ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 5, May 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Constructing IDPF to control IP Spoofing Based on BGP Updates

Vikrant G. Madankar[1]
Department of Information Technology,
H.V.P.M's C.O.E.T
Amravati – India

Prof. Ranjit R. Keole[2]
Department of Information Technology,
H.V.P.M's C.O.E.T
Amravati – India

Abstract: IP spoofing is a well-liked method to initiate Distributed Denial of Service attacks. Numerous mitigation schemes have been proposed to detect fake source IP addresses. IP spoofing remains a problem today in the Internet. Solution for this problem is interdomain packet filters. The packet filters rely on the information that BGP updates are valid and reliable. Packet filter uses implicit information enclosed in BGP rout updates. Attackers may use false source IP address to hide their real locations. This paper proposes an interdomain packet filter design that can alleviate the level of IP spoofing on the network. Main characteristic of this scheme is that it does not need global routing information. Interdomain packet filters are constructed from the information implicit in Border Gateway Protocol route updates and are deployed in network border routers.

Keywords: BGP; Interdomain routing; Packet filter; DDoS attack; IP Spoofing.

I. INTRODUCTION

The Internet is composed of thousands of network Domains. Each of them is a logical collection of networks under the common administrative control. A number of notorious attacks rely on IP spoofing, including SYN flooding, SMURF, DNS amplification. The interdomain routing scheme underpins almost all the activities on the Internet, and plays a crucial role in the user-alleged end to end network performance. To capture the origins of IP spoofing traffic is of more important. As long as the real locations of spoofers are not disclosed, they cannot be deterred from launching further attacks. Packets arriving at a destination domain with an invalid authentication key are spoofed packets and are discarded. The filter based packet filtering is a key technology to defend against the DDoS attacks. Protecting against DDoS attacks is not easy for two reasons. First, the numbers of attackers involved in a DDoS attack are very large. Although the traffic sent by a single attacker might be little, the volume of aggregated traffic arriving at the victim host is devastating. Second, attackers typically spoof their IP address, which makes it very tricky to trace the attack traffic back to its sources.

The advantage of sending a spoofed packet is that the sender has some kind of spiteful intention and does not want to be recognized. We can trace the location of the sender by using the source address in the header of an IP datagram. Mainly systems keep logs of Internet activity, so if attackers want to hide their identity, they need to modify the source address. The host which will receive the spoofed packet responds to the spoofed address, so the attacker will not receive reply back from the victim host. Although the spoofed address belongs to a host on the same subnet as the attacker, then the attacker can sniff the reply. IP spoofing can be used for several purposes, for some scenarios an attacker may want to inspect the response from the target victim called non-blind spoofing, whereas in other cases the attacker might not care called blind spoofing.

Packet filtering is the method of selective passing or blocking of data packets as they pass through a network interface. Filter rules clearly describes the criteria that a packet must match and when a match is found the resulting action, either block or pass, is taken. Filter rules are evaluated in successive order, first to last. The Existing System uses Route Based Packet Filters for controlling Ip spoofing. In the existing system the idea is to assume a single path routing, there is exactly one single path between source nodes and the destination node. Hence any packet with source address and destination addressed that appear in a router that is not in the path specified then that packet is discarded. Also the existing system uses Network Ingress Filters, which prevents a specific Network from being used for attacking others.

II. RELATED WORK

The basic idea of inter domain packet filter is based on the study of the association among network topology and the usefulness of route based packet filtering. Unicast invalidate path forwarding requires that a packet is forwarded simply when the interface that the packet arrives on is accurately the same used by the router to reach the source IP of the packet. In the case when interface does not match, then the packet is discarded. On the other way, the method is imperfect given that Internet routing is inherently asymmetric, i.e., the forward and reverse paths among a pair of hosts are repeatedly quite different. Hence, the loose mode is less efficient in detecting spoofed packets. In Hop-Count Filtering, system at each end will uphold a mapping between IP address aggregates and valid hop counts from the origin to the end system.

