Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Reinforcement of Security on BGP

Priyanka Sharma, Dr. Vishnu Sharma
Computer Science & Engineering & Galgotias University
Uttar Pradesh, India

Abstract— The internet autonomous systems interchange their routes using BGP (Border Gateway Protocol). BGP is responsible to determine the way that IP datagram must follow to reach a target address. The attacks to BGP protocol can allow a malicious person rectifier IP datagram of another autonomous system, modify them and even leave inaccessible from all internet networks. The security in BGP is a crucial aspect for the accurate operation of the internet. But not only attacks must be considered, the network misconfiguration by administrators should also be considered. The aspect of security in BGP is critical because BGP maintains routing in the internet infrastructure. Depends on when a BGP host sends a packet to another host located in a different autonomous system correctly it reaches its destination. Once raised protocol vulnerabilities has developed an application for minimize risk. In this paper, we approach the main vulnerabilities of BGP protocol and the solutions to improve the security.

Keywords— Border Gateway Protocol (BGP), ISP, MD5, Route filtering, Authentication, Security, Routing.

I. INTRODUCTION

The BGP protocol has been established as the main external routing protocol used on the Internet. Virtually all traffic flowing between them and other ISPs (Internet Service Provider) is routed through BGP. The current version, BGP-4, is described in RFC 1771 [1] and 1772 [2]. In order to reduce the size of routing tables and to facilitate their management, Internet is divided into autonomous systems (AS).

An autonomous system is a set of network managed by a single organization which has defined a single policy routing [3] .This policy routing paths decides admitted from neighbouring autonomous systems and routes that are sent to these autonomous systems. Inside, the AS uses an internal routing protocol such as OSPF and the BGP routing protocol between autonomous systems. Each autonomous system on the Internet has an identifier (ASN) formed by 16 bits, allowing up to 65536 different theoretical autonomous systems, although the range of 64512-65535 are reserved for private use.[4]

Routing tables stored in BGP-4 stores network routes to reach more specifically prefixes number of bits. The paths are formed by a sequence of numbers of autonomous systems that must be followed to achieve the specified prefix. The latest issue of AS route corresponds to the organization that has registered prefix. The main reason for storing the full path is the detection and removal of loops, i.e. packets are forwarded endlessly between a same autonomous systems (ABCABCA ...) without ever reaching the destination or, in otherwise, the same packets to pass several times by the same autonomous system. An autonomous system can be of different types depending on the number of connections to other autonomous systems and policies defined. [5] If the AS had more of a connection to other systems, usually for reasons of redundancy, it is called multihomed. The traffic circulating within the AS would remain local. Finally, an autonomous transit system is a system with multiple connections, which forwards traffic from one connection to another. Of course, autonomous systems can decide the types of traffic transported by establishing policies indeed.

Border Gateway Protocol is a routing protocol that serves as a gateway between external domains (Interdomain Routing Protocol) which once was designed without integrated security. Over time have proposed alternative protocols but till now none have been widely implemented. [6] When BGP protocol that serves as a guide and trace routes internet, a proper configuration thereof is critical. BGP errors may result in disasters that may isolate or render large internet service areas. Incidents can be both local and remote networks, and is considered absolutely necessary to deepen the consequences of decisions relating to the configuration and implement some actions to increase the security and defense of the BGP protocol.

The objective is to educate and warn entities need for improved transmission systems whose end shall ensure confidentiality, availability and integrity of data. Developing a security system covering the main BGP known vulnerabilities, and to balance the degree of security and factors complexity, performance and cost, should be a key objective for all organizations.

The intention of this paper is to demonstrate that by following a few simple steps can configure the protocol efficiently. However, we explained MD5 authentication and Route filtering algorithm and understand the different configuration options for deploying more correct, more valid and appropriate security to each situation.

II. EASE OF USE

A. SECURITY TEMPLATES

For the development of these templates and security configuration, we have done work documentation, and publications were consulted to effect as per National Institute of Standards and Technologies [7] (US NIST), an agency of the Department of Commerce of the United States. In turn, were checked monitored sites, analysis and BGP as BGP monitoring recommendations [8]. Not known organization profit technical support and network operators on the Internet. Finally, include a Packet Clearing House [9] Research Institute without profit on internet communications.

In this research BGP, previously named organizations make constant reference to the security templates BGP developed and published by team Cymru Community Services [10]. This is a US company located in the state of Illinois, specialized in research on Internet security. Team Cymru is also known for their dedication and helps organizations to identify and eradicate problems in their networks. Team Cymru team has developed various security templates, and here we have selected those belonging to Cisco routers.

