Configuration of BGP route reflector and Convergence criteria

*Harsumar Singh**

M.Tech, Dpeartment of Computer Science & Engineering, Sri Guru Gobind Singh World University, Fatehgarh Sahib, Punjab, India.

*Lalit Singh Mann***

Dpeartment of Computer Science & Engineering, Sri Guru Gobind Singh World University, Fatehgarh Sahib, Punjab, India.

Abstract

Border_Gateway_Protocol (BGP) is classless protocol and EGP protocol which refers to exterior classless path vector routing protocol. Border gateway routing protocol administer to trading routing information among different autonomous system over the internet. BGP hold uncounted Not protechted security, since it works with the received information from neighboring routers which could be wrong sometime. Routing is the backbones of any network, the road transport network to the wide area network via telecom network. Its Need or significances networks (which have no middle center), that is to say, in networks where information is not spread.in this work there is a use of path change with weight up and down technique.

Keywords—TCP, authentication, Border_Gateway_Protocol (BGP), security, Interdomain routing, route reflection .weight

I. Introduction

BGP is used by most ISP's (Internet Service Provider) to transmit information about their different networks. AS (Autonomous System) are commonly defined as a network's under common administrative control. The process of routing within an AS is called intradomain routing, and routing between different Assess is called interdomain routing. The dominant interdomain routing protocol on Internet is the Border_Gateway_Protocol (BGP). BGP is a standard protocol for exchanging routes on Internet. The trading of routes is done over a

TCP (Transmission Control Protocol) session on port 179. BGP is a distance vector routing protocol that uses address prefixes as unit of routing. It is a network peer configured manually: a peer is transmitted to the neighbor to know the roads. They are then transmitted to other neighbors. A Road announcement includes IP prefix and AS path. The originating AS is the rightmost.

Another feature of BGP is that it is a protocol which is based on trust in the benevolence of AS: Any AS may advertise or relay any information, typically a road without information is genuine, that is to say without advertiser or runner has indeed a route for the prefix that add. This is BGP root problem, one that led to seek a security solution for many years. BGP is a protocol whose operation has direct influence on the Internet.

The Internet is based on administration of various kinds of networks independent hanging by a wide number of operators. Each of them manages blocks of IP addresses that can be divided into smaller sizes prefixes, for his needs or those of its clients. These independent networks are interconnected through BGP [1] Protocol, which aims to trading prefixes. In BGP terminology, a network is called Autonomous System. A company using BGP will usually have an AS number Internet. Part ant unique in the fact that BGP does not use strong security mechanisms, this paper first presents the problems faced by this protocol.

For this work, we chose to be interested in securing routing on Internet. It is also about understanding the underlying instrument at secure routing issues that meet this security requirement:

II. Ease Of Use

A. Principles of the solution

1. Confidentiality: intercepting data stream, understand the routing of an AS policy information for attacks on the upper layers.

2. Integrity: modify data in the intercepted flow.

3. Performance: prevent access to prefixes, overburden links / routers.

B. Maintaining the Integrity of the Specifications

1. Misappropriation of a prefix (prefix hijack):

An attacker announces cause of a previously announced prefix. The announcement will spread and the attacker will recover a portion of his victim traffic. Only part because the prefix being announced by several AS, traffic will be distributed between different AS announcing the prefix depending on the path length and routing policies. Moreover, it is this principle that is used in any cast. In the same vein, it Is quite possible to advertise prefixes that have not yet been allocated [2].

2. Diversion of a sub-prefix:

Same as above, but this time, the attacker announces sub-prefix. The prefix is more specific than that of the legitimate announcement; the traffic to this sub-prefix will be fully carried forward. According to the organization of network that you want to spoof an advertisement in sub-prefix is sufficient. Imagine that all machines hosting the service of a company A are all in 198.18.1.0/24 network. The company announces prefix that has been allocated to the base, but it is clear 198.18.0.0/16 enunciate sub-prefix / 24 achieves same objectives only if the attacker is the service A. In the same vein, if a sub-prefix is not used by the holder of a prefix, an attacker can announce and used maliciously without compromising the activities of the prefix of the holder and be stealthy longer.

