ENGINEERING AND TECHNOLOGY IN INDIA
Volume 1 Issue 2 (October, 2010) Page : 110-114

REVIEW ARTICLE

Accepted : June, 2010

A method to prevent IP spoofing attacks

R. ABIRAMI ARASI, K. KUPPUSAMY AND T. RAJENDRAN

Key words : I.P. spoofing, Spoofing attack

Distributed Denial - of - Service (DDoS) attacks pose an increasingly grave threat to the Internet, as evident in recent DDoS attacks mounted on both popular Internet sites and the Internet infrastructure. Alarmingly, DDoS attacks are observed on a daily basis on most of the large backbone networks one of the factors that complicate the mechanisms for policing such attacks is IP spoofing, which is the act of forging the source addresses in IP packets. By masquerading as a different host, an attacker can hide its true identity and location, rendering source based packet filtering less effective. It has been shown that a large part of the Internet is vulnerable to IP spoofing.

Recently, attackers have increasingly been staging attacks via botnets. In this case, since the attacks are carried out through intermediaries, that is, the compromised "bots" attackers may not utilize the technique of IP spoofing to hide their true identities. It is tempting to believe that the use of IP spoofing is less of a factor. The ICANN Security and Stability Advisory Committee made three recommendations. The first and long-term recommendation is to adopt source IP address verification, which confirms the importance of the IP spoofing problem.

IP spoofing will remain popular for a number of reasons. First, IP spoofing makes isolating attack traffic from legitimate traffic harder: packets with spoofed source addresses may appear to be from all around the Internet. Second, it presents the attacker with an easy way to insert a level of indirection. As a consequence, substantial effort is required to localize the source of the attack traffic. Finally, many popular attacks such as man - in - the - middle attacks, reflector - based attacks and TCP SYN flood attacks use IP spoofing and require the ability to forge source addresses. Based on this observation, Park and Lee proposed the route - based packet filters as a way of mitigating IP spoofing. The idea is that by assuming single - path routing, there is exactly one single path p (s, d) between the source node s and the destination node d. Hence, any packet with the source address s and the destination address d that appear in a router that is not in p (s, d) should be discarded.

These study mainly concentrate on following objectives to describe how can practically construct IDPFs at an AS by only using the information in the locally exchanged BGP updates; to establish the conditions under which the proposed IDPF framework works correctly in that it does not discard packets with valid source addresses; and to evaluate the effectiveness of the proposed architecture, we conduct extensive simulation studies based on AS topologies and AS paths extracted from real BGP data.

Content on a spoofed page, the highjacker can gain access to sensitive information or computer or network resources. He could steal or alter sensitive data, such as a credit card number or password, or install malware. The highjacker would also be able to take control of a compromised computer to use it as part of a zombie army in order to send out spam. Web site administrators can minimize the danger that their IP addresses will be spoofed by implementing hierarchical or one - time passwords and data encryption / decryption techniques. Users and administrators can protect themselves and their networks by install ting and implementing firewalls that block outgoing packets with source addresses that differ from the IP address of the user's computer or internal network.

Methods of attack:

A "denial - of - service" attack is characterized by an explicit attempt by attackers to prevent legitimate users

Abirami Arasi, R., Kuppusamy, K. and Rajendran, T. (2010). A method to prevent IP spoofing attacks, *Engg. Tech. India,* **1** (2) : 110-114