Securing Routing Protocol BGP

Priya Wani[1], Swati Mali[2]

[1] *M.E Student, Computer Engineering, Somaiya College of Engineering, Maharashtra, India*

[2] *M.E.Project Guide, Computer Engineering, Somaiya College of Engineering, Maharashtra, India*

---***---

Abstract - ***Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. The key issue associated with BGP is lack of strong security measures. Ultimately this routing infrastructure in the Internet is vulnerable to various sorts of attacks. Throughout the connection incorrect routing data might be traded. It is the issue of prefix hijacking. Proposed strategy employs cyclic shift algorithm along with secure hash algorithm-1 to secure the network. Recommended approach uses hashing algorithm to create hash of only key as a result of SHA-1. This particular hash value for private key sent with Open messages during session establishment. When this open messages are obtained by means of neighbors BGP routers, very first it creates key employing same password with same algorithm and create hash code for same and compare each hash unique codes. If it matches then establish protected session with master BGP router. In this way each BGP speaker make believe in relationship between the other and change route UPDATE inside secure channel.***

Key Words: *Autonomous systems (ASs), border gateway protocol (BGP), denial of service attack (DoS), secure hash algorithm (SHA-1)……*

1. INTRODUCTION

Routing protocols specifies exactly how routers communicate with one another, analyzing details that enable them to select paths among a couple of nodes on a computer network. The Internet's current routing system is divided into a two level hierarchy.

Border Gateway Protocol (BGP) is used to share routing information between autonomous systems. BGP routers join to each other to switch routing details. BGP routers linked to each other are known to be BGP peers. The two routers develop a TCP session, and then exchange OPEN and KEEPALIVE messages. Open messages permit the peering routers to realize suitable alternative settings. If this exchange is successful, then the routers alternate routing state information. If no routing upgrades are interchanged, then routers will send KEEPALIVE messages at regular interval in order to maintain the peering connection open [6].

IP hijacking at times termed to as BGP hijacking, prefix hijacking or maybe path hijacking. Prefix hijacking would be the unauthorized control group of IP addresses by corrupting Internet routing tables. The routers cannot validate details of the BGP messages in process of message exchange; hence routers trust what they receive. This weakness allows ASs to promote incorrect routing information that forwards IP packets along the incorrect routes.

Attackers may hijack IP addresses for two main reasons:

(1) Utilize the hijacked addresses to perform destructive thing. For example spamming and Denial of service attack without unveiling their own identity.

(2) Purposely disturb communication of established hosts designated with the hijacked addresses, affecting their reachability – successfully a stealthy type of DoS invasion. Both sorts of hijacking may interrupt the stability as well as security with the World Wide Web [7].

This paper explores; (1) The function of BGP in internet, (2) the security issues arising from prefix hijacking, (3) Recommended system makes a way of securing BGP and create a reliable connection between two routers (4) evaluate the outcomes against time, energy and traffic.

2. BACKGROUND & OVERVIEW

Prefix hijacking is really a considerable BGP security menace through which attackers grab IP addresses belonging to some other networks. Malicious AS injects phony path into global routing table by promoting an additional network's IP prefix. With prefix hijacking the attacker announces precisely identical IP prefix already mentioned by target. Other autonomous system will follow such path to send all packets towards attacker's router also attacker router sends undesirable packets to other AS with target's IP prefix and decelerate other AS BGP router effectiveness [10].

In Fig -1, five autonomous systems are linked together like AS-150, AS-160, AS-170, AS-180, and AS-200. Here AS-150 is genuine owner of IP prefix 10.0.32.0/8 along with router A. AS-150 have two neighbors –AS-160 and AS 170 with different IP prefixes. AS path for 10.0.32.0 /8 for AS 160 is <160 150>. Similarly, for AS-180, is <180 160 150>.

When comp1 (source) broadcast packet with destination IP 10.0.32.0 /8 then it traverse via AS path 180-160-150 and reach to actual destination. But AS-200 is attacker and advertises its own IP prefix as 10.0.32.0 /8 to neighbor AS- 150. Although actual owner connected with IP prefix 10.0.32.0 /8 is AS-150.