3. Change the path AS (Autonomous System):

It is possible to add or remove AS path. If an attacker only wants to read a stream (and forward it to the destination), it can be inserted into the path of AS, taking care to be connected directly with AS that surrounds the AS path. If an attacker wants to divert / an inaccessible (sub) prefix without changing the original, it can change the path of AS to announce as the frontal AS, the only entrance / exit of the original AS. The AS path also allows the addition of trigger loops and slow detections (or prevent) the transport of a flow of information. The problem of changing the way AS, especially the addition is a road with an extra AS in the chain will not be selected by majority of routers. Beforehand, attacker can announce withdrawal of the original road in a BGP UPDATE message but it will quickly detect. The challenge is to build a path to be considered interesting by the number of routers required to achieve the target of the attack while being valid (validity depends on the purpose of the attack), and acceptable.

III. BGP Security Threats and Goals

This section is described to protect Interconnections and filter received BGP announcements. A BGP route is analogous with a number of elements and paths are elected based on local routing policy. One important avenue attribute is AS PATH, which exists of the sequence of ASes traversed by the route that is being generated.

A **route reflector** (**RR**) is a network routing component. It offers an alternative to the logical full-mesh requirement of internal border gateway protocol (IBGP). A RR acts as a focal point[*clarify*] for IBGP sessions. The purpose of the RR is concentration. Multiple BGP routers can peer with a principal point, the RR - acting as a route reflector server - rather than peer with every other router in a full mesh. All the another I-BGP routers become route reflector clients.

This approach, similar to OSPF's DR/BDR feature, provides large networks with added IBGP scalability. In a fully meshed IBGP network of 10 routers, 90 individual CLI statements (spread throughout all routers in the topology) are needed just to define the remote-AS of each peer: this quickly becomes a headache to administer. A RR topology could cut these 90 statements down to 18, offering a viable solution for the larger networks administered by ISPs.

A route reflector is a single point of failure, therefore (at least) a second route reflector may be configured in order to provide redundancy. As it is an additional peer for the other 10 routers, it comes with the additional statement count to double that minus 2 of the single Route Reflector setup. An additional 11*2-2=20 statements in this case due to adding the additional Router. Additionally, in a BGP multipath Environment this also can benefit by adding local switching/Routing throughput if the RRs are acting as traditional Routers instead of just a dedicated Route Reflector Server role.

A BGP session is established by clear and is based on information spoofing is possible in some contexts (such as the AS number and IP address). To rule out injection of data via a packet forged upstream network, most Route devices(routers)manufacturers implement TTL security. Since a BGP packet normally passes through a router, its TTL 5 only decremented by the route devices(routers)receiving it. An authentication mechanism called TCP MD5 (Message Digest 5) [3] based on a shared secret is available on most of protocol implementations BGP. In the specification of this extension, the prediction of TCP sequence numbers of the routers was a significant threat. [4] An attacker with the ability to spoof a route devices(routers)and to guess the TCP sequence number could then be injected UPDATE messages to advertise or delete routes, or NOTIFICATION messages to stop the session. With this mechanism, each transmitted TCP segment is integrity protected using the function MD5 hash and shared secret. This allows the receiver to verify TCP segment that has been issued by a route devices(routers)knows the secret.maximum number of prefixes exchanged session eBGP is thus the main mechanism on all sessions external to quickly isolate overflows. This mechanism automatically triggers the sending of a NOTIFICATION message, and then breaking BGP session when the pair announces a greater number of prefixes threshold. In general, the threshold is achieved due to human error, that is to say a misconfiguration causing re-announced the complete routing table to hand. Closing the BGP session protects the even both in terms Control [5] and transfer of Plan [6] (congestion avoided by rerouting traffic through others functional BGP peers).

BGP bearing affects from both BGP speakers and BGP sessions. Attacks against BGP control messages include, for example, modification, insertion, deletion, exposure, and replaying of messages. Here, we focus on modification and insertion (hereafter *falsification)* [8] of BGP control messages; deletion, exposure, and replaying can be addressed by a point-to-point authentication protocol [9]. The three parts of BGP update message are: unsociable routes, network layer reachability information (NLRI), and path attributes. A party which had previously announced that route can only withdraw the route. Or else a service disruption could be caused by a malicious entity and a route could be withdrawn, which is in service.

