ISSUES AND SECURITY TECHNIQUES FOR THE BORDER GATEWAY PROTOCAL

V.C Gayathri[1]
K. Arun kumar[2]
Asst.professor[12]
M. Tech (CSE)[2]
M. Tech (SE)[1]
Mallareddy Institute of science and Technology (MRITS)[12]
gayathri1252@gmail.com[1]
kandruarun002@gmail.com[2]

Abstract: The Border Gateway Protocol (BGP) is the de facto inter domain routing protocol of the Internet. Although the performance of BGP has been historically acceptable, there are continuing concerns about its ability to meet the needs of the rapidly evolving Internet. A major limitation of BGP is its failure to adequately address security. Recent outages and security analyses clearly indicate that the Internet routing infrastructure is highly vulnerable. BGP (Border Gateway Protocol) is the protocol used in the internet to exchange routing information between network domains. This protocol does not directly include mechanisms that control that route exchanged conform to the various rules defined by the Internet community. The limitations and advantages of proposed solutions are explored, and the systemic and operational implications of their designs considered. We note that no current solution has yet found an adequate balance between comprehensive security and deployment cost. This work calls not only for the application of ideas described within this paper, but also for further investigation into the problems and solutions of BGP security. This work reviews recent techniques to secure BGP. These security techniques are categorized as follows: 1) cryptographic/attestation, 2) database, 3) overlay/group protocols, 4) penalty, and 5) data-plane testing. The techniques are reviewed at a high level in a tutorial format, and short comings of the techniques are summarized as well.

Keywords: BGP, BGP Security.

I INTRODUCTION

Information on the Internet is sent via IP packets, which follow a path of routers from their source to their destination. Routers are collectively responsible for maintaining paths, or routes, to all reachable destinations on the Internet. Reach ability information is shared between routers by routing protocols. As traffic is received at a router, it is forwarded based on the reach ability information stored in the router's forwarding table, and other information stored in the packet's header. Routers on the Internet use an inter domain routing protocol called the Border Gateway Protocol (BGP) to share routing information. BGP has been around since the commercialization of the Internet and is widely deployed, maintained and researched. BGP works well in practice. However, it does not provide performance or security guarantees. BGP is a path-vector protocol which stores set of ASNs as to represent a route. Thus, the problem of loop detection is easily solved in this protocol even for larger number of nodes and hence, the protocol is easily scalable. The loop in a route can be detected in the following way - if an ASNA being added corresponding to node A to an optimal path from B (ASNB) to C (ASNC) to obtain optimal path from A to C and if it is found that ASNA already exists in the path from B to C, then there is a loop and hence, a better route between A and C is present. These attacks and misconfigurations can cause anything from an inconsequential annoyance to a devastating communications failure. For example, critical applications such as online banking, stock trading, and telemedicine run over the Internet. Significant harm may arise if communication is lost at a crucial time. As the number of critical applications on the Internet grows, so will the reliance on the underlying network infrastructure to provide reliable and secure services. Consequently, there is great interest in increasing the security of BGP, as it is essentially the glue that holds the disparate parts of the Internet together. For example, the United States government cites BGP security as part of the national strategy to secure cyberspace. In addition, the Internet Engineering Task Force (IETF) has working groups focusing on Routing Protocol Security Requirement and Secure Inter domain routing to investigate these security issues and define practical

solutions. BGP security is also a prominent topic at network operator meetings and mailing lists, such as the North American Network Operators Group (NANOG). Current research on BGP focuses on exposing and resolving both operational and security concerns. Operational concerns relating to BGP, such as scalability, convergence delay (i.e., the time required for all routers to have a consistent view of the network), routing stability, and performance, have been the subject of much effort. Similarly, much of the contemporary security research has focused on the integrity, confidentiality, authentication, authorization, and validation of BGP messages. These two fields of operational issues and security research are inherently connected. Successes and failures in each domain are informative to both communities.

II INTERDOMAIN ROUTING SECURITY

Interest in BGP grew tremendously during the 1990s [Stewart 1999]. Prior to that, few had thought deeply about routing security [Perlman 1988]. In 1995, RFCs 1771 and 1772, describing BGP4 and its application in the Internet, were published [Rekhter and Li 1995; Rekhter and Gross 1995]. Since this time, a number of issues have emerged related to using BGP for inter domain routing. Li reports issues related to the scalability, slow convergence, instability, and efficiency of inter domain routing [Li 2003]. In this survey, we focus on security related issues and defer to other sources for discussions of these and other operational concerns. BGP messages are subject to modification, deletion, forgery, and replay [Murphy 2003]. These exploits can be caused by malicious intent as well as faulty or misconfigured BGP routers. Moreover, bogus messages can originate from malicious sources or accidentally misconfigured peers. The effects of misconfiguring a BGP router can be similar to those of an attack. An analysis of BGP misconfigurations suggests that better router design could prevent most occurrences [Mahajan et al. 2002]. This study found that in the course of a day, 200-1200 prefixes, equivalent to 0.2-1% of the global routing table size, are misconfigured. Mahajan et al. identify two areas of globally visible misconfigurations in BGP:

(1) A router exports a route it should have filtered (export misconfiguration).