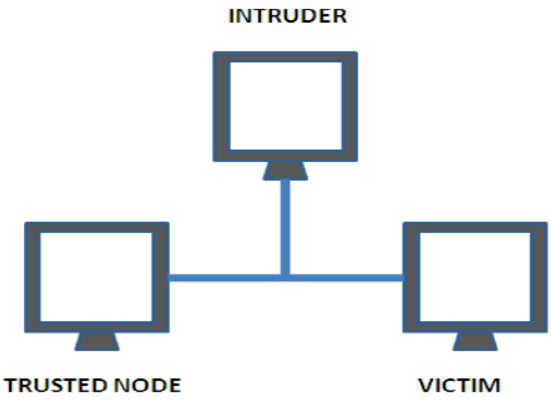

Fig. 1 Role of Intruder in Communication.

Fig. 1, shows the role of intruder in communication. Intruder is interrupting between trusted node and victim. Packets that appear with a disparate hop count are doubtful and are therefore leftover or marked for further processing. In Path recognition each packet along a path is marked by a unique Path identifier of the path. Victim nodes can filter packets based on Path carried in the packet header. StackPi enhanced the incremental deployment property of Path by proposing two new packet marking schemes. In the Packet Passport System, a packet originated from a participating prefecture carries a passport that is computed based on secret keys pooled by the source domain and the shipment domains from source to destination. The packets carrying an invalid passport are leftover by the transit domains.

In the Network Ingress Filtering function, traffic originating from a network is forwarded only if the source IP in the packets belongs to the network. Ingress filtering principally prevents a specific network from being used to attack others. Thus, while there is a combined social benefit in everyone deploying it, individuals does not obtain direct incentives. Packet filters resulting from the global routing information can significantly limit IP spoofing when deployed in just a small number of ASs.

III. IP TRACKBACK SCHEME

IP traceback is a method used to locate the source of an IP packet on the Internet without trusting on the source IP address field. Because of the credulous nature of the IP protocol, the source IP address of a packet is not authenticated. As a outcome, the source address in an IP packet can be spoofed.

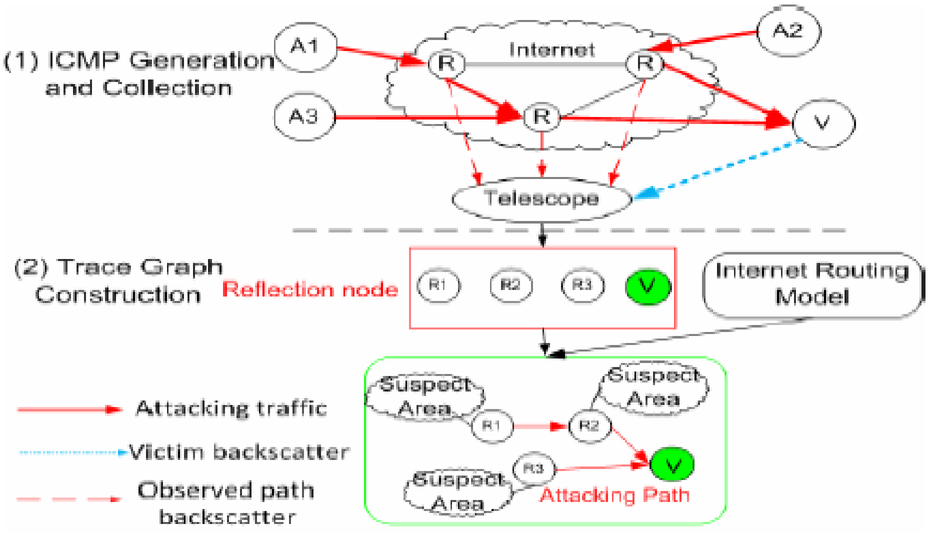

Fig. 2 Passive IP Traceback.

Fig. 2, shows passive IP traceback, Such a type of spoofed IP packets can be used for different attacks. The difficulty of finding the source of a packet is called the IP traceback problem. IP traceback has a significant ability for identifying sources of attacks and instituting defence channel for the Internet. Mainly active approaches to this problem have been adapted toward DDoS attack detection. Inter Domain Packet Filter is used to find the feasible routes. If the packet is not amongst the set of the feasible routes, it is detected as spoofed packet and is discarded. The spoofed packet's route is traced to detect the intruder. IP traceback is a name specified to a method for constantly determining the source of a packet on the Internet. Owing to the credulous nature of the IP protocol, the source IP address of a packet is not authenticated.