NLRI contains a set of IP prefixes with same characteristics defined by path attributes, Falsification of NLRI is done if a prefix generated by AS is either not held by that AS or gets unauthorized by the holder of that prefix from other routes. The two types of AS PATH are: AS SET and AS SEQUENCE. An AS SET contains of an unordered list of AS's, which are sometimes created by aggregation of multiple.

BGP Security Goals

It is important to become shielded protocol extensions for BGP, which can prevent threats like BGP update messages falsification. Like other secure communication protocols, BGP security goals should include data integrity and data origin authentication also the propriety verification of BGP messages will be required to prevent false attacks. NLRI propriety and AS PATH propriety should be specifically verified.

The five major security goals for BGP [13], also see [11] [12] that could create serious attacks against BGP.

1. *AS Number Authentication:* It should be confirmable that an entity using an AS number a_i as its own is, in fact, an authorized representative of the AS to which a recognized AS number authority assigned a_i.
2. *BGP Speaker Authentication:* It should be confirmable that a BGP speaker, which asserts an association with an AS number a_i, has been authorized by the AS to which a_i was assigned by a recognized AS number authority.
3. *Data Integrity:* It should be confirmable that a BGP control message is not illegally modified during a point-to-point BGP session.
4. *AS Path Verification:* It should be confirmable that an AS PATH ($pk = [a1, a2, \ldots, ak]$) of a BGP route m being propagated consists of a sequence of AS's traversed by m in the specified order, i.e., m originated from $a1$ and has traversed $a2, \ldots, ak$ in order.
5. *Prefix Origin Authentication:* It should be confirmable that it is proper for an AS to originate an IP prefix. It is *proper* for AS $a1$ to originate prefix $f1$ if (1) $f1$ is actually held by $a1$ (prefix allocation); (2) $a1$ is authorized by the holder of $f1$ (prefix delegation); or (3) $a1$ is designated a set $F1$ of prefixes; $a1$ has received a set of routes

with a set $F2$ of prefixes; and $f1$ is totaled from $F1$, $F2$, or both, such that $f\ x\ f1$, $f\ x\ F1$ $F2$ [14]

Before moving to the security proposals, let's find out the goals we want to achieve. BGP Attacks can be classified into following two categories. (i) Internal attacks and (ii) External attacks, which can also be categorized as: (1) AS Number Authentication (2) BGP Speaker Authentication (3) Data Integrity (4) Prefix Origin Verification (5) AS PATH

Verification. Depending on these five goals, we will now discuss the recently proposed BGP security approaches along with their operational features, security considerations, scalability and deployment issues [15][16].

TABLE I

Criteria	Secure BGP	Secure origin BGP	Pretty secure BGP	Pretty Good BGP
Authentication	**	**	*	*
Complete	**	**	*	*
Ease Of Deployment	**	**	*	***
Efficiency	**	**	*	*
Normalization	**	**		

- Authentication. 3 (best) to 0 (worst) based on the security of network, database etc.
- Complete. 2 (best) to 0 (worst). -1 If the solution that solves any problems (validation of the origin OR validation path).
- Ease of deployment. 3 (best) to 0 (worst). -1 If the solution is based on cryptography (unfamiliar to operators), -1 if the solution combines multiple mechanisms (e.g. PKI and trusted network).
- Efficiency. 2 (best) to 0 (worst) based on the theoretical potential vulnerabilities.
- Normalization. 2 (best) to 0 (worst). 0: the solution is the subject of consensus and is not deployed. 1: The solution is deployed but not normalized. 2: the solution has

been attempted standardization [17] [18].

Impacts of Malformed Messages

Updates

BGP batteries can have very different reactions to the reception a BGP UPDATE message type mismanaged by a router. The package can be detected as having a malformed attribute, the road is then not taken into account for the selection of best paths and no additional consequence is observed. In some cases, treatment of the UPDATE may, in order of severity, cause: an unexpected shutdown of the BGP process, stopping the process complete routing of the route devices(routers)or the full reboot of the router. The road with a mismanaged attribute can also be elected as BEST by the selection algorithm, and with its attribute unchanged at its eBGP and iBGP peers in accordance with the routing policies, spreading the risk of failures to other network nodes. Cases of the simplest failure, the filter set-up has sufficient to reduce breakdowns. For updates with of AS long paths by chance the packet is discarded by the filter before treatment, which prevents the route devices(routers)reboots or sessions BGP.

