IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. V (May – Jun. 2015), PP 17-25
www.iosrjournals.org

Solution against BGP vulnerabilities

Praveen Mandloi, Praveen Kaushik

Dept. of Computer Science and Engineering Maulana Azad National Institute of Technology Bhopal, India
Dept. of Computer Science and Engineering Maulana Azad National Institute of Technology Bhopal, India

Abstract**:** *The Border Gateway Protocol (BGP) is the only inter-domain routing protocol.Routing information among Autonomous Systems (AS) is exchanged using BGP. BGP protocol does not provide any security mechanism, so it is weak to provide security for AS path, verification of AS number ownership as well as network prefix. Due to lack of security measures, BGP remains vulnerable to various types of misconfiguration and attacks.*

The objective of this paper is to introduce BGP, to present its current vulnerabilities of inter-domain routing system, to survey some proposed solution for securing BGP and also propose a solution that will overcome almost all vulnerabilities regarding BGP. We use x.509 certificates for authentication of address space and BGP speaker. IPsec is also applied for creating secure communication between BGP speakers.In our proposal, we first authenticate BGP speaker after verifying its certificate, if the certificate is valid then only BGP session is established. In our analysis we found that our proposed solution has very low computational cost, reduction of memory requirement at BGP speaker in comparison to other proposals.

Keywords: *BGP, x.509v3 certificate, IPsec, MD5, and SHA-1.*

I. Introduction

Internet is a collection of networks. While surfing over Internet, user desire service provided by server somewhere in the Internet. To provide service data must be routed from user's end to the server. In Internet, part of network under single administration is called an Autonomous system (AS). Local routing (with respect to user) infrastructure provides support within a domain and cannot provide complete route for data. All these local networks exchange their routing information to create a complete path between user and server. This routing information is exchanged with the help of BGP.

Today, an Internet can be so large that one routing protocol cannot handle the task of updating routing table of all routers. For this reason, Internet is divided into Autonomous System (AS). Routing is classified into two categories: Intra-domain routing and Inter-domain routing. Routing within an AS i.e. local AS is called Intra-domain routing eg. OSPF, RIP. Routing outside AS i.e. with different AS is called Inter-domain routing eg. BGP.

BGP [6, 7] design did not include security measures against intentional or coincidental errors that could disrupt routing behavior. Due to lack of security mechanism BGP is vulnerable to various kind of attacks[18]. BGP messages exchanged between BGP peers are sent in plain text. An intruder can alter, forge or replay BGP packets.Also he can insert bogus routing information that will contaminate complete routing behavior by advertising a prefix that he do not own, he can alter the AS_PATH mentioned in the UPDATE.Various kinds of attacks are: attack against confidentiality, integrity, DOS, replay attack, prefix hijack etc.Cryptographic techniques, certificate attestation, use of shared secret key and many more solutions have been proposed. But unfortunately none of them worked well. Secure BGP (S-BGP) proposed by Kent is most reliable proposal till date.

This paper is organized as follows. In section II, we provide a brief overview of BGP, various kinds of BGP messages and there header format. In section III, we discuss various types of attacks due to lack of security mechanism. Section IV, describes how attack can be implemented by an intruder by advertising a prefix that it does not own. Section V, provides summary of work done so far on securing BGP. Section VI contains our proposed work for securing BGP. Analysis of proposed work is mentioned in section VII.
Section VIII has concluded this paper.

II. BGP Overview

BGP version 4 is current version of BGP. Routers running BGP are called BGP speakers. The primary function of BGP is to exchange network layer reachability information (NLRI) with other BGP speakers. BGP uses TCP [11] as its transport protocol. Routing information is exchanged by BGP speakers via UPDATE messages. BGP does not provide any authentication or integrity checking mechanism for UPDATE message that are received. No mechanism is provided by BGP to check whether NLRI information announced by AS is authorized to announce or not. BGP provides no way to ensure that the AS's in the AS_PATH are legitimate.