Now AS-180 receives the same IP prefix with shortest AS path <180 200> instead of <180 160 150>. AS-180 updates its routing table for IP prefix 10.0.32.0 /8 with new AS path <180 200>. When comp1 (source) try to communicate with Comp0 then data traverse through from AS-180 to AS-200 and towards router E which is false router and lastly reach at Comp2 in place of Comp0. This type attack is called as BGP prefix hijacking attack [9]. Just like other networked products, routers are usually susceptible to unauthorized accesses, eavesdropping, packet manipulation, session hijacking, along with other attacks. [3]

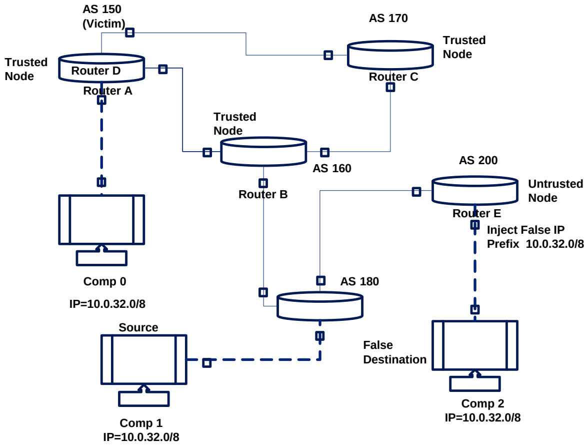

Fig -1: IP prefix hijacking

2.1 Related work

Secure Border Gateway Protocol (S-BGP) is the initial platform to secure BGP. Due to significant use of asymmetric cryptography and certificates, S-BGP becomes more expensive in storage, computation and time taken for key generation and verification. S-BGP also has higher cost for storing the detailed topology information [1].

Pretty Secure BGP (psBGP) signifies a new alternative for prefix authentication through the decentralized authentication system. Every autonomous system keeps a new prefix assertion list (PAL), which include the address ownership declaration in the local autonomous systems and its neighbors. Prefix information is verified by checking regularity of prefix assertion list around its source [4].

Secure Origin BGP (SoBGP) is another light-weight security structure. Its role is to identify doubtful advertisements using traditional hints and delay the propagation of them. Suspicious origin autonomous systems are assigned with a low preference and suspicious sub-prefixes are shortly ignored [6].

Symmetric Key Approaches to Securing BGP uses two kinds of methods the centralized and distribution key approach. Although the centralized key approach improves sign generation cost but it takes long time for sign verification. A combination of centralized and distributed methods slows down the routing performance. It also increases surplus charges for processing along with overheads [2] [11].

ID-based Aggregate Path Verification protocol (IDAPV) provides authenticity for route announcements in the Border Gateway Protocol (BGP). In such cryptosystems, the public key of user is extracted from his personal details, and private key is created by a trusted third party called Private Key Generator (PKG). Practically the ID-based cryptography has built in weakness: PKG is aware of system master key as well as private keys of all the users. Practically it is very challenging. Hence this key escrow issue must be resolved when this ID based cryptography is used [7].

3. PROPOSED WORK

The recommended method uses only one time attestation when it sets up the connection. It means create the trustful relationship between BGP peers. As shown in fig-3, cyclic key shifting algorithm is used for key generation and SHA-1 for hashing of key only. This method uses one time hash to make trust between BGP speakers.

3.1 System Architecture

BGP peer transition through several states before becoming adjacent neighbors and exchanging routing information. BGP peer transition through all the following states until an established BGP session has been created: Idle; Connect; Active; OpenSent; Open Confirm; and Established [1].

