Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Is Your Data Secure: Breach in BGP

Dr. Naasir Kamaal Khan
Associate Professor, Department of Information Technology
NIIST, NRI Group of Institutions, RGPV, Bhopal, India

Abstract— Border Gateway protocol (BGP) is inter domain routing protocol. BGP security classification is broadly classified in two planes, control plane and data plane. Control plane deals with routing policies whereas data plane talks about secure data delivery. This paper describes data plane security and breach in data delivery using example of Hash function and MD5. As a conclusion it is obtained no perfect mechanism is designed and implemented for data security whether cryptography or hash function is used in BGP sessions.

Keywords— BGP, Data Plane, sessions, breach, hash function

I. INTRODUCTION

The Internet consists of independently administered networks, which are called autonomous systems (ASes). The Border Gateway Protocol (BGP) is the de-facto interdomain routing protocol that connects ASes together [1]. BGP provides two essential services: mapping IP prefixes onto the ASes that own them and the construction of source specific paths to each reachable prefix. Every BGP router announces the IP prefixes that its AS owns in an update message and sends the message to its neighbouring BGP routers. Received update messages are recursively concatenated with an additional AS number and propagated from AS to AS forming a routing path, which will be used to forward traffic. When a BGP router receives multiple paths for the same prefix, the router chooses the best path based on multiple criteria such as path length, routing policies, etc. Although one AS may have multiple BGP routers, all BGP routers within the same AS use the same AS number. Due to the lack of security mechanisms in the current BGP protocol, attackers may spoof or tamper BGP messages. Thus, it is critical for a recipient AS to validate the authenticity and integrity of update messages before making routing decisions. Several solutions for securing BGP have been proposed earlier including public and private key approach.

II. SESSION SECURITY

A threat at the session level is that a third party may attempt to break into the TCP session, and alter the BGP message flow. There are various forms of attacks at this level [2], one form is by injection, where an intruder eavesdrops on the conversation and injects unauthentic messages into the BGP session. Eavesdropping allows the attacker to have knowledge of the TCP sequence numbers. Another form of threat is by active intermediation where an attacker sits on the wire between the two BGP nodes and intercepts all traffic in both directions. In this case an attacker node has complete control of the BGP message stream and can perform any form of message alteration. A variation of this form of threat is by session hijacking, where an attacker wiretap upon an active BGP session and injects its own traffic into the message stream that allows the attacker to take over the session and masquerade as one of the parties to the BGP session. As the overall performance of BGP depends on timing another form of attack at this level is to delay messages. Here the content of the messages are unaltered, the timing signals within the message stream are altered by this form of interposition, potentially causing the local BGP speaker to behave differently and fall out of sync with its routing peers. For example, it is possible to exercise various forms of local inhibition of routes by altering the timing of propagation of BGP messages. Another form of attack is a replay attack, where older BGP messages are replayed into a hijacked TCP session. One form of this replay attack could be to replay a pair of messages that withdraw and then declare the same address prefix [3]. Selective dropping attack [4] has a feature of dropping malicious router from the network so that communication can be established without intervention of potential intruder; this type of attack is further explained and implemented [5] to demonstrate its severity. A solution given by Khan [6] using PLECC is somewhat feasible.

III. DATA PLANE

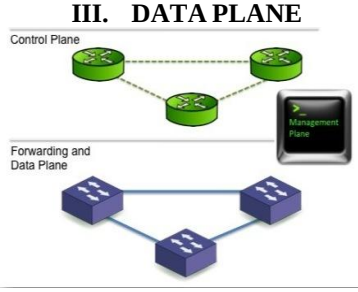

Fig 1: Control Plane and Data plane

As depicted in figure 1 Control plane deals with routing policies and data plane deals with data delivery. Data packets are transferred along data network to BGP peers. Several solutions are suggested for secure delivery of packets. Cryptographic principles are used by various researchers which increases overhead and make solution bulky. But this paper advocates that breach is possible in data plane. Hash function and message digest is used secure data packets but in hash function equation the loophole is shown below.

Hash function for strings

```
int sascii(String x, int M) {
char ch[];
ch = x.toCharArray();
int xlength = x.length();
  int i, sum;
  for (sum=0, i=0; i < x.length(); i++)
    sum += ch[i];
  return sum % M;
```

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

Fig 2 is depicted below. Breach in MD5 checksum can be done by MITM attack at padded level and when message digest is generated

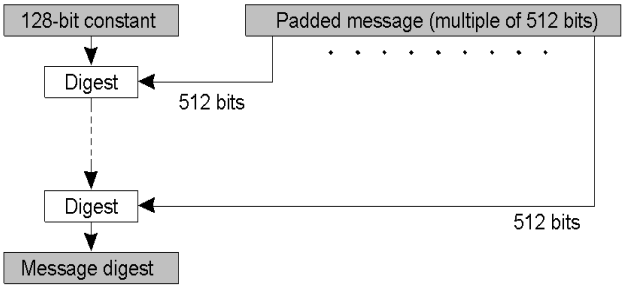

Figure 2: MD5 Checksum

IV. CONCLUSIONS

Network layer security can be achieved without securing the routing protocols as the properties such as confidentiality and integrity can be provided end-to-end by applications requiring strong security. As far as availability is concerned it is better achieved by securing data delivery rather than routing protocol. By recognizing that many applications today already require and use end-to-end security. Although there is many shortfalls in security of BGP at seesion level the problem is still open. In this paper we analysed the security weakness of BGP in data plane using example of MD5 Checksum and hash function and thus concluded that data plane is vulnerable to security breach.

REFERENCES

[1] Y. Rekhter, T. Li, and S. Hares, "*A border gateway protocol 4 (BGP-4),*" RFC 4271 (Draft Standard), Internet Engineering Task Force,Jan. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4271.txt

[2] O. Nordström and C. Dovrolis, "*Beware of BGP attacks,*" SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 1–8, 2004.

[3] K. Sriram, D. Montgomery, O. Borchert, O. Kim, and D. Kuhn, "*Study of BGP peering session attacks and their impacts on routing performance*," Sel. Areas Commun., IEEE J., vol. 24, no. 10, pp. 1901– 1915, Oct. 2006.

[4] K. Zhang, X. Zhao, F. Wu, "*An analysis of Selective Dropping Attack in BGP*", Proceedings of IEEE IPCCC, April, 2004.

[5] Lata L. Ragha, B. B. Bhaumik, S. K. Mukhopadhyay "*Malicious Dropping Attack in the Internet: Impacts and Solution*" IJCA Volume 2 – No.3, May 2010.

[6] Khan N K, Gupta G.K "*securing BGP sessions using peer link elliptic curve cryptography*" IJCSET , December 2012, Volume 2, Issue 12, 1502-1509

ABOUT AUTHOR

Naasir Kamaal Khan has received his B.E (Hons.), & M.Tech in Information Technology & Ph.D in Network Security. Over the span of 10 years of his teaching experience he has Published & Presented Several Research Papers in National & International Conferences, Delivered expert lectures in India & Abroad. He has supervised several student research projects. He is a Life Member of Indian Society of Technical Education (ISTE). His areas of interest are Cryptography & Network Security, Information & System Security and Computer Networks.