IP traceback technology can be used to traceback the source of spoofed attack packet and rearranges attack graph by tracing attack paths and the sender or receiver of packets. There are numerous representative techniques such as the technique using marking tactic focusing on packets, the technique controlling escape path information of the source packet all the way through deformation of ICMP protocol and other protocols and the technique using managing protocol from the aspect of network structure. Each traceback method has its own strength and weak point and has diverse presentation by means of its deployment location of traceback element and the characteristics of hacking scheme. Existing IP Traceback methods can be considered as proactive or reactive tracing. Proactive tracing prepares information for tracing when packets are in transfer. Reactive tracing starts tracing past an attack is detected.

IV. Role of Border Gateway Protocol

In particular, BGP network design was undertaken in the comparatively homogenous and equally trusting environment of the early Internet. The original distributed distance vector computations rely greatly on relaxed trust models associated with information propagation to create reliable and correct results. The approach to information exchange was not primarily measured for forcefulness in the face of various forms of negotiated conviction or overt hostility on the part of some routing nodes in the network. BGP has numerous well-known vulnerabilities. These vulnerabilities are the undeviating consequences of three elementary weaknesses in the BGP and the inter-domain routing environment. The first weakness is there is no mechanism to confirm the integrity, freshness and source authenticity of BGP communication. Also, BGP doesn't offer any mechanism to authenticate the authenticity of an address prefix and an AS instigation of this prefix in the routing scheme. Last, the BGP protocol doesn't offer any way to assurance that the attributes of a BGP UPDATE message are correct.

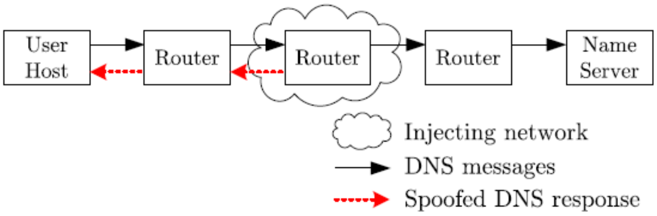

Fig. 3 Injection of Spoofed DSN response.

The principle of this type of attack is shown in Fig. 3. The spoofed reaction contains an IP address that diverts the abuser application to the incorrect server or to an inaccessible destination. The attacker may well also spoof a negative answer with a name declaration or server error in its place to prevent contact to the server.

The need of security concepts in BGP plants it vulnerable to several types of control plane attacks. In addition, the IDPF method, which relies on BGP updates to detect and prevent source IP address spoofing, will fail if the BGP updates are not correct. The IDPF method assumes that BGP routing updates are secure and hence trustworthy. However, by accepting fake BGP updates, the IDPF filters become fewer effective. The presentation of IDPF scheme suffers when unfriendly nodes, which can create non-trustable BGP updates and hence produce incorrect filters, are introduced in the network. This turn down in IDPF performance can be in prison by deploying a mechanism to secure BGP. At there are a numeral practical and a number of more essential questions unfolding to securing BGP. The first is a practical question unfolding to the inevitable design exchange between the level of security and the presentation overheads of processing security recommendation connected with BGP UPDATE messages. It is not completely known as to what aspects of BGP performance and load are significant for the robust operation of network applications and what are not so decisive. With such considerations, it is extremely imperative that any answer to secure BGP should try and minimize collision on current schedule of BGP and should be incrementally deployable. Given this, there is a sturdy incentive to alter BGP such that it will present reasonable amount of security at both control plane and data planes and will have negligible impact on BGP messaging. Route instigation validation score is unoriginal based on the ability of a route receiving node to conclude whether the AS originating the route in reality is authorized to do so. Route AS-Path substantiation score is derived based on the capability to which the node is able to establish whether the received update truly traversed the ASs listed in the AS Path.