B. MAINTAINING THE INTEGRITY OF SPECIFICATIONS

The measures advised to take to ensure safety in BGP. Protect the update messages from causing erroneous or falsified update the wrong choice routes. Access control to prevent unauthorized information (spoofing).This is performed by input filters that prevent unauthorized network enter into an autonomous system. Using rules filter can be defined routes that are accepted and those that will be announced. An ISP (Internet Service Provider) should filter all routes that come from a different end organization corresponding to their registered prefixes. Meanwhile, a final organization must adjust their filters to not advertise routes to other autonomous systems (not to transit). Notice of update messages (updates) to avoid monitoring for unauthorized intruder. This is done using encryption. The key can regenerate in every 30 minutes. Integrity to verify that the information has not been altered, for which hash functions (MD5) are used.

III. MD5 ALGORITHM

Message-Digest Algorithm 5 (Message Summary Algorithm 5) is an algorithm that provides 128-bit encryption. For example, this allows to easily checking a download for correctness. MD5 was developed in 1991 by Ronald L. Rivest [11]. Encryption is the process to make important information unreadable. The information once encrypted can only be read by applying a key. Configuring BGP MD5 is pretty straightforward. A network administrator has to establish a encryption algorithm like MD5 between two routers which will ensure that each segment sent in a TCP session will be verified previously. Using MD5 is both the routers should have the same password, or else the connection is never performed.

MD5 is an extension to TCP MD5 signatures. MD5 is widely used and originally considered cryptographically secure. The use of TCP / MD5 in TCP segments exchanged between two BGP peers provides integrity and authentication in BGP messages. However, it does not solve other problems as validating BGP routes announced. The main problem with TCP / MD5 is the key distribution between BGP peers, which in practice causes them to use a "shared secret" between the two extremes (symmetric key) and that it does not change as regularly as would be advisable.

After a successful download of a file or folder with files of the corresponding MD5 hash is often provided in another file. About a test program can then turn the hash value from the downloaded file will be calculated, which is then compared with the hash value provided. If both hashes are identical, the integrity of the downloaded file is confirmed. Thus, when downloading the file, there were no errors. This provides no assurance with regard to specific data manipulation by the attacker (man-in-the-middle attack), because the attacker can manipulate the transfer of the MD5 hash value.

MD5 generates an output of fixed length (128 bits) from a variable length message. First, one is appended to the outgoing message. Thereafter, the output message is padded with zeros so that its length is 64 bits away from being divisible by 512. Now, a 64-bit number encoding the length of the output message appended. The message length is now divisible by 512 [12].

The main algorithm MD5 uses a 128-bit buffer which is divided into four 32-bit words A, B, C and D. These are initialized with certain constants [13]. Now this buffer compression function is called with the first 512-bit block as a key parameter. The treatment of a message block is done in four steps similar to each other, called "rounds" of cryptographers. Each round consists of 16 operations, based on a nonlinear function "Q" modular addition, and left rotation. There are four possible "Q" functions in each round another thereof are used:

Q(x, y, z) = (x AND y) OR (NOT x AND z)

R(x, y, z) = (x AND z) OR (y AND NOT z)

S(x, y, z) = x XOR y XOR z

T(x, y, z) = y XOR (x OR NOT z)

In the result the same function with the second message block is called as a parameter and so on until the last 512-bit block. As a result, in turn, a 128-bit value is returned - the MD5 sum. Now we design and implement of data integrity checking system for MD5.

A. BUILD GRAPH IN SYSTEM

If consider the data in the files "topology" and "given, can be deduced by the following algebraic query the vertices and edges of graph:

/ * List the areas BGP_AS * /

For each value in topology [bgp_as_id] do

/ * List the areas BGP_ABC * /
For each topology in value1 [bgp_ABC_id] where do bgp_as_id = value
/ * List routing sessions between routers * /
topology [router_name] have given you a join b join topology [router_name] as c
We have [bgp_ip_address] = b [ip_address] and
b [router_name] = c [router_name]
Where
a [bgp_ABC_id] = value1 and
a [bgp_ABC_id] = c [bgp_ABC_id]
End
End
BGP routers are connected, if a router has a routing session to the IP address of an interface of the second router.