However, sending notifications on detection of malformed attribute is dependent on the location of the manufacturer: it is possible that route devices(routers)forcing the judgment of the BGP session, isolating the network of the operation to the other networks. Indeed, routers following scrupulously standards must reset the BGP session on receipt of a UPDATE containing a malformed attribute. [21] Or some batteries may disregard this statement, or not to consider an attribute as malformed because of the shadow of standards or error zones implementation.

BGP Vulnerabilities

Vulnerabilities provide huge chance of attacks on Internet. Currently, interdomain routing is Not protechtedto many attacks [22]. These threats manipulate: control messages when setting up a session, reachability updates and error messages throughout the session. The effect of these attacks:

•Eavesdropping: An attacker passively listens to data on the wire. This gives the attacker access to sensitive policy and route information being forwarded between AS's.

•Replay: An attacker records messages and resends them to the original destination. In this process attacker manipulate the valid data and sends fake data.

•Message insertion: An attacker inserts false data into a BGP session. These data can create error and terminate BGP sessions between peers or inject bad routing data.

• Message deletion: An attacker intercepts and deletes a message passed between BGP peers. Deleted BGP UPDATE messages can cause routing tables inaccuracy. Message modification: An attacker removes messages from a BGP session and reinserts them after doing some modification. Like message insertion, this also leads to inaccurate routing table and could lead to breaking of peering, which could result in routing failures.

•Man-in-the-middle: An attacker gets inserted between two peers and poses as the receiver to the sender and vice versa. This type of attack creates similar threats as that of message insertion, deletion and modification.

• Denial of service: An attacker floods the victim with resource request in an attempt to degrade or eliminate the availability of that resource. In BGP, the victim route devices(routers)is flooded with messages. Self disaggregation is a kind of denial of service, where an AS announces prefixes that should rightfully be aggregated, thereby unnecessarily advertising more specific prefixes [23]. Attacks may be passive or active. An attack is passive if the attacker does not perform any overt (and often externally observable) act. Rescorla and Korver advise writers of security specifications to classify attacks and countermeasures as being/addressing passive and active attacks [24].

VI. The Design and Operation of BGP

BGP was designed to work on the very large networks and gone through a number of updation and upgradation over its operational life. BGP was originally described in RFC1105, in June 1989 [25], allowing the Internet's inter-domain architecture to move on from a constrained architecture of a ''core'' and attached ''stub'' domains into a framework of peer routing domains without any principal ''core''. BGP-2 was described in RFC1163, in

June 1990 [26], and BGP-3 was described in RFC1267 in October 1991 [27]. The current version, BGP-4, was first deployed in 1993. The RFC describing this protocol, RFC1771 [28], was published in March, 1995, and subsequently refined with the publication of RFC4271 in January 2006 [29].

A. iBGP and eBGP

BGP is based on two types of sessions established over the transport protocol TCP. Two BGP routers connected separate SA physical link use an eBGP session to tradingcross-roads. The routes received by cross-border routers a SA must be propagated within the AS, which is usually done through iBGP sessions. The original specification assumed that a BGP complete graph of iBGP sessions would be used in the SA to distribute routes cross-domain. One consequence of this is that a full BGP routing should not redistribute iBGP session on a road he learned from another session iBGP. The problem with this complete graph of iBGP sessions is that [N × (N-1)]/2 sessions iBGP is needed in itself having N BGP routers, which quickly becomes unmanageable in large current networks which can include several hundred BGP routers.

The complete graph of iBGP sessions has the following two proposed solution: BGP Confederations [30] and road reflectors [31]. A "road reflector" is a BGP route devices(routers)particular, which can redistribute iBGP sessions on roads that has learned from other iBGP sessions. A road reflector has two types of neighbor's iBGP: neighbors "clients" and neighboring "non-customers". Typically, neighbors no clients are other routes of reflectors. A route reflector receives road all its neighbors and uses its iBGP BGP decision process to determine best routes to reach each destination. If the best route was received on an iBGP session with a client neighbor, reflector road re-announce this route iBGP to all its neighbors. Against by, if the road has been received from a non-customer neighbor, then the road will not be announced to customer's neighbors.