DOI: 10.9790/0661-17351725

BGP believes whatever information is received is true, which cause vulnerabilities. BGP UPDATE message either advertises a feasible route or a withdrawn route. BGP speaker change routing table according to the UPDATE message. Since there is no checking mechanism any faulty or misconfigured source can inject bogus information. The received bogus information is sent to BGP peers who can disrupt complete routing behavior. BGP header format is as follows:

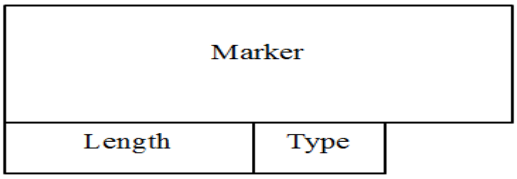


Fig 1: BGP header format (Source: RFC 4271)

Marker: This is 16 bytes field. It must be set to all 1's.
Length: This is 2 bytes field. This field indicates total length of message including header in bytes.
Type: This is 1 byte field. Type indicates type of message.

Type	Message
1	OPEN
2	UPDATE
3	NOTIFICATION
4	KEEP-ALIVE

BGP's smallest message size is 19 bytes and maximum message size is 4096 bytes. All BGP messages have fixed size header of size 19 bytes. There are four types of BGP control messages: OPEN, KEEP-ALIVE, NOTIFICATION and UPDATE.

- **OPEN message:**

After TCP connection is established by BGP peers, first message sent by each side is an OPEN message. If OPEN message is satisfactory a KEEP-ALIVE message is sent as an acknowledgement.

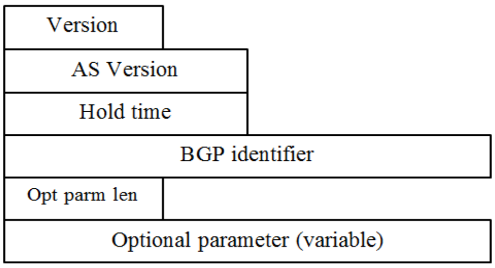


Fig 2: OPEN message format(Source: RFC 4271)

Version: This field is of 1 byte. Current version of BGP is version 4.
My Autonomous system: This field is of 2 bytes. This field mentions AS number of sender.
Hold time: This field is of 2 bytes. This value indicates maximum number of seconds that may elapse between receipts of successive UPDATE or KEEP-ALIVE message.
BGP Identifier: This field is of 4 bytes. IP address of BGP speaker is BGP identifier.
Optional parameter length: This field is of 1 byte and indicates length of Optional parameter length field in bytes.
Optional parameter: This field is of variable length. This field contains list of Optional parameter.

- **UPDATE message:**

UPDATE messages are exchanged only if there is change in the topology, i.e. either the route is withdrawn or a feasible route is advertised.

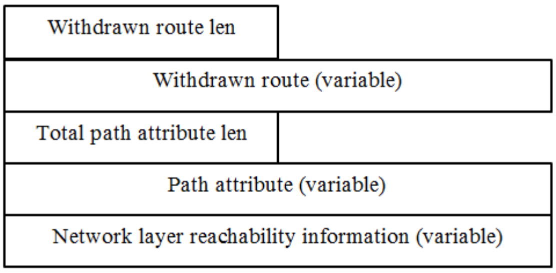

Withdrawn route len
Withdrawn route (variable)
Total path attribute len
Path attribute (variable)
Network layer reachability information (variable)

Fig 3: UPDATE message format(Source: RFC 4271)

Withdrawn route length: This field is of 2 bytes. This field indicates length of withdrawn routefield in bytes.
Withdrawn routes: This field is of variable length. This field contains IP prefixfor the routes that is being withdrawn.
Total path attribute length: This field is of 2 bytes.This field contains total length of path attribute field in bytes.
Path attributes: This field is of variable length. When an UPDATE message is sent by a BGP speaker to its peer it prepends its AS number in this field, which forms a chain of AS number that is the path for that IP prefix.
Network Layer Reachability Information: This variable length field contains list of IP address prefix.

- **KEEP-ALIVE message:**

This message is to inform other BGP peer that other BGP peer is still alive and reachable. A KEEP-ALIVE message must be exchanged before expiration of hold time mentioned in OPEN message. Size of KEEP-ALIVE message is 19 bytes. It contains only BGP header. BGP header is shown above.

- **NOTIFICATION message:**

Notification message are sent if there is any error in BGP session. After sending Notification message BGP connection is terminated immediately.

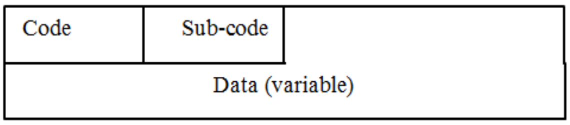


Fig 4: NOTIFICATION message format (Source: RFC 4271)

Error code: This 1 byte field indicate type of NOTIFICATION.
Error sub-code: This 1 byte field indicate more specified reason for the NOTIFICATION.
Data: This variable field is used to know the reason for getting NOTIFICATION.

