilization in around 50 minutes. Combination used for the above graph is AES 256, SHA and DH5.

Also the below figure shows the utilization of cpu resources rise by applying ipsec. Command used to view the rise in CPU resource utilization is "show processes cpu sorted 5sec". The output showed pretty clearly that it utilizes much higher cpu resources when compared with the last combination of AES 128, SHA and DH5 and a huge difference between the plain traffic and this combination. ISP routers that holds the internet routing table can have a severe impact on them if IPSec is implemented on them. Its much better security practice if IPSec is deployed on some other device and let the routers that hold the full internet routing table do the work of forwarding traffic on the basis of data plane. Therefore BGP can only do the control plane work and data plane is done by the Forwarding Information Base or Cisco Express Forwarding in case of routers and IPSec work is totally separated from the control plane and data plane on routing tables holding Internet Routing tables.

**Figure 3.14 - High CPU Load on Rogers Router**

**Figure 3.15 - Packet drop as traffic is increasing at a rapid rate.**
The impact of rise in CPU load can be seen in the above graph from PRTG. As the internet traffic grows rapidly and IPSec is applied on the same router that holds the internet routing table shows the increase in packet loss.

**Figure 3.16 - Graph showing decline in CPU Load as IPSec is removed.**
As I disable the IPSec on the Rogers and Bharti Airtel router, the cpu load started to decrease at a rapid pace. Also the packet loss is also decreased and almost eliminated along with faster response..

**Figure 3.17 - Figure showing decline in echo reply from Bharti connected PC to Rogers when IPSec is disabled.**
PROPOSED SOLUTION FOR PROBLEM 1 - There is a proposed solution to this kind of problem where CPU gets exhausted by large number of encryption and decryption related tasks. To overcome the problem that internet routers face with IPSec because of all traffic is encrypted rather than the important one only, below algorithm with lower level encryption can be used, where encryption bits are lowered to 56 bits from 256 bits.

A = internet-rtr
B = voip-lev-1-enterprise
C = voip-lev-2-enterprise
D = non-enterprise-traffic
E = Customer encrypted traffic

If a has d in fastethernet0/0 :
Then traffic will be forwarded to next-hop without being encrypted

Elif a has c in fastethernet0/0 :
Then perform a 56 bit encryption on all the incoming Voice/Video Packets and forward them to next-hop router

Elif a has b in fastethernet0/0 :
Then perform a 128 bit encryption on all the incoming Voice/Video packets and forward them to next-hop-router

Else
Send traffic will be forwarded to next-hop without being encrypted

Below is the result of the above algorithm:

![Figure 3.18 – An improved result with new method.](image)

Problem 2 - Route Leaking :-
Route leaking or Route Hijacking is a very severe problem on Internet, where the routes of one ISP are advertised by some other ISP, which can be intentional or by mistake. If the ISP that advertises false routes into the BGP internet table has better path to customer than the real one or enters a longer prefix than the original one, then the traffic towards that routes are either black holed or goes through the false ISP, that adds the delay. Below is the screenshot of route leakins in the regions as per August 4, 2016 of bgpstream.com, which is the website that monitors the route leaks continuously using the API of BGPMON.net:

![Figure 3.19 – bgpstream.com showing continuous route leaking in BGP.](image)

There are route servers of all the major Internet Service Providers around the world that peer with BGP internet routers of the ISPs. These route servers are mostly on the Linux based machines running Red Hat Enterprise Linux or SUSE Linux etc with Quagga running over it. Large Service providers like AT&T, Bharti Airtel, Vodafone, Colt, British Telecom etc have their route servers where the full internet routing table is synced with all their internet routers. That route server can be used as a controller as it has all the routes stored in it. What can be done is that we can use a Linux Based route-server with Quagga running over it. Red Hat Enterprise Linux can sync with all other routers and can work as a controller type machine as it has all the internet routes present in its routing table. With all the routes present in the routing table, there is just one point from where all the routes from the service provider is controlled. This can bring the entire new revolution in the service providers, where a single controller is needed to control all the traffic and there is only need of a single control plane and all other devices can act as data or forwarding plane. This can also be said as Software Defined Networking, the revolutionary approach to the network Industry by Google and Stanford University under their clean slate project. Below are the commands to make red hat enterprise linux as BGP compatible:

