Security Problems in BGP: An Overview

Sara BAKKALI, Hafssa BENABOUD, Mouad BEN MAMOUN
Research Computer Laboratory, Faculty of Sciences at Rabat,
Mohammed V-Agdal University,
Rabat, Morocco.
bakkalisara@gmail.com, benaboud@fsr.ac.ma, ben_mamoun@fsr.ac.ma

***Abstract*— The Border Gateway Protocol (BGP) is the routing protocol used to route Internet's traffic between different Autonomous Systems. The BGP can control the traffic but it is vulnerable to communication interruptions and failures. This weakness could be the source of a several security attacks which could cause serious damages to the inter-domain network.**

The objective of this paper is to introduce briefly BGP, to present its vulnerabilities, and also to survey some proposed solutions for securing BGP. The paper introduces three secured versions of BGP, secure-BGP (sBGP), secure-origin BGP (soBGP) and pretty-secure BGP (psBGP). It discusses their advantages and identifies their limitations.

Keywords-BGP, BGP vulnerabilities, inter-domain security.

I. INTRODUCTION

Routing in Internet Network is guaranteed by two classes of protocols. The Interior Gateway Protocols (IGP) which are used for routing within the same AS, and, the Exterior Gateway Protocols (EGP) which are used for routing between different ASs. The Border Gateway Protocol BGP (RFC 4271) [1] is the single EGP protocol operational in Internet until now.

BGP is a distance vector routing protocol that uses address prefixes as unit of routing. The principal role of BGP nodes, named BGP speakers, is to exchange network's reachability information. BGP speakers assume a certain trust level between each others, that's why; as explained in [2], BGP doesn't offer a mechanism to verify node's identity or routing information's authenticity.

However, today's internet is a large space of attacks, and the trust assumed by BGP becomes a serious vulnerability [3] that could be source of diverse network attacks. The network attacks could be by intercepting routing information propagated through inter-AS network, or by removing valid routing information, or even by injecting false routing information. So, it could cause very important damages to the network like complete deny of service.

The remainder of this paper is organized as follows. Section II is a brief presentation of BGP, and its operation. In section III, we describe BGP vulnerabilities and some examples of inter-AS network attacks. Then, in section IV we present three solutions to secure BGP, secure-BGP (sBGP) [4], secure-origin BGP (soBGP) [5] and pretty-secure BGP (psBGP) [6], we define advantages of each solution and identify its limitations. We conclude our paper in section V and we give future works.

II. BGP DESCRIPTION

BGP is the most used by the Internet Service Providers (ISP's) to transmit information about their different networks. It ensures communication between the different Autonomous Systems (AS's) that form Internet. AS's are commonly defined as a network or group of networks under common administrative control.

Several BGP versions have been deployed; in this section we present BGP4 according to standardization in [1]. BGP4 is an enhanced version of BGP introduced firstly in RFC 1771 and then in RFC 4271. It presents new mechanisms to reduce the size of the routing table and also supports the use of classless inter-domain routing (CIDR) [7].

A. BGP Operation

BGP is an inter-Autonomous System routing protocol. It came to replace the EGP (Exterior Gateway Protocol) [8] which became obsolete.

Each BGP speaker is responsible for exchanging network reachability information with its BGP neighbors or peers via BGP session. These informations are stored in a router table named Routing Information Base (RIB), each entry of the RIB represents a route to a prefix address and is characterized by a set of attributes.

There are two types of BGP sessions:

- iBGP: internal BGP is a session between two BGP speakers within the same AS.
- eBGP: external BGP is a session between two BGP speakers located in two different As's.

Also, session between two BGP peers uses TCP as transport protocol [9], which means that there is no need to implement an additional mechanism for fragmentation, retransmission or sequencing.

B. BGP Messages

As mentioned before, BGP messages are exchanged between BGP peers over TCP connections. These messages, as we will explain below, are divided into four types: Open, Update, Keep-Alive and Notification.

