# Executive Summary

# Introduction

Nowadays, internet has become large domain for attackers and sources of malware. This is the serious problem as BGP (Border Gateway Protocol) do not have any efficient security mechanism so contains many vulnerabilities.

This section describes about BGP. BGP has weakness about securing and verifying the integrity and authenticity of the BGP messages between BGP neighbors. As each BGP speaker send network reachability information to its neighbors via BGP message. Also, these messages are exchanged between them through TCP connections. These impose two main vulnerabilities relating to BGP message and use of TCP session which are explained below:

1. BGP message vulnerabilities

BGP message impose serious vulnerabilities which can be exploited to perform attacks against BGP neighbors. The types of BGP messages and their relating vulnerabilities which can be exploited are described below:

* BGP header: BGP has no mechanism to check for syntax error in header. If attacker success in injecting an error BGP header, the BGP session closes removing all the routes learned in this session. So, attackers readily target header message.
* Open message: This message is exchanged to initiate a BGP session. If an open message is sent over already established session, session closes deleting all the routes learned in this session. The attackers can exploit this weak point.
* Update message: Issues relating to any syntax error in any field or transferring an update message before session establishment can cause closure of the session.
* Keep-Alive Message: this message is sent when the session is already established, if this session is on any other state than it switches to idle mode and session is closed.
* Notification Message: There is no mechanism to verify the identity of the neighbor any attacker can spoof notification message. On the reception of this message the session closes automatically and can affect inter-domain routing infrastructure.

1. TCP vulnerabilities: As already discuss the BGP uses TCP protocol as Transport protocol so BGP is exposed to all TCP related attacks. Some of them are described below:

* TCP synchronization: the TCP SYN and TCP ACK messages are sent during the TCP session initiation as BGP does not have any mechanism to validate its neighbor identity. So, attacker can send these TCP packets at the same time with other BGP node and the node may establish session with attacker rejecting the trusted connection.
* TCP Acknowledgement: This packet is used to complete establishment of the TCP connection so attacker can spoof this packet to connect to BGP peer and acquire BGP messages with routing information.
* TCP Reset: TCP RST packet closes the TCP connection immediately which eventually closes BGP session as well so if attacker succeed in spoofing this message can raise significant threat to the organization.

# Risk Analysis

Some of the attacks exploiting the above-mentioned vulnerabilities are analyzed below:

1. Spoofing: Spoofing means BGP peers are imitated. This is accomplished by targeting ports and spoofing packets. As explained BGP uses TCP as Transport protocol so spoofing TCP can be done by spoofing source IP address of the BGP neighbor, capturing packet to distinguish which peer is using port 179 to connect to BGP session initiator peer and which peer is using random port to initiate the session, matching the TCP sequence number and packet TTL matching. However, to accomplish this task advance technique and high level of understanding of routing and ISP peering working on internet is desired. Also, over the years there are known techniques for TCP sequence number prediction which have added resistance to these attacks.

Likelihood :2 Impact: 5, Risk:10

1. Hijacking: This requires successful spoofing. This attack will pretend that packet is coming from the neighbor. This packet looks valid for the peer but contains malicious BGP status update. This update can close the BGP session, inserting routing information or removing valid routing information. To accomplish this task vast knowledge of prevailing BGP interaction between BGP peers is required. Attempting to exchange Updates message to inject new prefix to BGP table, understanding of peering connection is required. So BGP communities and prefix filters on how peering is accomplished add more complexity to this type of attack.

Likelihood :1 Impact: 5, Risk:5

1. Route Flapping: The route flap is two stage change to a route in the Internet Global route table. This might be current route that is removed, or new route added. For every time these flapping occurs BGP must work and update the tables. Ultimately increases the load on the routers as they must regularly recalculate BGP compelling the router CPU to saturate. Every flap caused a stability problem on the internet, so industries responded with route flap dampening algorithm.

Likelihood :1 Impact: 5, Risk:5

1. Confidentiality attack: BGP routing information are sent in clear and plain text so if any attacker eavesdrops on peering session and have access to routing information. This will prevent the traffic from reaching the intended destination.
2. Route Hijacking: An attacker can maliciously announce the peer prefixes to reroute the traffic to or from itself which was never meant to happen. It can cause instability in network with immediate load increase. This allows intruders to gain potentially unencrypted traffic which is helpful to initiate the spamming.
3. Man, in the middle attack: Attacker can readily intercept the message as BGP lacks peer’s authentication.
4. DOS (Denial of Service): It can be done by injecting massive number of routing information and flooding the router’s table thus denying all the BGP services.
5. Wormhole Attack: It is done by confusing two peers to generate fake links to hijack traffic and update routing tables with fake paths. Thus, these fake paths are verified and adopted by victim peers.
6. Protocol Manipulation Attack: This attack is initiated in the routing control plane by manipulating all the routing paths which have high preference over the benign paths.

# Security Program

Some of the security program that can be implemented for tackling the above attack and vulnerabilities are described below:

1. Secure-BGP: This is first complete architecture proposed to minimize most of the security issues which mechanism are described below:
2. PKI (Public Key Infrastructures certificates): This mechanism is used to verify the authenticity of BGP data by verifying the BGP speaker identity. S-BGP uses two PKI’s:

* The first one is used to authenticate address allocation
* The second one is used to bind AS number to organization and organization to routers in their network

The BGP messages send by speakers are signed with private key and receiver peer verify it with two PKI’s. So, it allows BGP speaker to authenticate all the routing information to decide which is coming from trusted peer and attacker message.

1. Route Attestations: AS must have proof which shows that its valid to advertise the routes to the IP destination. This proof allows BGP speaker to verify it’s the authenticity by sending updates message and route advertised.
2. IPsec (IP security): IPsec ensure more security and verifies the BGP message integrity and speaker identity. It also protects from TCP related attacks.

At conclusion S-BGP demonstrate security measures to allow protection to BGP speakers who advertises the routing information with some limitations relating to implementation on large internet network and use of PKI’s with many nodes and huge internet traffic.

1. Secure origin BGP: It provides the database called “authorization database” in which secure information to assist speaker to verify about the authenticity of the received routing information. It mainly based on use of public keys and introduces following certificates:
2. Entity Certificate: It is X.509v3 certificate which binds each speaker to public key and allows them to recognize the sender.
3. Authorization certificates: It helps to authorize BGP peer to advertise the routes. It helps to secure the authenticity of the routing information.
4. Policy Certificate: It is the certificate which contains policies applied to the advertised routes approved by authorization certificate.

Thus, soBGP demands certificates for every exchanged message in peering session to secure BGP.

1. Pretty secure BGP: The aim of secure BGP is to balance between security measurement and deployment ability. Its operation is based on two models:
2. Centralized trust model: Each psBGP speaker demands certificate from one trusted certificate authorities’ example Regional Internet Registry to verify the AS number authentication.
3. Decentralized trust model: It is used to verify the origin of the routes as each AS create PAL (Prefix Assertion List Named which has address assertion of Local AS and its peers. Origin verification is accomplished comparing PAL with advertised origin.

Hence psBGP provides different mechanism to resolve security and BGP vulnerabilities.