Research Paper Computer Science

Security of Border Gateway Protocol

* Sridevi

* Assistant Professor, Department of Computer Science, Karnatak Univerity,Dharwad

ABSTRACT

This paper discuss the current methodologies used by ISPs to secure their Border Gateway Protocol routing infrastructure. Then, it covers the security requirements needed to minimize the issues and mainly concentrates on the security problems that should be emphasized to provide a protection at the BGP protocol level.

Keywords :

1. Introduction

Although not well known among everyday users, the Border Gateway Protocol (BGP) is one of the critical infrastructure protocols for the Internet. BGP is a routing protocol, whose purpose is to keep systems on the Internet up to date with information needed to receive and transmit traffic correctly. Sending and receiving email, viewing Web sites, and performing other Internet activities require the transmission of messages referred to as packets. Packets sent on the Internet contain source and destination addresses, much like paper mail sent in envelopes. But packets do not go directly from a user's computer to their destination. Many intermediate systems may be involved in the transmission, and because there are many paths from one point to another, not all packets follow the same path between source and destination. The systems that packets pass through from one point to another all need to know where to forward a packet, based on the destination address and information contained in a routing table.

The routing table says, for example, that packets with a destination of A can be sent to system H, which will then forward the packets to their destination, possibly through other intermediate nodes. Because the Internet changes continuously, as systems fail or are replaced or new systems are added, routing tables must be updated constantly. BGP is the protocol that serves this purpose for the global Internet. When BGP fails, portions of the Internet may become unusable for a period of time ranging from minutes to hours. Most of the risk to BGP comes from accidental failures, but there is also a significant risk that attackers could disable parts or all of network, disrupting communications.

2. Current Protection Mechanisms for BGP

Since BGP is the main protocol used in interdomain routing, securing it by any means while research is in progress is a must for all ISPs. Generally, the protection mechanisms used nowadays is to protect the TCP session from attacks. Actually, it is not for protection but only making it harder for attackers to affect ISPs and their upstream providers and downstream customers. Moreover, traffic filtering is used extensively in border routers.

2.1 TCP MD5 Authentication

TCP MD5 is not part of the BGP protocol and is implemented by most ISPs. it is used to protect BGP sessions against the introduction of spoofed TCP segments into the connection stream. It is used for each message exchanged between peers. However, a password or key is chosen manually and inputted as such in both ends of the session. Considering thousands of routers used concurrently, maintaining shared secrets between them is extremely complicated. Furthermore, these shared secrets need to be changed regularly or they will be subject to different attacks against the cryptographic function. In addition, it will add more complexity to key management, since it is manual.

2.2 IPsec

It is not widely used by ISPs to protect their BGP sessions. This is a protection mechanism for the layer three IP datagram. IPsec is widely used for tunnelling VPNs over Internet between endpoints when transmitting confidential or important data [3,4]. This security mechanism can be used to protect BGP sessions from Integrity violation, Replay and DoS attacks through its Authentication Header protocol (AH). It can also be extended to an additional confidentiality security service via its Encapsulating Security Payload (ESP). In addition, it can dynamically negotiate secret keys and has an implemented key management mechanism. The latter uses the IPsec Internet Security and Key Management Protocol (ISAKMP) [5] and the Internet Key Exchange (IKE) [6]. IPsec is used to protect the BGP peering sessions by implementing Virtual Private Networks [7]. The implementation of this safeguard is efficient to tackle BGP session local vulnerabilities. However, it does not address widespread attacks and cannot scale with them.

2.3 Generalised TTL Security Mechanism (GTSM)

This is a security mechanism that prevents attackers from remotely sending BGP spoofed messages to targets. This mechanism uses the TTL attribute in the IP packet. The TTL is a value that is decremented at every hop and if reaches zero (0), the packet is dropped. Originally, between BGP peers TTL is set to 1 by the sending router. As illustrated in the last chapter in spoofing attacks, an attacker can set the TTL by counting the number of hops so that it arrives to the target with the value 1. This mechanism uses a different value to be set between peers. Peers that require multi hops to reach each other are rare. Thus, GTSM uses a TTL with a value 255 for the sending speaker. The receiving peer needs to check that the value of TTL is not less than 254. If it is not the case, the packet is dropped or flagged according to the implementation. This will assure that no remote attack can be conducted.