V. CONCLUSION

This paper aims to address the challenges in the network security. Above work, concludes that the IDPF architecture as a important countermeasure to the IP spoofing- based DDoS attacks. IDPFs rely on BGP update messages exchanged on the Internet to infer the validity of source address of a packet forwarded by a neighbor. Work done in this field showed that IDPFs can easily be deployed on the current BGP-based Internet routing architecture. We have studied the conditions under which the IDPF framework can correctly work without discarding any valid packets.

We found the conditions, under which the IDPF framework appropriately works in that it does not reject packets with valid source addresses. According to the simulation studies, it is found that, even with partial deployment on the Internet, IDPFs can proactively bound the spoofing capability of attackers, as well as they can help to localize the origin of an attack packet to a small number of candidate networks.

ACKNOWLEDGEMENT

I would like to thank my Guide, Prof. R. R. Keole and Principal Dr. A. B. Marathe, who provided me constructive and positive feedback during the preparation of this paper.

References

1. Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson, "Network Support for IP Traceback" IEEE/ACM Transactions on Networking, Vol. 9, No. 3, June 2001.
2. Lixin Gao, "On Inferring Autonomous System Relationships in the Internet" IEEE/ACM Transactions on Networking, Vol. 9, No. 6, December 2001.
3. Ramana Rao Kompella, Sumeet Singh and George Varghese, "On Scalable Attack Detection in the Network" IEEE/ACM Transactions on Networking, Vol. 15, No. 1, February 2007.
4. Ruiliang Chen, Jung-Min Park, Randolph Marchany, "A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks" IEEE Transactions on Parallel and Distributed Systems, Vol. 18, No. 5, May 2007.
5. Ming-Hour Yang and Ming-Chien Yang, "RIHT: A Novel Hybrid IP Traceback Scheme" IEEE Transsactions on Information Forensics and Security, Vol. 7, No. 2, April 2012.
6. Bingyang Liu, Jun Bi, and Athanasios V. Vasilakos, "Toward Incentivizing Anti-Spoofing Deployment" IEEE Transactions on Information Forensics and Security, Vol. 9, No. 3, March 2014.
7. Zhenhai Duan, Xin Yuan, and Jaideep Chandrashekar, "Controlling IP Spoofing through Inter domain Packet Filters" IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 1, January-March 2008.
8. Basheer Al-Duwairi and Manimaran Govindarasu, "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback" IEEE Transactions on Parallel and Distributed Systems, Vol. 17, No. 5, May 2006.
9. Abraham Yaar, Adrian Perrig, and Dawn Song, "StackPi : New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense" IEEE Journal on Selected Areas in Communications, Vol. 24, No. 10, October 2006.
10. Haining Wang, Cheng Jin, and Kang G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering" IEEE/ACM Transactions on Networking, Vol. 15, No. 1, February 2007.
11. Jelena Mirkovic and Ezra Kissel, "Comparative Evaluation of Spoofing Defenses" IEEE Transactions on Dependable and Secure Computing, Vol. 8, No. 2, March-April 2011.
12. Alberto Garcia-Martinez and Marcelo Bagnulo, "An Integrated Approach to Prevent Address Spoofing in IPv6 Links" IEEE Communications Letters, Vol. 16, No. 11, November 2012.
13. Junaid Israr, Mouhcine Guennoun, and Hussein T. Mouftah, "Mitigating IP Spoofing by Validating BGP Routes Updates" International Journal of Computer Science and Network Security, VOL.9 No.5, May 2009.
14. Guang Yao, Jun Bi, and Athanasios V. Vasilakos, "Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter" IEEE Transactions on Information Forensics and Security, Vol. 10, No. 3, March 2015.

AUTHOR(S) PROFILE

Mr. Vikrant G. Madankar, has received the B.E.degree in Computer Science from H.V.P.M's College Of Engineering And Technology, Amravati in 2014. He is currently pursuing Master's Degree in Computer Science and Information Technology from H.V.P.M's College of Engineering And Technology, Amravati.

Prof. Ranjit R. Keole, has received the B.E. and M.E degree in Computer Science from Prof. Ram Meghe Institute of Technology, Badnera in 1992 and 2008, respectively. His field of specialisation is web Mining. He is currently working as Associate Professor at H.V.P.M's college of Engineering and Technology, Amravati.