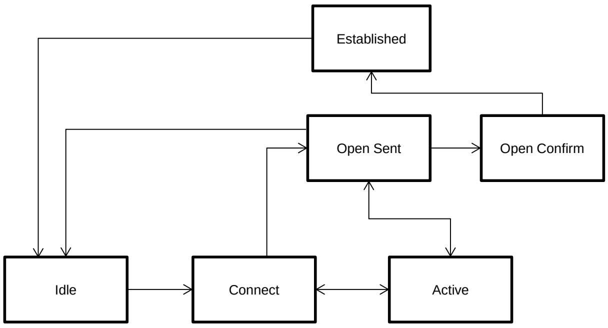

Fig -2: BGP state machine

For each peer-to-peer session, a BGP implementation maintains a state variable that tracks which of these six states the session is in. In the first "Idle" state, BGP initializes all resources, refuses all inbound BGP connection attempts and initiates a TCP connection to the peer. In the "Connect" state, the router waits for the TCP connection to complete and transitions to the "OpenSent" state if successful. If unsuccessful, it starts the ConnectRetry timer and transitions to the "Active" state upon expiration. In the "Active" state, the router resets the ConnectRetry timer to zero and returns to the "Connect" state. In the "OpenSent" state, the router sends an Open message and waits for one in return in order to transition to the "OpenConfirm" state. Keepalive messages are exchanged and, upon successful receipt, the router is placed into the "Established" state. In the "Established" state, the router can send/receive: Keepalive; Update; and Notification messages to/from its peer.

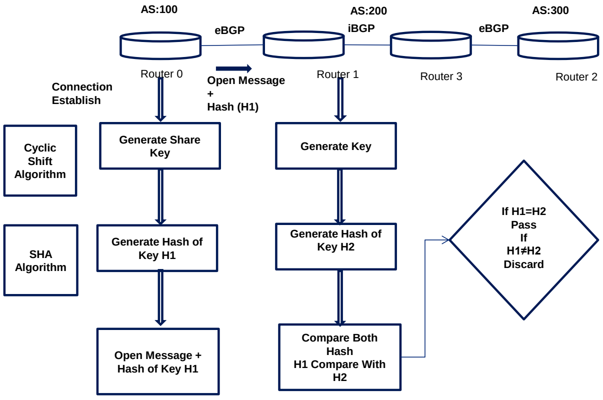

Fig - 3: Establish trust relation between BGP peer

As shown in fig - 3, BGP Router-0 linked in AS-100, Router-1 as well as Router-2 linked in AS- 200, as well as Router-3 linked in AS-300. Router-0 as well as Router-1 set up e-BGP peer. Router-1 and also Router-2 set up i-BGP peer. Router-0 with AS-100 initially ensures the connection with Router-1 in AS-200 through passing OPEN message. Before sending OPEN message Router-1 generate secure key with the help of cyclic shifting algorithm. Only the BGP speakers generate secure key which has authorized certificate id. This secure key is dispatched with OPEN message during initial connection set up. As generated secure key is in plain text form, so can't be transmitted directly. So secure hash algorithm-1 (SHA-1) is used to produce hash code for secure key and then send with OPEN message (H1).

Router-0 transmit OPEN message along with hash value of secure key (H1) to Router-1 in other autonomous system AS-200. Similar to Router-0, Router-1 also generate secure key by using cyclic shift algorithm and secure hash algorithm produces its respective hash value (H2).

If hash value (H1) of Router-0 and hash value (H2) of Rouer-1 is equal then a trust relationship is established between these two peers. Afterwards, each route updates travel on secure channel. During session, false route updates can't be injected by attackers also the attackers can't behave as owner of false autonomous system [12].

3.2 Cyclic Shifting Algorithm

A cyclic shift is the operation of rearranging the entries in a row, either by moving the final entry to the first position, while shifting all other entries to the next position, or by performing the inverse operation. A circular shift is a special kind of rotation. For example, repeatedly applying circular shifts to the four-tuple (a, b, c, d) successively gives

(d, a, b, c),

(c, d, a, b),

(b, c, d, a),

(a, b, c, d) (The original four-tuple),

Circular shifts are often used in cryptography in order to permute bit sequences.This particular algorithm builds symmetric key is actually situation sensitive as well as be based upon every single byte of password.