The following is a table1 that shows the efficiency of those three techniques to protect peering sessions [9].

	Integrity	DoS prevention	Replay Prevention	Confidentiality
MD5 Integrity	Yes	No	Yes	No
AH (IPsec)	Yes	Yes	Yes	No
ESP (IPsec)	Yes	Yes	Yes	Yes
GTSM	No	No	No	No

Table 1: **BGP Peer Session Security Mechanisms**

This technique is conducted using defensive routing policies. The latter are used to filter out malicious or suspicious announcements. This includes checking for hazardous and risky attributes of UPDATE messages. Most ISPs, for example, implement ingress and egress filters derived from routing policies. They use lists of loopback addresses and addresses with no match, in a document called Documented Special Use Addresses (DUSA), provided by IANA. These filters can parse all BGP messages and especially UPDATE messages to retrieve and drop malicious looking packets. This method is a good defence method but this depends on the policies and filters which become very messy and hard to control after a while.

3. Security Requirements

In order to protect interdomain routing, the solution has to consider many parameters that relate to the protocol itself. Thus, there needs to be a few requirements set that define correct operation of BGP as a protocol and speakers. This means that any attack against BGP ought to determine a non-correct operation. The security services that should be provided for proper BGP operation are the authenticity, freshness and integrity of the routing information exchanged. In addition, a BGP speaker's decision process, storing and distribution of routing information must be in accordance with the BGP specification and routing policies established by ASes [10].

Initially, high level requirements should be put in place before setting the more detailed ones. Firstly, any security architecture must not rely on mutual trust amongst subscribers and ISPs. There must be no trust between entities because there are some parties that can never be trusted, and those that can be, are prone to error, misconfigurations or can be apprehended by a malicious adversary. Secondly, the elements of security solutions must exhibit similar dynamics as the parts of BGP they protect. This means that the solution must scale within the BGP architecture and protocol. Moreover, it must be backward compatible, which means that the deployment of the solution can be incremental. Thirdly, the resources required for the solution ought to be in the same range of requirements of memory and processing power for BGP. Thus, the solution should demonstrate similar reliability, efficiency and performance. Fourthly, the security services described before (i.e. integrity, freshness and data origin authentication) must be assured at the traffic itself. For the fifth point, BGP routers should be capable of verifying not only the owner of each prefix that authorised the origin AS, but also that each succeeding AS in the path has been authorised by its predecessor [1].

Following the high level needs, more specific requirements can clarify the objectives for securing BGP. These requirements are well illustrated in [10] by S. Kent et.al. The main concern in BGP is the security of UPDATE messages, since they define the healthiness of routing tables. If UPDATE messages are malicious, then the whole routing infrastructure functions wrongly leading to disastrous communication on the Internet. Thus, to ensure security, the following requirements need to be realised. Firstly, the UPDATE message should be kept integral and authentic. The BGP speaker receiving the UPDATE message must be able to validate that it was sent by the intended peer. Moreover, it can verify that the message was not modified while in transfer and the routing information is fresh and not replayed. Secondly, there must be a mechanism implemented that ensures that the receiver of the UPDATE message is the intended one. Thirdly, the receiving speaker must be able to verify that the sending peer is authorised to advertise routing information on behalf of its AS. As a fourth requirement, there must be a method to verify any prefix advertised in an UPDATE that it was authorised by its parent organisation to own that address space. Fifthly, a BGP speaker receiving an UPDATE message must be able to verify that the first AS in the route was authorised to advertise the prefixes by the owners of their address spaces. Another requirement is the ability of a receiving speaker to verify withdrawals. The verification encompasses the ability to confirm that the peer before withdrawing the route was a legitimate advertiser of that route. Seventhly, a security mechanism needs to be applied to make ensure the well functioning or the BGP decision process and operations. This covers speaker's BGP rules, its AS's routing policies for storage, modification and distribution, decision process, and deriving the forwarding table. Finally, the receiving BGP speaker must apply correctly its decision process and routing policies to decide whether to accept the UPDATE message or reject it. Because the routing policies are not defined in BGP and left to the AS's administration, the last two security requirements are not reliable to securing BGP and should be done separately. If they have to be included, the semantics of BGP itself need to be changed since the protocol does not address this issue.