B. BGP (Border_Gateway_Protocol) neighbor relationship

To establish a BGP neighbor relationship between two routers, it must be manually configured on both routers. Unlike other protocols where neighbors are detected automatically, BGP must learn the address of the neighbor, so as to establish the connection.

As said before, the session uses the TCP protocol.

Here are the states of a connection:

a) Idle: First stage of a BGP session. When a logon is required (configuration, starting the router), the route devices(routers)initiates a TCP session and then goes into Connect mode (to wait for the answer)

b) Connect: The route devices(routers)waits for a response (TCP Syn-Ack) neighbor or a request for establishing TCP connection. Indeed, the two routers will want to establish a session simultaneously. One session is retained (one initiated by the route devices(routers)with the highest ID). There will be a route devices(routers)"leader" of the neighborhood relationship. When the session is established, it sends the message and open it enters Open Sent fashion

c) Active (optional): The connection attempt failed with the neighbor (Timeout). The route devices(routers)again, if it fails, it falls in Idle mode. If successful, it goes into Open Sent mode. This status is therefore reached in the event of failure in the Connect mode.

d) Open Sent: Open the message was sent. It contains various information (Version BGP route devices(routers)ID, AS number, Hold down Timer). Upon receipt of the message Open neighbor, if all should, the route devices(routers)sends a KeepAlive and goes into the Confirm Open.

e) Open Confirm: Waiting for KeepAlive neighbor, before entering Established.

f) Established: The neighbor relationship is established. The routers can tradingroutes.

C. BGP Selecting Routes Process

A BGP speaker could receive more than one announcement from different peers for the same address prefix. Among these announcements the "best" one is selected and called the locally used announcement, and then this best announcement is announced to its BGP peers. The ordered comparison sequence used to determine route object by local BGP speaker is: (i) Route object with the highest value for LOCAL_PREF attribute value is selected. (ii) *S*hortest AS_PATH attribute length is selected. (iii) MULTI_EXIT_DISCRIMINATOR with lowest attribute value is selected. (iv) Minimum IGP cost to the NEXT _HOP is selected. (v)eBGP routes are selected before iBGP learnt routes.(vi) If the lowest BGP Identifier value is selected by iBGP, then a network administrator's usually employs routing policies regarding his needs [32] [33].

VII. Conclusion and Future Work

In the following paper, we observed th Various BGP ROUTE REFLECTION and presented the Internet routing gaps. This research project allowed us to review the basics knowledge of inter-domain routing. It has reviewed and discovered in detail, , a security system that may be taken in the coming decade to be a must as soon as a new network will connect to the rest of the Internet. Through BGP more efficient cryptographic operations are applied to improve performance. In this project work packet send to destination will change automatically with less convergence with the weight command .The issues regarding address security and their advertisement in the inter-domain routing system could be possibly improved.

REFERENCES

1. Y. Rekhter, T. Li, and S. Hares. A Border_Gateway_Protocol 4 (BGP-4). RFC 4271 (Draft Standard), January 2006. Updated by RFC 6286.
2. http://albatross.ripe.net/cgi-bin/rex.pl?res=042%2F8&type=all&stime=2000-08-20&etime=2010-09-30&cf=1&af=1.
3. Heffernan. Protection of BGP Sessions via the TCP MD5 Signature Option.RFC 2385 (Proposed Standard), August 1998. Obsoleted by RFC 5925.
4. M. Zalewski. Strange Attractors and TCP/IP Sequence Number Analysis Cisco IOS, 2001. http://lcamtuf.coredump.cx/oldtcp/tcpseq.html#ios>.
5. Cisco. Cisco IOS XR Software Border_Gateway_Protocol Vulnerability, 2010.<http://www.cisco.com/en/US/products/csa/cisco-sa-20100827-bgp.html>. McPherson. When Hijacking the Internet... ARBOR SERT, 2008. <http://ddos.arbornetworks.com/2008/11/when-hijacking-the-internet/>. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_s-bgp.html
6. R. White. Deployment considerations for secure origin bgp (soBGP). Internet draft, IETF, juin 2003. URL https://tools.ietf.org/html/draft-white-sobgp-bgp-deployment-01.
7. R. White. Architecture and deployment considerations for secure origin bgp (soBGP). Internet draft, IETF, juin 2005. URL https://tools.ietf.org/html/draft-white-sobgp-architecture-02.