All BGP messages have the same header which takes the following format:

978-1-4799-0324-5/13/$31.00 ©2013 IEEE

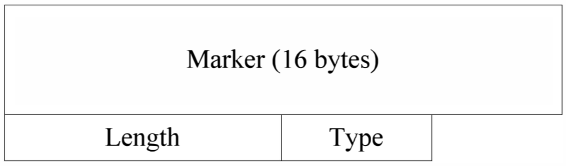

Fig. 1 BGP Header format

The BGP header is formed by three fields:

- Marker: is a 16 bytes field used for compatibility. All its bits are set in 1.
- Length: is 2 bytes a field used to indicate the total length of the message including the header. Thus, its minimum value is 19 bytes and the maximum value is 4096 bytes.
- Type: is a 1 byte field used to specify the message type according the following code. 1= Open, 2= Update, 3= Notification and 4= Keep-Alive.

In the rest of this part we describe each type of BGP messages.

1) Open Message: This message is sent by the BGP peers just after the establishment of the TCP connection. It's used to start a BGP peering session by requesting the establishment of a BGP session over the existing TCP connection, and sending to the BGP neighbour information about the BGP node that initiates the session. The open message format is presented in the following figure:

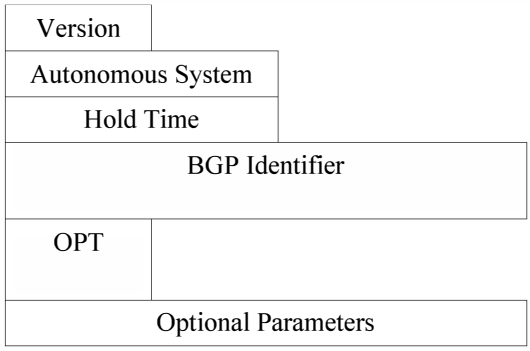

Fig. 2 Open Message format

The signification of each field is given as follows:

- Version : is 1 byte field used to indicate the BGP's version number of the message, currently it's set to 0000 0100 that represents BGP version 4.
- AS number: is 2 bytes field used to indicate the AS number of the sender node.
- Hold Time: is 2 bytes field used to state the number of seconds that the sender node proposes to its neighbor for the hold timer. It represents the time that may pass between the reception of two successive Keep-Alive or Update messages. It must be set in zero or at least 3 seconds.
- BGP Identifier: is 4 bytes field used to identify the sender node. It's equal to the IP address of the sender speaker and it's the same for all peering sessions on that node.
- OPT: Optional Parameters Length: is 1byte field that indicates the length of the Optional Parameters field.
- Optional Parameters: it's variable field that contains all optional parameters for the BGP sessions.

2) Update Message: it's the main BGP message. Using it, the BGP peers exchange their BGP tables that contain routing information. An update message is used either to advertise feasible routes to a peer, or to remove unfeasible routes from a peer routing table. The update message is formed by the following fields:

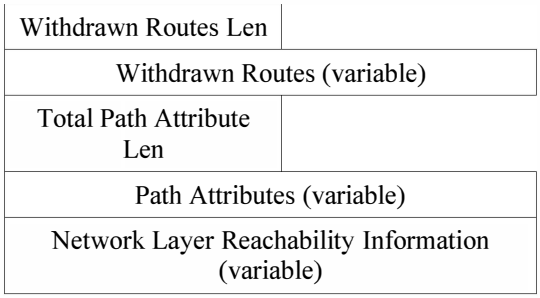

Fig. 3 Update Message Format

- Withdrawn Routes: is variable field that indicates the IP address prefixes for the routes that became down or no longer reachable.
- Path Attributes: is variable field that indicates the attributes for each path announced in update message. We will detail these attributes in the next section.
- Network Layer Reachability Information: is a variable field that contains a list of IP address prefixes which represent the different destinations announced by the update message.

3) Keep-Alive Message: this message is used to test if a BGP peer is steel reachable. A keep-Alive message must be exchanged before the expiration of the Hold Timer specified in the Open Message. Generally, it's sent every one third of the Hold Timer. The Keep-Alive message's length is equal to 19 bytes since it contains only the BGP header.