4. BGP Security Problems

After specifying the security requirements for BGP, security problems can be derived from it. These are the current main efforts that are focused on to provide higher security for the protocol. From the previously derived requirements, the main focus on securing BGP deals with UPDATE messages and the environment that they depend on. As described in [1], T. Vardar has provided three main security problems for BGP: Hop Integrity, Origin

Authentication, and Path Validation.

4.1 Hop Integrity

Gouda et.al. define in [11] the state of a computer network providing hop integrity. If a router A receives a message M from a router B, the A can check that M was not altered during transmission and is not a replay of an old message [51]. However, BGP does not provide this service. To do so, it needs to provide Data Integrity and Source Authentication. Messages ought to be verified at each hop to ensure that they have not been altered, replayed, destroyed in both an unauthorised and accidental way. As defined previously, source authentication represents the validation that the sender of the messages is a legitimate one and not an imposter. These are the two services that need to be addressed properly to provide hop integrity.

4.2 Origin Authentication

This represents the evidence that the data received is the one that should be received. It represents the validation of claims of address ownership from ASes. This will allow a speaker for example to authenticate a BGP peer. Then, it needs to be able to verify that it is authorised to advertise routes. Since the Internet is somehow hierarchical in the provision of AS numbers and IP addresses and prefixes (Chapter 1), this hierarchy should be kept to validate the AS chains of address ownership. This can be used in a PKI (Public Key Infrastructure) format or any means that can provide this service.

4.3 Path Validation

BGP UPDATE message contains a prefix and its associated AS path to reach it. Path validation should allow that the path of ASes is valid and should reach the intended prefix. This means that each BGP speaker in the path must be reachable by the previous one. Moreover, each AS present in the path must be authenticated. This ensures that a malicious UPDATE that contains false routes will not be used.

5. Conclusion

BGP was provided with a few security mechanisms, it has not shown that it is safe and secure. Moreover, these mechanisms are independent from the protocol and they represent measures applied only by those who want to. Thus, mechanisms inclusive to the protocol should be designed and implemented. Thus, the security requirements for BGP were defined with the security problems that raise the white flag. However, research has brought us a few still debatable solutions to this issue.

REFERENCES

[1] Tuna Vardar, "SECURITY IN INTERDOMAIN ROUTING", Helsinki University of | Technology, T-110.551 Seminar of Internetworking, 2004. | [2] H. Krawczyk et. al. “HMAC: Keyed-Hashing for Message Authentication”, Internet | Engineering Task Force, April 1997, RFC 2104. | [3] S. Kent and R. Atkinson. “Security Architecture for the Internet Protocol”, Internet | Engineering Task Force, November 1998, RFC 2401. | [4] R. Thayer et. al. “IP Security Document Roadmap”, Internet Engineering Task Force, | November 1998, RFC 2411. | [5] D. Maughan et. al. “Internet Security Association and Key Management Protocol | (ISAKMP)”, Internet Engineering Task Force, November 1998, RFC 2408. | [6] D. Carrel et. al. “The Internet Key Exchange”, Internet Engineering Task Force, | November 1998, RFC 2409. | [7] G. Armitage et. al. “A Framework for IP Based Virtual Private Networks”, Internet | Engineering Task Force, February 2000, RFC 2764. | [8] V. Gill et. al. “The Generalized TTL Security Mechanism (GTSM)”, Internet Engineering | Task Force, February 2004, RFC 3682. | [9] K. Butler et. al. “A Survey of BGP Security Issues and Solutions”, AT&T Labs Research, | January 2008. | [10] S. Kent, et. al. “Secure Border Gateway Protocol (Secure-BGP)”, IEEE Communications | Vol. 18, No. 4, pp. 582-592, April 2000. | [11] M. G. Gouda et. al. “Hop Integrity in Computer Networks”, Proceedings of the IEEE | International Conference on Network Protocols, 2000. |