Before exchanging updates, BGP speaker establishes connection with BGP peer. Firstly it performs 3 way handshaking with other BGP peer. After handshaking both BGP peers exchange OPEN message, if OPEN message is acceptable a KEEP-ALIVE message is sent in response as an acknowledgement. Once both sides have received KEEP-ALIVE message, BGP session gets established. If routes are withdrawn or feasible routes are found then BGP peer sends an UPDATE message. Otherwise KEEP-ALIVE messages are exchanged between BGP peers. When an error occurs NOTIFICATION message is sent and BGP session is terminated.

III. BGP Security Issues

Since there is no security mechanism provided by BGP, BGP is vulnerable to various kinds of attack [8, 10].

a) Attack against confidentiality:

Data that is exchanged between two parties should not be known to third person. If the information is known to someone else, data exchanged is not confidential. Information exchanged between BGP peers is in plain text. Eavesdropping on the message stream disclose information.

b) Attack against integrity:

Data exchanged should not be modified by someone else in between during transmission. It should be received in same way as it was sent. Modification in the information is attack against integrity. If the information gets modified routing information will become inconsistent.

c) Prefix hijack:

An AS announces itself as originator of the prefix that it does not own. As the bogus path propagates, some AS will route data to hijacker instead of legitimate host.

d) Path spoofing attack:

Path spoofing attacks are initiated by malicious agent. Path spoofing attack occurs when AS palaces itself in AS_PATH that it does not announce, and makes the path invalid. This causes legitimate traffic to pass through that AS.

e) Denial of Service:

Making resources unavailable to its intended users is DOS attack. Bogus routing information will never lead data to reach its end system.

f) Replay attack:

Sending captured messages after some time interval to receiving host is replay attack. Receiver of message thinks as if this is new message coming from a legitimate host. BGP has no mechanism to differentiate between messages. Previous UPDATE messages can be resent by an intruder causing link to be withdrawn which is currently working.

IV. Motivational Work

As BGP does not provide any means to authenticate BGP speaker nor there is any means to verify if the prefix that is announced is legitimate or not. An intruder can generate an UPDATE for a particular IP prefix that it does not own or an intruder can alter the AS_PATH. Both can contaminate complete routing behaviour. If an altered UPDATE message is received and routing is updated according to the UPDATE many kind of attacks can be implemented.

If an AS announces an IP prefix that it does not own, BGP peers accept that UPDATE message and make changes according to the UPDATE and send the same UPDATE to its own peers after appending there AS number in the AS_PATH. Most of the BGP speakers will use the same incorrect path for forwarding the packets to particular IP prefix. Since the origin is not the owner of IP prefix and cannot deliver the packets to the actual owner.

An intruder can also alter the AS_PATH, they can introduce their AS number in the AS_PATH and make the UPDATE invalid. As the UPDATE is traversed all the BGP speakers will use the same path as mentioned in UPDATE. While sending data to particular destination, data is forwarded to intruder. An intruder can alter or read the messages, the packets may even be dropped and not reach its destination.

Now we will see how above mentioned attack is implemented: Below shown is the arrangement of a network. AS1, AS2, AS3, AS4 are the AS with their respective AS numbers. IP prefixes they own are also mentioned corresponding to each AS. Each BGP speaker will create a TCP session with neighbouring BGP speakers. After exchanging OPEN messages and KEEPALIVE in response, UPDATE messages are exchanged.

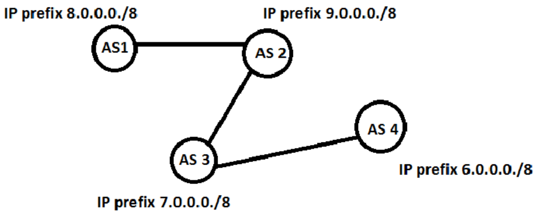


Fig 5: AS's connected to each other

Routing table for AS1 will be:

IP prefix	AS_PATH
8.0.0.0/8	AS1
9.0.0.0/8	AS1 AS2
7.0.0.0/8	AS1 AS2 AS3
6.0.0.0/8	AS1 AS2 AS3 AS4

Routing table for AS3 will be:

IP prefix	**AS_PATH**
8.0.0.0/8	AS3 AS2 AS1
9.0.0.0/8	AS3 AS2
7.0.0.0/8	AS3
6.0.0.0/8	AS3 AS4

If everything goes well this routing table will remain consistent. But suppose if AS 4 gets compromised and it start advertising its IP prefix as 8.0.0.0/8 instead of 6.0.0.0/8 then how routing table is changed and how attack is performed.