B. SYSTEM IMPLEMENTATION

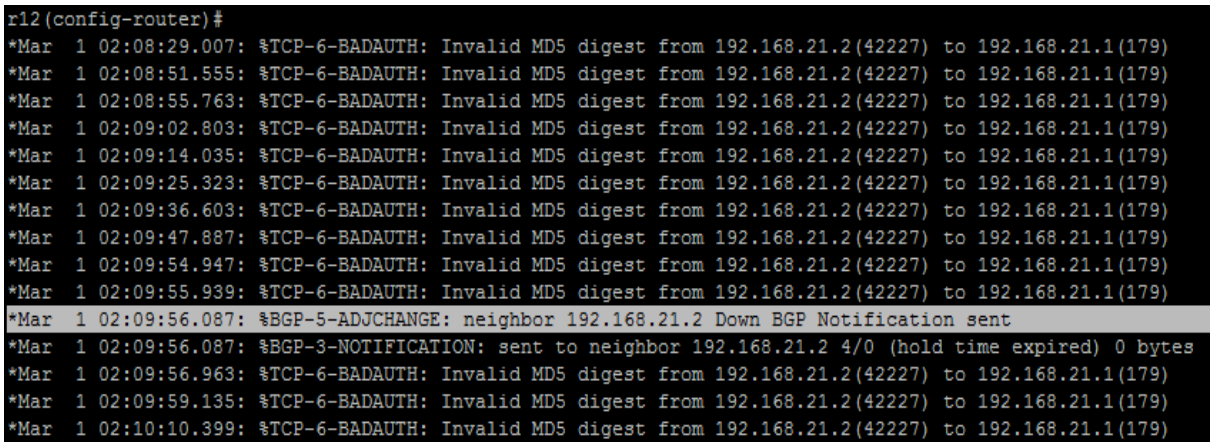

Figure 1.Communication failure between two routers due to MD5 Authentication Mismatch

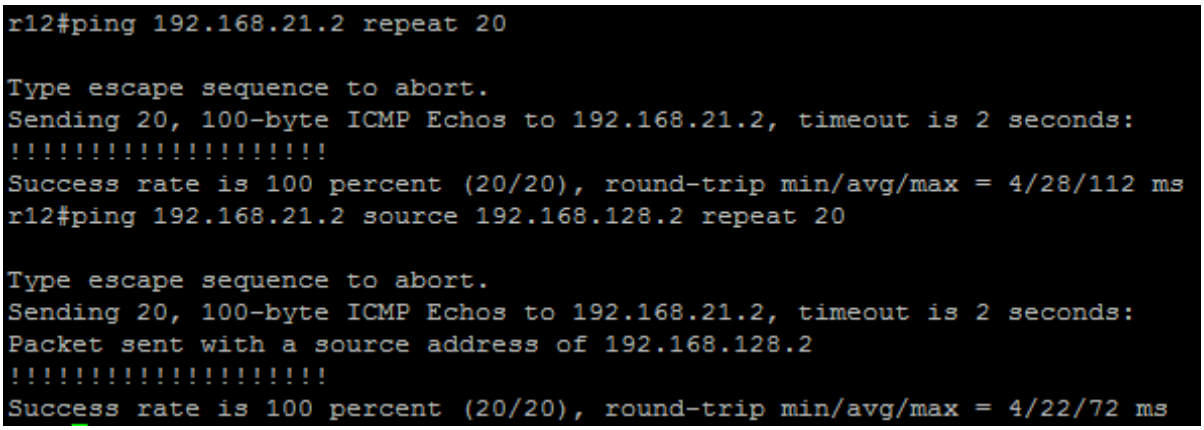

Figure 2.Successfull communication between two routers after verified MD5 Authentication

IV. ROUTE FILTER ALGORITHM

BGP will route a packet for each destination prefix by controlling preference which can control it. It can change preference by adding, deleting or modifying the attributes of BGP route announcements. An announcement is the announcement of a change in a routing table. Filter eliminates or controls how certain routes operate. They do not appear in the routing table and labelling also controls the fate of the available packages. Filtering may be applied before the preference (input filter) or preferably after complete (filter output) occurs. When it comes to protecting the network, it is essential to know their type: protocols authorized, permitted address ranges, etc [14]. There are some mechanisms fundamental to protect the network using routers through filtering. Filtering allow or deny traffic, generally through lists access control list (ACL) but can also do this by other mechanisms such as route map filtering or discard routes (null routes).