4) Notification Message: is used to signal an error in the BGP session. Once the Notification message is sent the BGP session is closed immediately. Its format is shown in the Fig. 4

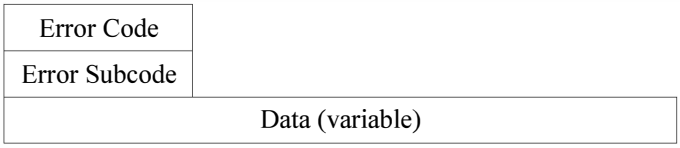

Fig. 4 Notification Message format

- Error code: is a 1 byte field that indicates the notification type.

- Error Subcode: is a 1 byte field that specifies more the error indicated with the Error code field.
- Data: is a variable field used to identify the reason for the Notification.

C. Path Attributes

In this section we will give the principal path's attributes used in the Update Messages.

1) Origin: The origin attribute defines the origin of the path information. Its value is specified by the node that initiates the path information and it's not modified by any other speaker.

2) AS Path: This attribute indicates the sequence of the AS number crossed by a route object included in the update message.

3) Next Hop: This attribute indicates the IP address of the router that represents the next hop for the paths mentioned in the update message.

4) Multi_Exit_Disc: The Multi-Exit Discriminator (MED) is the metric. It represents a suggestion to an external peer used to promote one route within the AS sending the update message if many routes are available. The route with the lower metric is preferred.

We note that MED value can be transferred over an iBGP session, but if it's received from a neighboring AS it should not be transferred to the other ASs.

5) Local Pref: This attribute is included only in update messages sent to internal peers. It's used to indicate the preferred exit node from the AS for each external route. The node with the higher local preference is preferred.

D. Path Selection Process

A BGP speaker can receive a multiple advertisement from its different neighbors concerning the same destination. However, only a single path must be selected and inserted to the IP routing table to be advertised later to the other BGP neighbors, this single path is the "best path" to reach this destination.

To select the "best path" the BGP speaker can apply a local policy as explained in [10] and [11], or generally it uses an algorithm that compares each route peers and try to choose the best route.

Next session introduces the security issues in BGP and discusses BGP vulnerabilities.

III. BGP VULNERABILITIES

As mentioned before, during the last ten years Internet environment became a large domain rich in attacks and source of bugs. This can present serious problems since BGP does not provide any efficient security mechanism, and presents many security vulnerabilities.

The objective of this section is to present the BGP security vulnerabilities according mainly on the study's results of [3], and also to list some attacks type.

A. Main Vulnerabilities

BGP presents diversified sources of vulnerabilities related to many weakness points concerning:

- Protection of the integrity and authenticity of the BGP messages.
- Verification of the BGP peers identity.
- Verification of the authenticity of the path attributes advertised by a BGP peer.

In the rest of this section we define two main BGP vulnerabilities related to BGP messages and to the use of TCP protocol.

1) BGP Messages Vulnerabilities: BGP messages represent serious sources of security vulnerabilities that can be used to perform attacks against BGP peers.

- BGP Header: any syntactic error in the BGP header can close the BGP session, thus all routes learned via this session will be removed. BGP does not offer any mechanism to check the BGP header syntax, so any outsider can attack the BGP peers session by injecting an erroneous BGP header.
- Open Message: the open message is sent to initiate a session between BGP peers. However, if an open message is sent through an active session it could cause the session closure and could delete the BGP routes learned via this session. This weak point can be used by outsiders as an attack by sending an open message over a session that is already established or sometimes even a trust BGP peer can accidentally do the same thing.
- Update Message: Many security vulnerabilities are related to this message. For example, any syntax error in any field of the received message may close the BGP session. Also, if the update message is received when the session is not yet established it causes the session's closure. Since BGP does not ensure any method to avoid these problems, outsiders can take advantage of these message's security weaknesses and can use them as sources of attacks.
- Keep-Alive Message: this message should be sent when the peering session is already established, if this session is in any other state and the BGP node receives the keep-alive message, it switches to the idle state and the session is closed.
- Notification Message: the reception of this message causes automatically the session's closure. Because of the absence of a mechanism to verify the peer identity, any outsider can spoof this message, close the session and affect the entire inter-domain routing infrastructure.