(2) An AS accidentally injects a prefix into the global BGP tables (origin misconfiguration).

III SECURITY TECHNIQUES

A. *Cryptographic/Certi_cate based*

Cryptographic techniques are the most effective and most used techniques for security in BGP. These techniques may range from attestation of every link on path or use some external entity To authorize, these may be certificate based or authentication of a node or encryption and issue Of keys (public and private) etc. But, they bring about overhead in messages or time required in case of verifications with external entity. Recent directions of exploration in this field are towards optimization of overheads and cycles for verification. SBGP [2] is an example of certificate based cryptographic security technique.

B. *Database based*

In Database-based approaches, the history(databases) of common paths existing is maintained. This could be used to maintain the likelihood of existence of a path. Very low probability paths advertised can be dropped in that case.

C. *Penalty based*

In Penalty based approaches, cycles of announcement and with drawl of paths is monitored. The paths with frequent such cycles are penalized and generation of update messages is delayed. As router misconfiguration updates are short lived, giving time would prevent unnecessary updates. Thus, along with decreasing bad routes propagation, network gets time to recover from generated bad routes.

IV BGP SECURITY TODAY

Securing inter domain routing has been a challenge for many years. Seminal work by Perlman showed that a fundamental problem in securing protocols like BGP is that routers may exhibit Byzantine, or faulty and possibly malicious, behavior. Consequently, a secure inter domain routing protocol must display Byzantine robustness; that is, in the face of malicious or faulty behavior from other hosts, all non-faulty hosts in the system should reach a decision on a particular message's contents within a finite time period (termination), this decision should be the node (validity). Existing solutions to date largely only provide some facets of Byzantine robustness. The majority of defenses that have been implemented by ISPs to protect BGP have focused on solutions that can be implemented locally or require only limited interaction with parties outside the local administrative domain. In particular, protection of the underlying TCP connection and defensive filtering of BGP announcements are the most commonly implemented solutions, with some limited deployment of cryptographic protections between routers. However,

these solutions are ultimately limited in the protections they can offer against more complex and sophisticated attacks that target BGP itself. Ultimately, a more complete view of which routes are valid is necessary for protecting against this latter class of attacks. In this section, we describe the currently-implemented solutions and levels of protection they provide, starting with an overview of the cryptographic techniques used in many of the current and proposed solutions for improving BGP security.

A. MD5 passwords on BGP peerings

BGP sessions can be secured with MD5 passwords to protect against attacks that could bring down the session (by sending spoofed TCP RST packets) or possibly insert packets into the TCP stream (routing attacks). The drawback of TCP/MD5 is additional management overhead for password maintenance. MD5 protection is recommended when peerings are established over shared networks where spoofing can be done (like internet exchanges, IXPs). You should block spoofed packets (packets with source IP address belonging to your IP address space) at all edges of your network, making TCP/MD5 protection of BGP sessions unnecessary on iBGP session or EBGP sessions run over point-to-point links.

B. BGP TTL security

BGP sessions can be made harder to spoof with the TTL security. Instead of sending TCP packets with TTL value = 1, the routers send the TCP packets with TTL value = 255 and the receiver checks that the TTL value equals 255. Since it's impossible to send an IP packet with TTL = 255 to a non-directly-connected IP host, BGP TTL security effectively prevents all spoofing attacks coming from third parties not directly connected to the same subnet as the BGP-speaking routers.

C. BGP route flap dampening

BGP route flap dampening mechanism makes it possible to give penalties to routes each time they change in the BGP routing table. Initially this mechanism was created to protect the entire internet from multiple events impacting a single network. RIPE community now recommends not using BGP route flap dampening

.Author of this document proposes to follow the proposal of the RIPE community.

V BGP VULNERABILITY

Vulnerabilities provide an open door for attacks on the Internet. Currenty, inter domain routing is vulnerable to a number of specific attacks [Murphy 2003]. These threats manipulate the three distinct types of BGP communication: control messages when setting up a session, or reach ability updates and error messages throughout the duration of a session. The following describes and highlights the effect of these attacks:

A.Eavesdropping:

An adversary passively listens to data on the wire. This gives the adversary access to sensitive policy and route information being forwarded between ASes. Note that inter domain routing information is not widely viewed as sensitive. However, because it may expose the existence and details of commercial relationships, organizations often desire that exchanged peering policy be kept confidential.