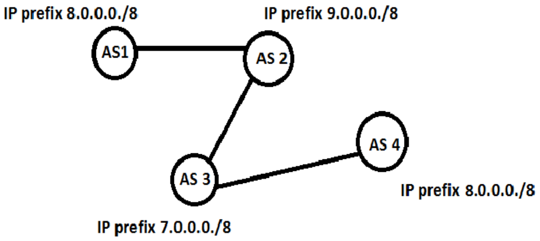


Fig 5: AS's connected with false advertisement

Routing table for AS3:

IP prefix	AS_PATH
8.0.0.0/8	AS4
9.0.0.0/8	AS3 AS2
7.0.0.0/8	AS3

As we can see AS_PATH corresponding to 8.0.0.0/8 has changed from AS3 AS2 AS1 to AS4. When AS3 BGP speaker receives UPDATE corresponding to 8.0.0.0/8 it compares length of AS_PATH. Since length of AS4 is smaller than AS3 AS2 AS1, it updates its routing table with AS4. But AS4 is not authorized to advertise the IP prefix 8.0.0.0/8 and also packets that should be delivered to AS1 which is actual owner of that prefix will never receive those packets.

V. Related Work

Several researches have been made to propose a solution for securing BGP. This section discusses various security proposals and their drawbacks. Several security mechanisms can be classified as: Cryptographic techniques, certificate and attestation, use of shared secret key and many more.

1. Cryptographic techniques:

Cryptography is applied most often in BGP. Confidentiality, integrity and entity authentication are achieved using cryptography.

a) Cryptographic hash function:

Cryptographic hash function compute a fixed length hash value from an input text and form the compressed message known as message digest. The most common hash functions in use are Message Digest Algorithm 5 (MD5) [9] and Secure Hash Algorithm 1 (SHA1) [12]. It is computationally infeasible to find input from message digest and also it is infeasible to find two different inputs having same hash value. Originator of message creates message digest from message and send message and message digest as well to the receiver. Receiver computes message digest on message using same algorithm as that of sender and verifies both the message digests, if they are same message is accepted and message integrity is verified. Security against entity authentication, prefix hijack and replay attack are not achieved using cryptographic hash function.

b) Message Authentication Code (MAC):

Secret key is required for computing MAC. MAC [13] is generated by computing a function that takes input i.e. message and secret key, and outputs a tag. The party receiving the message who has knowledge of the secret key will be able to compute the same function and verify whether the generated MAC matches the one that was sent. Integrity and Entity authentication are achieved using MAC. Prefix hijack and replay attack are not achieved using MAC.

c) Public key cryptography:

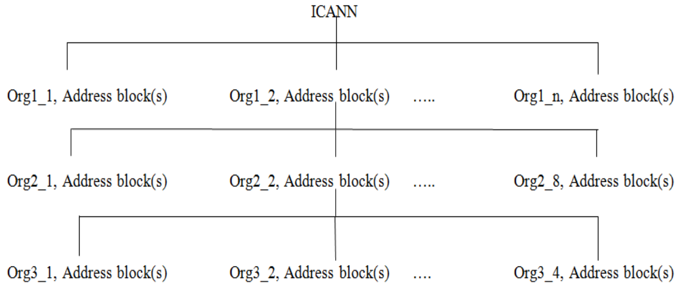
Asymmetric or public key cryptography (PKC) is used in many security solutions. Message confidentiality is achieved using encryption. Cipher text is generated with help of public key of message recipient. Only the AS with corresponding private key can decrypt the message. Integrity is achieved using digital signature. Entity authentication is also ensured because the message can only be decrypted using private of the recipient. Prefix hijack and replay attack cannot be prevented using public key cryptography.

Below shown is the table comparing above proposed algorithms and ensuring which attacks can be overcome using this approach.