2) TCP vulnerabilities: In the previous section, we have quoted that BGP uses the TCP protocol as its transport protocol.

This fact actually introduces a serious BGP security's concern since all BGP traffic is exposed to all attacks against TCP which are much more common in Internet environment. In the following paragraphs, we present some BGP vulnerabilities related to TCP.

- TCP Synchronization: the SYN message and the SYN ACK message are sent during the TCP session establishment. However, a BGP peer cannot verify the BGP peer's identity that is requesting the establishment of the session. That is why, any outsider can sent these packets to a BGP node at the same time with another BGP trusted node, so the first node may reject the trusted connection and establish a session with the outsider, and this can have a serious damages.
- TCP Acknowledgement: it's used to complete the establishment of the TCP session. It can also be spoofed by an outsider to be connected with a BGP peer and receives all BGP messages which contain all routing information.
- TCP Reset: the receipt of a TCP RST causes immediately the TCP session closure, which means the closure of the BGP peering connection and suppression of all routes learned via this session. It may constitute an important threat if an outsider can spoof this message.

B. *Exemples of BGP Attacks*

As we have just explained, BGP have many security vulnerabilities, which make it exposed to many diversified attacks. In this section we present some examples of these attacks as listed in [12].

1) Confidentiality Attack: BGP routing information are sent in clear text over the peering session, thus any outsider can eavesdrop on the peering session and have access to routing information.

2) Message deletion: an outsider can establish a connection with a BGP peer using the BGP vulnerabilities already explained. Then, he can delete the exchanged messages.

3) Man-in-the-Middle: Because of the absence of peers authentication in BGP, an outsider can easily stand between two peers and can intercept all exchanged messages.

4) Denial of service: it can be caused by many ways, for example by injecting large number of routes objects which can cause the saturation of the router's table and deny all BGP services.

After presenting some BGP vulnerabilities and attacks, in the next section we give some proposed solutions for securing BGP.

IV. SECURING BGP

Several studies and researches have been developed to propose a solution for securing BGP. In this section we describe three architectures that represent the most interesting solutions presented until today.

A. *Secure-BGP*

In this part we introduce secure-BGP (S-BGP) [4] which is the first complete architecture that has been proposed to solve most of BGP security issues. S-BGP uses three main mechanisms:

1) Public Key Infrastructures (PKI) certificates: this mechanism is used to verify the authenticity of the BGP data by validating the identity of BGP speakers. S-BGP uses two PKI's [13], the first one is used to authenticate address allocations, and the second one is used to bind AS numbers to organizations, and organizations to routers in their networks. All messages sent by a BGP peer are signed with associated private key, and the receiver BGP peer verify, using the two PKI's; that is came certainly form the peer using the certificate. So, it allows a BGP speaker to authenticate all routing information coming from the trusted peer, to detect and reject easily any outsider messages.

2) Route Attestations: it's a new path attribute included in the update message. Each AS must have an attestation which indicates that it's authorized to advertise routes to the IP destination. This attestation allows the BGP speaker to assert the authenticity of the BGP speaker sending the update message, and of the advertised routes.

3) IPSecurity (IPSec): to ensure more security against all outsiders threat, S-BGP proposes to use IPSec [14] for verifying the BGP messages integrity, and the speaker sender identity. IPsec protect the BGP traffic against several types of attacks including attacks related to TCP.

S-BGP provides security measurements that allow a considerable protection to BGP speakers.

However, it presents some limitations concerning its implementation on Internet network, related specially to the use of PKIs' with a large number of nodes and a huge quantity of traffic.

B. *Secure origin BGP*

Secure origin BGP (soBGP) [5] introduces a secure registry of securing information named "authorization database" which allows a BGP speaker to verify the authenticity of the received routing information. It's mainly based on the use of public keys PKI', and introduces three types of certificates [15]:

1) Entity Certificate: it's an X.509v3 [13] certificate which binds each soBGP speaker to a public key; it allows the BGP speaker to verify the identity of the peer sender.

2) Authorization Certificate: it's a certificate used to verify if a soBGP peer is authorized to advertise routes, it helps to protect the authenticity of routing information.