B. Replay:

An adversary records messages and resends them to the original recipient. This approach can be used to confuse the routing protocols by re-asserting width drawn routes or withdrawing valid ones. When sent in bulk, these messages

can overwhelm the victim routers, causing a denial of service attack.

C. Message insertion:

An adversary inserts forged messages into a BGP session. These messages can erroneously terminate BGP sessions between peers or inject bad routing data. While BGP does not directly protect against this, its transport protocol, TCP, provides limited protection. TCP uses sequence numbers to preserve the ordering of packets [J 1981]. Because sequence numbers are often unpredictable, an adversary with limited abilities will find it difficult to insert forged BGP messages. Of course, adversaries who can eavesdrop or hijack the BGP session can trivially inject forged messages.

D. Message deletion:

An adversary intercepts and deletes a message passed between BGP peers. Deleted BGP UPDATE messages can lead to inaccurate routing tables. Again, TCP provides limited protection against this kind of attack.

E. Message modification:

An adversary removes messages from a BGP session, modifies them, and reinserts them. Like message

insertion, this also leads to inaccurate routing (possibly across compromised links) and/or the breaking of peering relationships, resulting in routing failures.

VI CONCLUSION

BGP has been quite successful in providing relatively stable inter domain routing. Enhancements to the protocol, such as TCP MD5 Signatures, serve to add much needed security measures. This survey exposes areas where it is commonly believed that BGP still needs improvements in security. Inter domain routing security has progressed since being first investigated by Perlman, but few production environments are demonstrably more secure than they were when she began that work. Some operators are using incremental solutions that offer some protection, but comprehensive solutions have not been deployed. Notably, no solutions requiring more than lightweight cryptography have been deployed. There is a resistance in the operations community to using any sort of cryptography in networks, largely due to the costs imposed. In addition, there is resistance to a global PKI (required to deploy many of the security solutions) with a single root of trust; such issues are problematic with PKI in general [126]. Many of these issues must be solved before effective BGP security solutions can be deployed. Because of the global impact of even minor errors in BGP configuration and operation, such deployment is increasingly imperative. This survey has examined the threats to BGP and proposed solutions to ensure its security. While they have not been implemented yet in practice, and while their adoption may be difficult, good progress has been made. In the end, a methodology to securing BGP may be one of the best way to ensure that the Internet remains a reliable and
useful vehicle for private and public communication.

REFERENCES

[1] J. Hawkinson and T. Bates, "Guidelines for creation, selection, and registration of an autonomous system (AS)," RFC 1930, 1996.

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

[3] J. Stewart, BGP4: Inter-Domain Routing in the Internet. Reading, MA: Addison-Wesley, 1999.

[4] R. Barrett, S. Haar, and R. Whitestone, "Routing snafu causes Internet outage," Interactive Week, April 25 1997.

[5] P. Boothe, J. Hiebert, and R. Bush, "How prevalent is prefix hijacking on the Internet?" February 2006, NANOG 36, http://www.nanog. org/mtg-0602/boothe.html.

[6] Rensys Blog, "Con-Ed steals the 'Net," http://www.renesys.com/blog/2006/01/conedn stealsn then net.shtml.

[7] "Pakistan hijacks YouTube," http://www.renesys.com/blog/2008/02/pakistann hijacksn youtuben 1.shtml.

[8] A. Ramachandran and N. Feamster, "Understanding the network-level behavior of spammers," in ACM SIGCOMM, August 2006.

[9] H. Ballani, P. Francis, and X. Zhang, "A study of prefix hijacking and interception in the Internet," in ACM SIGCOMM, August 2007.

[10] Department of Homeland Security, "The national strategy to secure cyberspace," Feb. 2003.

[11] Routing Protocol Security Requirements, http://www.ietf.org/html.charters/rpsec-charter.

[12] Secure Inter-Domain Routing, http://www.ietf.org/html.charters/sidr-charter.html.

[13] North American Network Operators Group, www.nanog.org.

[14] N. Spring, R. Mahajan, and D. Wetherall, "Measuring ISP Topologies with Rocketfuel," IEEE/ACM Transactions on Networking, vol. 12, no. 1, pp. 2–16, Feb. 2004.

[15] W. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," RFC 4987, Aug. 2007.

I am V.C Gayathri, I did My B. Tech (IT) in JNTUH and I did my M.Tech (SE) in JNTUH. Now I am working as Assistant Professor in Mallareddy institute of science and technology(MRITS) in CSE department.

I am K. Ramesh. I did my B. Tech (CSE) in JNTUH and My M.Tech (CSE) in JNTUK. I am working as a Asst. Professor in IT department in Mallareddy Institute of science and technology (MRITS).