Here, consider [A1A2A3…An] be the security function code, where by 1, 2, 3… n = length of code. ASCII value of every code is increased in numbers through 2^i where i= position of each byte of code. Continue this process up till all bytes of password have been completed. The security code is produced after adding all this values.

Consider password 'DFeg' as an example

A1 = D A2= e A3= F A4= g

N = 68*2^1 + 70*2^2 + 101*2^3 + 103*2^4

N = 2872

Symmetric key= 2+8+7+2 =19

3.3. SHA-1: Secure Hash Algorithm

It is an algorithm that is used in cryptography to make information confidential. It accepts input message less than 2^{64} bits which are processed in 512 blocks and produce an output of 160 bit digest.

For example, the hash of the zero length string is:

SHA1 ("")=da39a3ee5e6b4b0d3255bfef95601890afd8079

A hash function takes a string of any length and produces a fixed length string as an output shown in fig - 4.

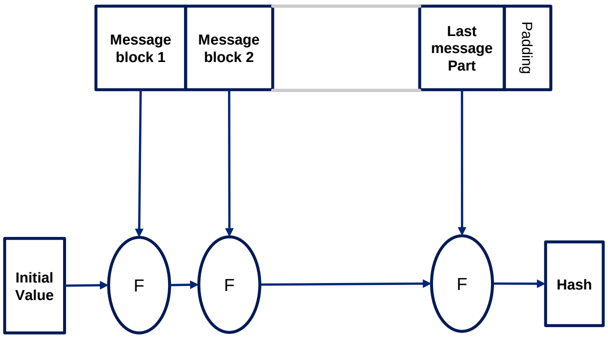

Fig - 4: Producing hash value from long string message

Cyclic shift algorithm produces symmetric key as an output. But this key is in plain text form. For security purpose SHA-1 is used. It takes this as input, produces its respective hash value as shown in fig -5.

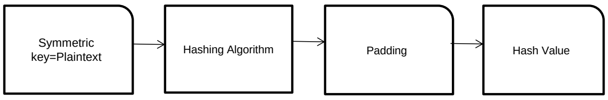

Fig -5 Generating hash value from plain text

3.4 Secure communication between two autonomous systems

As demonstrated in fig -6, five autonomous systems AS-150, AS-160, AS-170, AS-180 and AS-200 are connected to each other. Every AS has its IP address in addition to address path. AS-150 is the actual owner of IP address 10.0.32.0/8.

Autonomous system 200 tries to declare IP address 10.0.32.0/8 as its own prefix. Router4 in AS-200 does not have secure key, it means not having secure private key and hashing key. Ultimately, AS-200 cannot advertise stolen IP prefix to other autonomous systems. Thus a trust is established between two BGP peers.

As demonstrated in fig -6, five autonomous systems AS-150, AS-160, AS-170, AS-180 and AS-200 are connected to each other. Every AS has its IP address in addition to address path. AS-150 is the actual owner of IP address 10.0.32.0/8.

Autonomous system 200 tries to declare IP address 10.0.32.0/8 as its own prefix. Router4 in AS-200 does not have secure key, it means not having secure private key and hashing key. Ultimately, AS-200 cannot advertise stolen IP prefix to other autonomous systems. Thus a trust is established between two BGP peers.

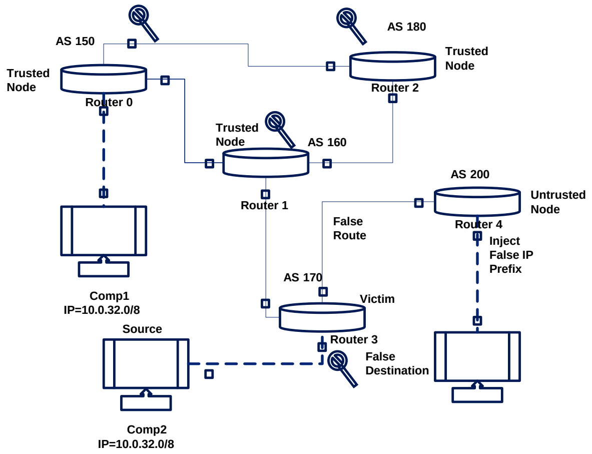

Fig - 6: Secure communications between Autonomous systems

NS-2 simulator is used to design analysis and simulate the algorithm. Using NS-2 one can simulate protocols graphically and other tool is TCL language of NS-2 simulator.