3) Policy cerificate: it's a certificate that includes a set of policies applied to the advertized routes that are approved by the Authorization certificate.

Clearly, soBGP uses the same mechanism as S-BGP which is the PKI. However, when S-BGP demands a certificate for each update message, soBGP uses only a set of certificates for the all exchanged message over a peering connection. This makes soBGP more feasible in a large scale implementation.

Nevertheless, security level in soBGP is questionable and it does not provide a complete architecture for securing BGP.

C. Pretty secure BGP

The objective of pretty secure BGP (psBGP) [6] is to equilibrate between security measurements and deployment ability. It operates basing on two trust model:

1) *Centralized trust model:* each psBGP speaker demands a Public Key Certificate from one of the trusted certificate authorities, e.g. Regional Internet Registries (RIRs) [16], this certificate is used to verify the AS number's authentication.
2) *Decentralized trust model:* it's used to verify routes origin. Each AS creates a Prefix Assertion List named (PAL) which contains address origin assertions of the local AS and its peers, the origin's verification is ensured by comparing the PAL with the advertised origin.

psBGP provides new mechanisms to resolve BGP security vulnerabilities , these mechanisms are adapted to large scale implementation.

However a certain weakness is signaled related to the origin authentication procedure.

In this section we have presented three solutions for securing BGP, but we note that several other researches and studies that have been proposed or are still in progress introduce other procedure to secure BGP.

However, until today no proposition has actually succeeded to compromise a strong level security and feasible deployment especially in large scale, that is why no solutions has been standardized yet for Internet implementation.

V. CONCLUSION

In this paper we were focused on security issues concerning BGP, which became a serious concern especially because of the large number of threat in Internet environment today.

The BGP protocol is presented in this paper and its vulnerabilities are given. Some proposed approaches for securing BGP are cited and described in order to give their advantages and their limitations.

In future works, we intend to propose our own approach for securing BGP considering the compromise between a strong security level and a feasible implementation.

REFERENCES

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

[2] G. Huston, M. Rossi and G. Armitage ,"Securing BGP - A Literature Survey", IEEE Communication Surveys and Tutorials, April 2011, volume 13, issue 2, pp. 199-222.

[3] S. Murphy, "BGP Security Vulnerabilities Analysis", RFC 4272, January 2006.

[4] S. Kent, C. Lynn, K. Seo, "Secure Border Gateway Protocol (S-BGP)", IEEE Journal on Selected Areas in Communications, volume 18, NO. 4, pp.582-592, April 2000.

[5] R. White, "Architecture and Deployment Considerations for Secure Origin BGP (soBGP)" , RFC Internet-Draft , June 2006 .

[6] P. Van Oorschot, C. Wan, T. Kranakis, "On interdomain routing security and pretty secure BGP (psBGP)", ACM Transactions on Information and System Security, volume 10, issue 3, July 2007.

[7] Y. Rekhter, T. Li, "An Architecture for IP Address Allocation with CIDR", RFC 1518, Standards Track, September 1993.

[8] D.L. Mills, "Exterior Gateway Protocol Formal Specification", RFC 904, Historic, April 1984.

[9] M. Del Rey, "Transmission Control Protocol", RFC 793, Internet Strandard, September 1981.

[10] T. Griffin and G. Huston, "BGP Wedgies," RFC 4264, Informational, November 2005. Available: http://www.ietf.org/rfc/rfc4264.txt.

[11] F. Wang and L. Gao, "On inferring and characterizing internet routing policies," IMC '03, New York, USA, 2003, pp. 15–26.

[12] E. Rescorla, B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[13] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 3280, Standards Track, April 2002.

[14] S. Kent, K. Seo, "Security Architecture for the Internet Protocol", RFC 2401, Standards Track, December 2005.

[15] B. Weis, "Secure Origin BGP (soBGP) Certificates", RFC Internet-Draft, February 2006.

[16] D. Karrenberg, G. Ross, P. Wilson, L. Nobile, "Development of the Regional Internet Registry System", The Internet Protocol Journal – Volume 4, Number 4, Editor Cisco Systems, 2001.