Security mechanism	Integrity	Entity authentication	Prefix hijack	Replay attack
Hash Function	Yes	No	No	No
MAC	Yes	Yes	No	No
PKC	Yes	Yes	No	No

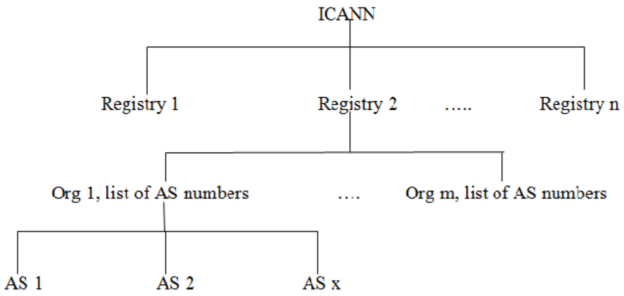
2. Certificate and attestation:

Certificates are provided in hierarchical manner. PKI's are strict hierarchies rooted at ICANN. Roots of PKI are natural trusted authorities for AS number i.e. Internet Assigned Number Authority (IANA) or Internet Corporation of Assigned Numbers and Names (ICANN). They provide certificate to Routing Information Registries (RIR), which further provide certificate to Internet Service Providers (ISP) and then to user. Proposed solutions using certificate and attestation are discussed below:



Term	Description
Org1_x	1st tier organization (A registry)
Org2_x	2nd tier organization (An ISP or DSP)
Org3_x	3rd tier organization (A DSP or user)

Fig 6: Address allocation PKI structure.



Term	Description
Registry n	DNS name of a registry.
Org m	DNS name of ISP/DSP/Organization m
AS x	DNS name of AS x

Fig 7: Autonomous system identification

Public Key Infrastructure (PKI) Certificate: PKI's are based on X.509v3 [14] certificates. PKI [15] is a model for creating, distributing and revoking certificate. PKI is a storage place for private key of those members that need to hold their private keys safe. This is used to authenticate data by approving the identity of BGP speaker.

a) Secure BGP(S-BGP):

Kent proposed Secure BGP(S-BGP)[1] for both origin authentication and path authentication. S-BGP contains three major components: PKIs, Attestation and IPsec.

PKI's are same as discussed above.Owner of IP prefixes signs using Address attestation certificate and when an UPDATE is sent to other BGP peers, it prepends it's AS number in AS_PATH and signs the message using Route attestation certificate. Address attestation is used to authenticate address allocation. Route attestation is used to authenticate AS in an AS_PATH. All UPDATE messages sent by BGP peers are signed using associated private key. IPsec is used to provide protection of BGP sessions. Each UPDATE receiving end has to verify all the route attestations and address attestation before accepting the UPDATE message. If everything is found correct, changes are made in routing table.

Still there are some limitations of S-BGP. Route attestation must be performed for every update that passes through the AS. At the end, the receiver has to verify all the AS that are mentioned in the AS_PATH and also verify origin. This process of signing and verifying has high computational cost.

b) Secure origin BGP (so-BGP):

so-BGP [2] also aims to provide both origin authentication and path authentication. so-BGP proposes use of centralized hierarchical PKI for IP prefix ownership and decentralized model for AS number authentication. Hierarchical PKI for so-BGP is same as that of S-BGP. For IP prefix ownership AS attach its Address attestation certificate, which is verified by other BGP peers to check whether originating AS is authorized to announce the IP prefix or not and for path authentication, so-BGP builds a topology map of the paths of entire network. After receiving route announcement, the speaker verifies the announced AS path with the topology.

so-BGP does not provide strong protection as S-BGP. It is not able to catch an AS path falsification.

c) Inter-domain Route Validation:

Inter-domain Route Validation (IRV)[3] combines features of S-BGP and Internet routing registries. Address attestation and route attestation are not sent along with the update message. Each AS provide IRV server. After receiving an UPDATE message, receiving AS can query originating AS to authenticate received route. AS mentioned in AS_PATH are also queried if they have received this advertised message and if they have received this, from which AS they have received and forwarded to which AS.

Are query and response are authenticated? How will the response be validated? Are query and response unaltered? These issues are not specified by IRV. Also additional overhead lies because of query and response with particular AS.

