IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 5, Ver. I (Sep. – Oct. 2015), PP 01-02
www.iosrjournals.org

Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates

Shyam Chandran.P , Lisi Mohanraj
M.Sc.,M.Phil.,(AssistantProfessor), LisiMohanraj M.Sc.,(Research Scholar)
Computer Science/Sree Narayana Guru College, Coimbatore, T.N, India

Abstract: *The Distributed Denial-of-Service (DDoS) attack is a serious threat to the legitimate use of the Internet. Prevention mechanisms are thwarted by the ability of attackers to forge or spoof the source addresses in IP packets. By employing IP spoofing, attackers can evade detection and put a substantial burden on the destination network for policing attack packets. In this paper, we propose an inter-domain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. A key feature of our scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in Border Gateway Protocol (BGP) route updates and are deployed in network border routers. We establish the conditions under which the IDPF framework correctly works in that it does not discard packets with valid source addresses. Based on extensive simulation studies, we show that, even with partial deployment on the Internet, IDPFs can proactively limit the spoofing capability of attackers. In addition, they can help localize the origin of an attack packet to a small number of candidate networks.*

I. Introduction

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 attackers use IP spoofing and require the ability to forge source addresses. Although attackers can insert arbitrary source addresses into IP packets, they cannot control the actual paths that the packets take to the destination.

Based on this observation, we have 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 between the source node and the destination node. Hence, any packet with the source address and the destination address that appear in a router that is not in path source and destination address should be discarded.

The Internet consists of thousands of network domains or autonomous systems (ASs). Each AS communicates with its neighbors by using the Border Gateway Protocol (BGP), which is the de facto inter-domain routing protocol, to exchange information about its own networks and others that it can reach. BGP is a policy-based routing protocol in that both the selection and the propagation of the best route to a destination at an AS are guided by some locally defined routing policies.

II. Headings

1. Check and lookup the local network
2. Content Selection
3. Encryption
4. BGP
5. Hackers
6. DecryptionIII. Indentation and Equation

1. Check and lookup the local network

This is module which executes at the loading time to check and lookup the local network. It gets all the systems which are connected to that local network. This helps to the gets current working nodes that means which are active and ready for access in the network.

1. Content Selection

It uses a dialog box to open a required file format, but it mainly supports only for the text support files. The file loaded to a file variable, Then it send to the next stage Encryption area.

2. Encryption

In this the original data is converted to some other format using chips algorithm so that incase some intruder may hack the file at any reason or at any cost, but they won't get the original data unless it decrypted in proper format.

3. BGP

In this Modules BGP (Border Gateway Protocol) is a protocol that communicates across the network and also monitoring the client present in the network. It has all client details as a table. The connection is established with the client and the Router. The Encrypted data is transmitted to the Router which can send or redirect to the correct destination address. The Router checks whether the sender and receiver are proper to the network. Incase the sender (hacker) is not a proper member in the network then that node is said to the attacker node, then the message will not sent to the destination. Otherwise the message will send to the destination address.

4. Hackers

The hacker will act as a client in the distributed network. The hacker may have false name in the network and virtually seems to be present within the current network. It selects the destination address which original present in the network.

5. Decryption

At the destination the received encrypted data will undergo decryption to get the original data which was sent by the sender. Decryption using chips algorithm for the decryption of the received data to the original content. After decryption only the data will be meaningful. The Encryption and Decryption gives the security to data while transferring.

Denial of service (DoS) attack on the Internet has become a pressing problem. In this paper, we describe and evaluate route-based distributed packet faltering (DPF), a novel approach to distributed DoS (DDoS) attack prevention. We show that DPF achieves proactiveness and scalability, and we show that there is an intimate relationship between the effectiveness of DPF at mitigating DDoS attack and power- law network topology.

III. Conclusion

The salient features of their work are two-fold. First, we show that DPF is able to proactively filter out a significant fraction of spoofed packet °flows and prevent attack packets from reaching their targets in the first place. The IP °flows that cannot be proactively curtailed are extremely sparse so that their origin can be localized, IP traceback to within a small, constant number of candidate sites. We show that the two proactive and reactive performance effects can be achieved by implementing route-based filtering on less than 20% of Internet autonomous system (AS) sites. Second, we show that the two complementary performance measures are dependent on the properties of the underlying AS graph. In particular, we show that the power-law structure of Internet AS topology leads to connectivity properties which are crucial in facilitating the observed performance effects.

References

Journals:

[1]. H. Aljifri, M.Smets and A.P. Pons.IP traceback using header compression.Computer &Swcurity, Feb.2003.
[2]. F. Baker and P. Savola, INgress filtering for multihomednerworks, RFC 3704, Mar.2004.
[3]. P.Ferguson and D.Senie. Networking ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2827,May 2000

Books:

[4]. "Atulkahate", "Cryptography and network security", Tata McGraw Hill Publishing Company, New Delhi 2003.
[5]. "Elliote Rusty Harod(1998)", "Java Networking Programming", Galgotia Publications.
[6]. "PatricNaughton(1999)", "Java Complete Reference", Tata McGraw Hill Publication.
[7]. S.Kaihara, "Realization of the computerized patient record: relevance and unsolved problems", intJ.Med inform. Vol.49,no .1. pp.1-8 Mar 1998
[8]. "Roger S. Pressman (2001)", "Software Engineering – A Practitioner's Approach", McGraw Hill International Edition.