The prefix-list allow quick filtering networks are more comfortable and less complex than the ACL, as each sentence includes a sequence number. The prefix-list containing an implicit deny any at the end. Upon applying for BGP, it can perform input or output. A normal ACL cannot check a network mask. We can only check bits to ensure a coincidence, nothing more. Prefix-list has the advantage over an ACL, we can check both: bits and mask; both must match the packet is permitted or denied network. If there is only one / after network then the mask, and the number after the / is checked. ip prefix-list permit test 192.168.21.0/24 So in this case are to check the 24 bits from left to right (no matter the last 8) and also will check that the network mask is 24 bits. Both must be true for the network is allowed. However, we can be

permissive in terms of the network mask: ip prefix-list permit test 192.168.21.0/24 will check the 24 bits of the network from left to right. If it matches then match ammos network mask, which in this case may be greater than or equal to 25 bits. While the first 24 bits of the network match bitwise, the mask can be / 25, / 26, / 27, / 28, / 29, / 30, / 31, or / 32.

```
>config >router >policy-options#
prefix-list "default-v4"
prefix 0.0.0.0/0 exact
exit
prefix-list “default-v6"
prefix: /0 exact
exit
policy-statement "reject-default-v4"
entry 10
from
prefix-list "default-v4"
exit
action reject
exit
policy-statement "reject-default-v6"
entry 10
from
prefix-list "default-v6"
exit
action reject
exit
```

```
r2#ping 192.168.21.2 source 172.168.102.1 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 192.168.21.2, timeout is 2 seconds:
Packet sent with a source address of 172.168.102.1
..................................................
Success rate is 0 percent (0/50)
r2#ping 192.168.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/102/148 ms
r2#ping 192.168.21.1 source 172.168.102.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
Packet sent with a source address of 172.168.102.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/90/188 ms
```

Figure 3.Blocking unwanted routes by applying Prefix-List

V. CONCLUSIONS

BGP uses TCP MD5 option for validating data and protecting against spoofing of TCP segments exchanged between its sessions. BGP data is provided using the IPsec encryption mechanism that encrypts the IP payload (including TCP and BGP data). In order to stop unauthorized interference in the network, we used MD5 which encrypts the data and protect it by a password which can be decrypted or regenerated in original format only by the allowed network. We used route filtering in this network. Using route filtering allows us to block unwanted networks and IP’s. We can also block all the network data and allow some special selected data to advertise in the network. By using route filtering, we make our network more secure as it gives us permission to select the required or important data for receiving or advertising.

ACKNOWLEDGMENT

We would like to thank Mr. Deepak Singh for his valuable inputs to this work and Galgotias University for its LAB support.

REFERENCES

[1] Y. Rekhter y T. Li, “A Border Gateway Protocol 4 (BGP-4)”, RFC 1771, marzo de 1995.
[2] Y. Rekhter y P. Gross, “Application of the Border Gateway Protocol in the Internet”, RFC 1772, marzo de 1995.
[3] J. Hawkinson y T. Bates, “Guidelines for creation, selection, and registration of an Autonomous System (AS)”, RFC 1930, marzo de 1996.

[4] Rekhter, Y. Li., T. et S. Hares, Eds., "A la frontier Gateway Protocol 4 (BGP-4) ", RFC 4271, janvier 2006.
[5] C. Olschanowsky ET L. Zhang J. Gersch, D. Massey. Dns resource records for bgp routing data. Internet draft, IETF, august 2012. URL https://tools.ietf.org/id/ draft-gersch-grow-revdns-bgp-01.txt.
[6] Fuller, V., Li, T., Yu, J., et K. Varadhan, "Classless Inter-Domain Routing (CIDR): Affectation d'une address et Aggregation Strategy ", RFC
1519, septembre 1993.
[7] Peter Rybazyk, Cisco Router TroubleShooting Handbook. New York: M & Books, 2000
[8] Giles Roosevelt, All-in-one CCIE Study Guide [2º Edición]. 1998
[9] Tim Boyles, Cisco CCNP Certification Library. 2001.
[10] Todd Lammle, CCNA Cisco Certified Network Associate Study Guide. 2011.
[11] Rivest R L. The MD5 message digest algorithm [EB/OL]. http://www.faqs.org/rfcs/rfcl320.html., 2005.
[12] [4] Wang Xiaoyun, Feng Dengguo, Lai Xuejia,et a1. Collisions for hash functions MD4, MD5, Haval-l28 and RIPEMD [EB/OL]. http://eprint.iacr.org/2004/199.pdf, 2004.
[13] Lai Xue Jia, An objective look at MD, SHA-l has been "cracked" [J]. National Information Security Evaluation and Certification, 2005, No.3 pp. 6-7.
[14] Z.M. Mao, R. Govindan, G. Varghese, and R.H. Katz, "Route flap damping exacerbates Internet routing convergence," Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications, 2002, pp. 221–233.