Previously proposed work	Integrity	Prefix hijack	Path spoofing	Computational cost
S-BGP	Yes	Yes	Yes	High
so-BGP	Yes	Yes	No	Moderate
IRV	Yes	Yes	Yes	High

3. Some more proposals:

Key chain based signatures and use of private key are other proposed solutions for securing BGP.

a) <u>Keychain Based Signatures:</u>

In KC-x [4], every BGP speaker generates a temporary key pair i.e. public and private key. A BGP speaker authorizes its next hop speaker. It passes its private key to next BGP speaker in plain text. In Keychain based signature, each BGP speaker signs the UPDATE message with temporary private key of preceding speaker that is received rather than its own private key. The UPDATE message and public key ofa BGP speaker are signed by its previous BGP speaker's private key that was received. The above idea forms a chain of authorization. The only exception is that the originating speaker does not receive any private key so it encrypts the message using its own private key that is authenticated by PKI. Verification of UPDATE message is done by using temporary public key of all previous speakers that are mentioned in the UPDATE message. Upon receiving the UPDATE the message is decrypted in the same way as it was encrypted. Initially the message is decrypted by origins public key, and then BGP speaker gets the public key of BGP speaker in UPDATE message.

b) <u>Trust between BGP speakers with the help of Secure Private key:</u>

It [5] creates trust between BGP speakers only one time i.e. during TCP session establishment. Instead of distributing key in plaintext, hash code of key is generated and sent to BGP peer.BGP speaker is authenticated with that hash code. If sent hash code matches with the hash code that is generated at the receiver end then the secure connection is established and routing UPDATE message are exchanged. If hash code does not match then connection not set up between BGP speakers. Cyclic key shifting algorithm is used for key generation and SHA-1 is used for hashing of key. Once secure session is established each route update travel on secure channel.

VI. Proposed Work

Our proposed work uses same architecture as that of S-BGP. We use x.509v3 certificate that are issued by trusted authorities. Certificates are provided in hierarchical manner. Public Key Infrastructure's (PKI) is strict hierarchy rooted at Internet Corporation of Assigned Numbers and Names (ICANN) or Internet Assigned Number Authority (IANA). They provide certificate to Routing Information Registries (RIR), which further provide certificate to Internet Service Providers (ISP) and then to user. These certificates namely address attestation certificate and route attestation certificate are used for entity authentication by approving the identity of BGP speaker.S-BGP sends one address attestation certificate and route attestation certificate equal to number of AS in AS_PATH for each UPDATE. Reducing number of route attestation certificate with each UPDATE message can reduce computational cost and time.

In this paper, we aim to propose a method through which we can reduce computational cost of S-BGP. We propose not to send route attestation certificate with the UPDATE message, only address attestation certificate is to be sent. Route attestation certificate is used to authenticate BGP speaker at the time of BGP session establishment. Valid route attestation certificate leads to BGP session establishment else the session won't be established. Now since only those BGP speakers are connected that are legitimate and hold route attestation certificate, only address attestation certificate is needed to be attested with the UPDATE message. This reduces number of route attestation certificate and also reduces computation cost to great level.

BGP session establishment process is mentioned above. While sending OPEN message, route attestation certificate is to be sent and verified by receiving BGP speaker, and then in response to valid route attestation certificate, KEEP-ALIVE message should be sent. This establishes BGP session with legitimate BGP speaker, now only receiving speaker has to verify address attestation certificate for each UPDATE message. Using this approach the time required to verify attestation certificate for each UPDATE is reduced to great extent. Only one certificate is to be verified for each UPDATE.

We use IPsec at network layer for security of BGP message. BGP is transported over TCP and is thus protected against disordered, lost or replayed packet. We use the Encapsulating Security Payload (ESP) protocol for maintaining integrity, authentication and anti-replay of BGP message. ESP header contains sequence number field that is used to avoid replayed packets.

VII. Analysis

Following an IETF standards action in November 2006, the Internet Assigned Numbers Authority (IANA) has extended the AS Number field to 32 bits in size, increasing the pool size from 65536 to 4,294,967,296 values [16]. There are about 69,638 AS till date 07th April 2015 [16, 17]. An X.509 certificate used in this environment is about 450 bytes long.

Assuming a network arrangement and analysing efficiency of the proposed protocol and S-BGP.

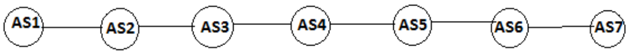


Fig 8: AS's connected to each other

Assuming:

i. Size of UPDATE message is 100 bytes.
ii. Size of address attestation certificate is 30 bytes.
iii. Size of route attestation certificate is 30 bytes.