# yum install quagga
# setsebool -P zebra_write_config 1
# cp /usr/share/doc/quagga-X XXXX/zebra.conf.sample /etc/quagga/zebra.conf
# systemctl start zebra
# systemctl start bgpd

# systemctl enable bgpd

# yum install quagga
# setsebool -P zebra_write_config 1
# cp /usr/share/doc/quagga-X XXXX/bgpd.conf.sample /etc/quagga/bgpd.conf
# systemctl start bgpd
# systemctl start zebra
# systemctl enable bgpd
# vtysh

Router-A# configure terminal
Router-A(config)# log file /var/log/quagga/quagga.log
Router-A(config)# exit

Below is the proposed solution pseudocode that can be done on the controller :-
Suggested Algorithm pseudocode :

x = Routing Table
y = Original Route entry
z = Longer prefix

if y == [x] & & routes in [y] is reachable :
print y is best route

elif y == [x] & & z enters bgp table with different originating AS than y
print y is best route and route leak occured by z

elif y | z == [x] & & routes in [z] are reachable from [yz] with same originating AS :
print z is best route for z prefix

else y | z == [x] & & routes in [z] are unreachable from [z] and reachable from [y]
print y is best route for z prefix

Example is given below with the following topology:

![Figure 3.20 - Route Leaking topology used for example](image)

Suppose in the above example, Rogers originated route 11.1.0.0/16 and Bharti Airtel is getting routes for 11.1.0.0/16 via British Telecom. Traffic from Airtel users and Rogers 11.1.0.0 is having no problem and has a constant flow. Vodafone, on the other hand, by mistake, advertised 11.1.0.24 in their network, which is a longer prefix than 11.1.0.0/16, therefore...
if other ISPs on the internet receives this route, they make 11.1.1.0/24 as the best route from 11.1.1.0 - 11.1.1.255.

V.REFERENCES


Example pseudocode -
x = Routing Table
y = 11.1.0.0/16
z = 11.1.1.0/24

if y == [x] && routes in [y] is reachable :
   print y is best route

elsif y == [x] && z enters bgp table with different originating AS than y
   print y is best route and route leak occured by z

elsif y == [x] && routes in [z] are unreachable from [z]
   print z is best route for z prefix

else y == [x] && routes in [z] are reachable from [y]
   print y is best route for z prefix

IV. CONCLUSION

BGP is the protocol that is used to share routes between the Internet Service Providers. It is the only exterior gateway routing protocol in the world. With Internet of Things and cloud computing, security is becoming a big concern with Border Gateway Protocol. Security can never be fully achieved and there is no such thing as 100 percent security in any industry. In our base paper, IPSec was used to make all internet traffic encrypted which can be severe in terms of delay and cpu utilization of routers, delay on internet can make internet slow and it will not work for application where benign traffic is needed and also results in packet loss. A better solution is to use low level encryption on selective traffic and let the plain traffic continue for unimportant IP traffic. It has show significant improvement and reduces the CPU Utilization level from 14 percent to 1 percent. Route Leaking is another big problem that internet is facing from last many years, a proposed solution to that is to use route server as controller, which can control the routes using the proposed algorithm and can act as a single primary control plane and all other internet devices at ISP can act as data or forwarding plane and can act according the control plane which is running the proposed algorithm to mitigate route leaking.

Figure 3.21 - Route Leak problem occured because Vodafone by mistake advertises Rogers route.

What my theoretical method in the form of pseudocode will do is that it will helps in reduction of Route Leaking problems which can make ISPs much secure than they are today. Following image displays what would happen if my algorithm would be used :-

Figure 3.22 - Route Leaking prevention

Example pseudocode -
x = Routing Table
y = 11.1.0.0/16
z = 11.1.1.0/24

if y == [x] && routes in [y] is reachable :
   print y is best route

if y == [x] && routes in [y] is reachable :
   print y is best route

elif y == [x] && z enters bgp table with different originating AS than y
   print y is best route

elif y == [x] && routes  in [z] are unreachable from [z] and same originating AS :
   print z is best route for z prefix

else y == [x] && routes in [z] are unreachable from [z] and reachable from [y]
   print y is best route for z prefix