4. RESULTS

4.1 Time Analysis

Fig -7 shows results under heavy work load and x-y geometry base on time. In Secure BGP with simple encryption takes more time for routing because each route UPDATE require authentication so get periodic variation in time, whereas using only one time authentication require less average time and it require only one time variation in time. Then after get less constant time for route UPDATES. Previous algorithm with each time encryption and authentication shown by red line and proposed one time authentication shown by green line in graph. According to this algorithm, during initialization more time is needed for connection establishment of BGP speakers then after each route UPDATE transaction require less constant time.

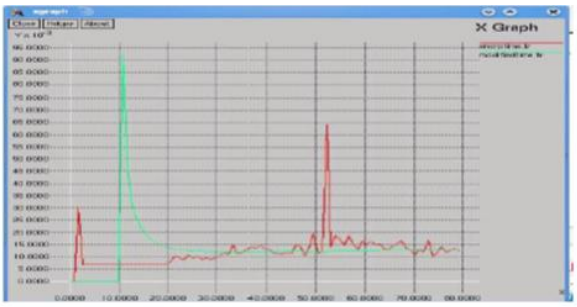

Fig - 7: Time analysis in previous algorithm and proposed algorithms

4.2 Energy Analysis

Fig-8 shows energy consumption during connection set up. In previous algorithms more energy is required for every route update authentication. The recommended algorithms provide higher security method and minimize loss in packets during routing process. In case of session termination between BGP speakers, a new session is established. Then some energy variations take place which is shown by green line.

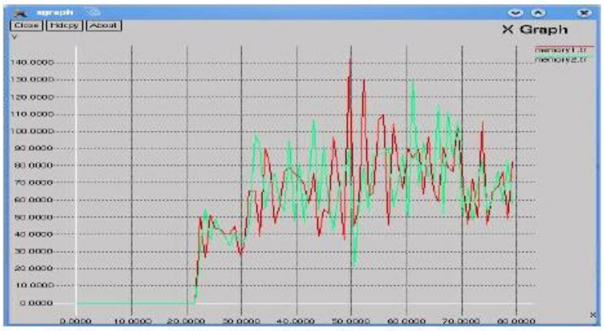

Fig-8: Energy Analyses

4.3 Traffic analysis

Fig - 9 shows previous secure BGP is vulnerable to attacks. Proposed algorithms provide more secure mechanism and reduce loss of packets between routing process.

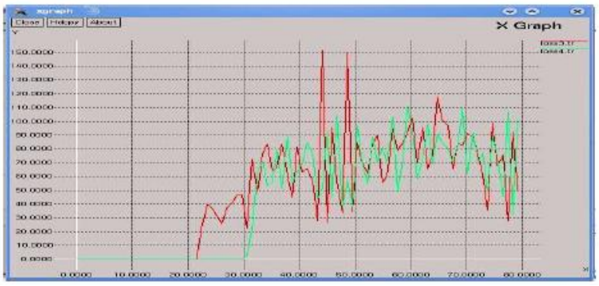

Fig -9: Output analyses

5. CONCLUSION

It is demonstrated that performance and security pertaining to BGP could be accomplished with the help of trust in BGP routers to ensure that fewer numbers of keys are important for attested the route. In this method, security provision is provided at the very first connection set up with the use of OPEN message of TCP for transmission of secure key.

Applied technique has done authentication key by making use of cyclic shift algorithm as well as secure hash algorithm-1.