AS1 advertise an UPDATE for address prefix say 8.0.0.0/8 to its peer AS2. UPDATE message has message, address attestation and route attestation certificate attached. The same UPDATE is advertised by AS2 to AS3 and by AS3 to AS4 and so on till AS7. Overall there are one address attestation and five route attestation certificates. Total size of UPDATE till it reaches AS7 is 280 bytes. To send UPDATE of size 100 bytes, 280 bytes are sent. This is wastage of bandwidth and consuming high computational cost as well.

According to our proposed work, BGP session is only established only when route attestation certificate is verified. So when an UPDATE is propagated no need to attest route attestation certificate with the UPDATE because all the BGP speaker connected have already verified their identity. Only address attestation certificate is to be sent with UPDATE. According to same scenario as discussed above, for each UPDATE only one address attestation certificate is sent and no route attestation certificate is sent. Total size of UPDATE till it reaches AS7 is 130 bytes, which is less than that of S-BGP.

Now since the size of UPDATE message is reduced, the bandwidth is efficiently utilized and also the BGP speaker receiving UPDATE does not have to verify the entire route attestation certificate which reduces computational cost.

VIII. Conclusion

In this paper we focused on BGP’s working, vulnerabilities, how attacks can be implemented and provided work done on BGP so far.We have seen different ways to secure BGP but using certificate attestation, BGP can be made more secure.None of the proposed work is implemented yet in practice. S-BGP is the most reliable proposed work till date. The only drawback of S-BGP is that it has high computational cost.

Our main purpose was to reduce high computational cost of S-BGP. The proposed solution can secure BGP from prefix hijacking, altering AS_PATH and replay attack. Using route attestation certificate for connection establishment reduces overhead of BGP speaker and also effectively utilizes bandwidth. Our proposed work also uses IPsec for packet security at network layer.

References

[1]. S. Kent, C. Lynn, and K. Seo“ Secure Border Gateway Protocol (S-BGP)” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION, VOL. 18, NO. 4, APRIL 2000.

[2]. R. White ”Architecture and Deployment Considerations for Secure Origin BGP (so-BGP)” , IETF ID draft-white-sobgp-architecture-02, June 2006.

[3]. G. Goodell,W. Aiello, T. Griffin, J. Ioannidis, P. McDaniel, and A. Rubin “Working around BGP: An incremental approach to improving security and accuracy of inter-domain routing” in Proc. ISOC NDSS’03, San Diego, CA, Feb. 2003.

[4]. Heng Yin, Bo Sheng, Haining Wang, Jianping Pan “Keychain-Based Signatures for Securing BGP” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 28, NO. 8, OCTOBER 2010.

[5]. Divan G. Raimagia, Shraddha Singh, and SameenaZafar “Trust between BGP speakers with the help of Secure Private key” 2012 NIRMA UNIVERSITY INTERNATIONAL CONFERENCE ON ENGINEERING, NUiCONE-2012, 06-08 DECEMBER,2013.

[6]. Y. Rekhter, T. Li, S. Hares “ A Border Gateway Protocol 4 (BGP-4)” RFC 4271, January 2006.

[7]. Rekhter, Y. and T. Li, "A Border Gateway Protocol 4 (BGP-

[8]. 4)", RFC 1771, March 1995.

[9]. S. Murphy ” BGP Security Vulnerabilities Analysis” RFC 4272, January 2006.

[10]. R. Rivest, “The MD5 Message digest algorithm” RFC 1321, April 1992.

[11]. Kevin Butler, Patrick McDaniel “ A survey of BGP security and solutions” Vol. 98 No.1, Proceeding of the IEEE, January 2010.

[12]. ”Transmission Control Protocol”, RFC 793, September 1981.

[13]. ”Secure Hash Algorithm 1 (SHA1)”, RFC 3174, September 2001.

[14]. MAC [Online] Available : http://en.wikipedia.org/wiki/Message_authentication_code

[15]. x.509 [Online] Available: https://en.wikipedia.org/wiki/X.509

[16]. Public Key Infrastructure [Online] Available: https://en.wikipedia.org/wiki/Public_key_infrastructure

[17]. Regional Internet Registries Statistics [Online] Available: http://www-public.it-sudparis.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html

[18]. AS number report [Online] Available: http://www.potaroo.net/tools/asn16/

[19]. Geoff Huston, Mattia Rossi, and Grenville Armitage “Securing BGP- A Literature Survey” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 2, SECOND QUARTER, 201