8. EVANGELOS Kranakis PC van Oorschot, TAO WAN. On interdomain routing security and pretty secure bgp (psBGP). Technical report, University of Carleton, juillet 2007. URL http://people.scs.carleton.ca/~paulv/papers/tissec-july07.pdf.
9. Josh Karlin Stephanie Forrest Jennifer Rexford. Pretty good bgp: Improving bgp by cautiously adopting routes. Technical report, University de New-Mexico / University Princeton, 2006. URL http://www.cs.unm.edu/~treport/tr/06-06/pgbgp3.pdf.
10. The first RFC describing were published in February 2012.
11. One of the objects of may be distributed in a new BGP attribute of a BGP UPDATE message, at most.
12. Aiello, W., Ioannidis, J., and McDaniel, P. 2003.Origin authentication in interdomain routing. ACM CCS, Washington, DC.
13. Murphy, S. 2003. Bgp security vulnerabilities analysis. IETF Draft.
14. Rescorla, E. and Korver, B. 2003. Guidelines for writing rfc text on security considerations. IETF Draft.
15. K. Lougheed and Y. Rekhter, "Border_Gateway_Protocol (BGP)," RFC 1105 (Experimental), Internet Engineering Task Force, Jun. 1989, Obsolete by RFC 1163.
16. "Border_Gateway_Protocol (BGP)," RFC 1163 (Historic), Internet Engineering Task Force, June 1990, Obsoleted by RFC 1267. "Border_Gateway_Protocol 3 (BGP-3)," RFC 1267 (Historic), Internet Engineering Task Force, Oct. 1991.
17. Y. Rekhter, T. Li, and S. Hares. A Border_Gateway_Protocol 4 (BGP-4). RFC 4271 (Draft Standard), January 2006. Updated by RFC 6286.
18. Y. Rekhter, T. Li, and S. Hares, "A Border_Gateway_Protocol 4 (BGP- 4)," RFC 4271 (Draft Standard), Internet Engineering Task Force, Jan. 2006.
19. TRAINA P.,"Autonomous System Confederations for BGP ", Internet RFC 1965, June 1996.
20. BATES T., CHANDRA R., CHEN E.," BGP Route Reflection – An Alternative to Full Mesh IBGP", Internet draft, draft-ietf-idr-rfc2796bis- 01.txt, work in progress, November 2003.
21. T. Griffin and G. Huston, "BGP Wedgies," RFC 4264 (Informational), Internet Engineering Task Force, Nov. 2005.
22. F. Wang and L. Gao, "On inferring and characterizing internet routing
23. Generic threats to routing protocols. Internet Draft.BELLOVIN, S. 1989. Security problems in the TCP/IP protocol suite.
24. KENT, S. AND ATKINSON, P. 1998a.Security architecture for the Internet protocol. IETF RFC 2401.
    a. REKHTER, Y. AND LI, T. 1995.A Border_Gateway_Protocol 4 (BGP4).IETF RFC 1771.
    b. WAN, T., KRANAKIS, E., AND VAN OORSCHOT, P. 2005. Pretty secure BGP (psBGP). In *Proceedings of the 2005 ISOC Symposium on Network and Distributed Systems Security (NDSS'05)*. San Diego, CA.
    c. WAN, T. 2006.Securing routing protocols through information corroboration. Ph.D. thesis, Carleton University,Ottawa, Canada.
    d. KENT, S., LYNN, C., AND SEO, K. 2000.Secure Border_Gateway_Protocol (S-BGP). *IEEE*

Journal on Selected Areas in Communications 18, 4 (Apr.), 582–592.

25. S. Kent and C. Lynn, J. Mikkelson, and K. Seo. Secure Border_Gateway_Protocol (Secure-BGP) - Real World Performance and Deployment Issues. In *Proc. of 2000 Internet* Society Symposium on Network and Distributed System *Security (NDSS'00)*, San Diego, USA. February 2000. [Kent (?)] Stephen T. Kent. Securing the Border_Gateway_Protocol.
26. Technicalreport,??URLhttp://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_s-bgp.html. Policies," in *IMC '03: Proc. 3rd ACM SIGCOMM Conf. Internet Measurement*. New York, NY, USA: ACM, 2003, pp. 15–26.