As the false AS can't have secure symmetric key and its corresponding hash value so it can't set up connection with BGP neighbors.

Thus the proposed method improves the overall performance of internet, require less memory of BGP routers and reduce the packet loss.

6. ACKNOWLEDGMENTS

I would like to express profound gratitude to my guide **Prof. Swati Mali** for her invaluable support, encouragement, supervision and useful suggestions throghout this project work. Her moral support and continuous gratitude enable me to complete my work successfully.

I am grateful for the cooperation from my Head of Department **Prof. Bharathi H.N.** Her regular suggestions made my work proficient.

I wish to express my appreciation to **Prof. Prasanna Shette** and **Dr. J H Nirmal** who helped me to overcome my dough in doing this project work.

Last but not the least ,I am thankful to all those who helped me directly or indirectly in completion of this project.

7. REFERENCES

[1] Geoff Huston, Mattie Rossi, and Grenville Armitage, "Securing BGP-A literature Survey", *IEEE Communication Surveys & Tutorials*, Vol. 13, No. 2, Second Quarter

[2] Bezwada Bruhadeshwar and Kishore Kothapalli and M.Poornima and M. Divya, "Routing Protocol Security Using Symmetric Key Based Techniques", Center Security and Algorithmic Research International Institute of Information Technology Gachibowli, Hyderabad 500 032, India. *2009 International Conference on Availability, Reliability and Security*

[3] Rick Kuhn, Kotikalapudi Sriram, Doug Montgomery, "Border Gateway Protocol Security", *Recommendations of the National Institute of Standards and Technology*, Special Publication 800-54, July 2007

[4] Martin O. Nicholes, Student Member, IEEE, and Biswanath Mukherjee, Fellow, IEEE,"A Survey of Security Techniques for the Border Gateway Protocol (BGP)", IEEE Communication Surveys &Tutorials, Vol. 13, No 2, First Quarter 2009

[5] A. Barbir, S. Murphy, and Y. Yang, "Generic threats to routing protocols," *RFC 4593 (Informational), Internet Engineering Task Force*,Oct. 2006.[Online]. Available: http://www.ietf.org/rfc/rfc4593.txt

[6] By Kevin Butler, Student Member IEEE, Toni R. Farley Patrick McDaniel, Senior Member IEEE, and Jennifer Rexford, Senior Member IEEE, "A Survey of BGP Security Issues and Solutions" *Proceedings of the IEEE* Vol. 98, No. 1, January 2010

[7] Kevin Butler, Toni Farley, Patrick McDaniel &Jennifer Rexford, "A Survey of BGP Security Issues and Solutions", August 7, 2008 DRAFT.

[8] D. Eastlake 3rd and T. Hansen, "US secure hash algorithms (SHA and HMAC-SHA)," RFC 4634 (Informational), *Internet Engineering Task Force*, July 2006. [Online]. Available: http: www.ietf.org/rfc/rfc4634.txt

[9] Christian Horn, "Understanding IP Prefix Hijacking And its Detection", *Seminar Internet Routing, Intelligent Networks (INET), Technische Universitat Berlin, June 8, 2009*

[10] Saburo Seto Naoki Tateishi, Manabu Nishio, Hikaru Seshake"Detecting and Recovering Prefix Hijacking using *Multi-agent Inter-AS Diagnostic System*", 978-1 4244- 5362/10/$26.00_c 2010 IEEE.

[11] Bezwada Bruhadeshwar Sandeep S. Kulkarni Alex X. Liu, "Symmetric Key Approaches to Securing BGP– A Little Bit Trust is enough", *Parallel and Distributed Systems, IEEE Transactions* on (Volume:22 , Issue: 9) January 2011

[12] Divan Raimagia, Shraddha Singh and Sameena Zafar," A Novel Approach For Secure Routing Through BGP Using Symmetric Keys", *International Journal of Network Security & Its Applications* (IJNSA), Vol.5, No.5, September 2013.