International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 9, November- 2012

Survey on Defenses Techniques Used For Controlling IP Spoofing

Shashikant S. Dumbare
ABHA Gaikwad-Patil
College of Engineering,Nagpur

Prof. Pragati Patil
ABHA Gaikwad-Patil
College of Engineering,Nagpur

Prof. Parul Bhanarkar
ABHA Gaikwad-Patil
College of Engineering,Nagpur

Abstract

This is a survey paper on defense techniques used for controlling of IP spoofing which impart a major role in improving network security. With the growth of network scale, now a days network administrators dissipate large amounts of time and costs to manage network addresses (IP/MACs). However, the current state of logical (IP) address management can be said to be extremely inefficient. Therefore, by considering through real time platform technology research on important apparatus that can protect network addresses, a ground breaking measure that can improve the reliability and stability of the network and system needs to be found. This paper focus on an effective method for defense against IP spoofing attack. It elaborates the Interdomain packet filtering techniques as well as hash based path Identification scheme. This paper detailed the method of network access controlling & managing using ARP spoofing in various windows environment and comparative evaluation of spoofing defenses.

General Terms

Security, Spoofing

Keywords

IP spoofing, Spoofing defenses, network security, Network access control

1.Introduction

IP spoofing has often been exploited by attacker by using Distributed Denial of Service (DDoS) attacks to Conceal flooding sources and dilute localities in flooding traffic and Coax legitimate hosts into becoming reflectors, redirecting and amplifying flooding traffic.

Thus, the capability to filter spoofed IP packets near victim servers is required to their own protection and prevention of becoming involuntary DoS reflectors. The explosive growth in computer systems and their inter connections via networks has increased the dependence of both organizations and individuals on the information stored and communicated on these systems. This led us to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network based attacks. As the disciplines of cryptography and network security have full-fledged, there is a need to the development of practical and readily available applications to enforce network security. Everyone has a different view about security and hence different security procedures have come up. The 16-bit identification field (IPID) has been studied recently to determine what information it might yield for network measurement and performance characterization purposes.

II. Yunji Ma's effective method for defense against IP spoofing attack

This method is proposed by Yunji Ma [1] which is an effective method for defense against IP spoofing attack based on traceroute and the cooperation with trusted adjacent nodes. By this method, it is easy to effectively detect and prevent IP spoofing attack.

A. Network Architecture with Trusted Nodes

Mr.Yunji Ma first propose the network architecture based on trusted adjacent nodes, which is shown as Fig. 1. In this network, each trusted node has access authority of others. Only these nodes can access each other, namely they are restricted access authority. he call these nodes as trusted nodes, where each trusted node has access information of the other trusted nodes, such as node name and IP address, hop count and traceroute from itself to the other trusted nodes. In figure (1), six trusted nodes include node A, B, C, D, E and F. The network can is used for campus network or enterprise network and these nodes can be scattered in different geographical location. After the trusted node passes IP authentication, the node can access each other, which is denoted as: A={B, C, D, E, F}, B={A, C, D, E, F}, and so on. Figure (2) shows the detailed network structure with routers, Nodes of R1-R9 are the routers which connect with the trusted nodes. Because we restrict the access authority, the user from outer can be identified by IP authentication. But if it intrudes the network by disguising IP address of a trusted node, it is difficult to be distinguished by IP authentication. In this paper, he was mainly focused on how to identify the attack by disguising the IP address of trusted node, namely IP spoofing attack [1].

B. The process of IP spoofing attack

For explaining the proposed defense method well, Mr Yunji Ma first introduce the process of IP spoofing attack. In Fig. 2, node A and node B are considered as trusted nodes. According to three-way-hand shakes [2], if a hacker intrudes trusted node B by disguising IP address of another node A, it must firstly attack and control the node A, then blocks it from connecting with internet. Next, it sends a TCP SYN connection request to node B by disguising IP address of node A, after node B receives the request, node B sends a SYN-ACK to node A, but node A can not receive the message actually. Once the hacker gets the SeqNo (sequence number), it can send ACK to B again, the connection is established between the hacker and node B, IP spoofing attack comes true.

C. The Model of Traceroute

According to the process of IP spoofing attack, he proposed the model of traceroute. As shown in Fig. 2, he suppose that node H is attacker, node A is source node and node B is victim/target node. When attacker H attacks node B by disguising the IP address of node A, on the third step of three-way handshake, attacker H will intercept the acknowledgement from victim node B to node A. So he can not detect IP spoofing attack by traceroute from victim node B to source node A directly. But in the network, these nodes can cooperate with each other. So the victim node gets help from other trusted nodes, IP spoofing detection can be implemented. Fig. 3 shows the model of traceroute model. Here, node C is a trusted adjacent node of node B, and he call node C as detection node. When source node A sends access request to target node B, he trace the route to node A with the help of detection node C. If the attacker H has controlled the node A, when we trace the route in hop-by-hop from IP address of node C to IP address of node A, the traceroute result is "host unreachable", otherwise, in normal access status, source node is reachable. He describe the process of traceroute as Fig. 4. [1]

D. Yunji Ma's Proposed System Model

Based on the network architecture with trusted adjacent nodes information and the model of traceroute, he propose the system model. Fig. 5 shows its architecture and he describe the model as follows in detail.

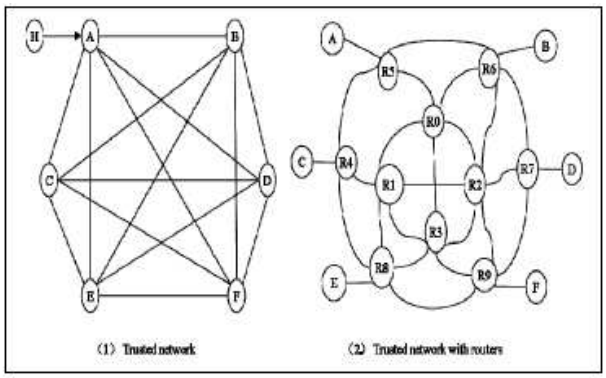

Figure 1. Network architecture with trusted nodes [1]

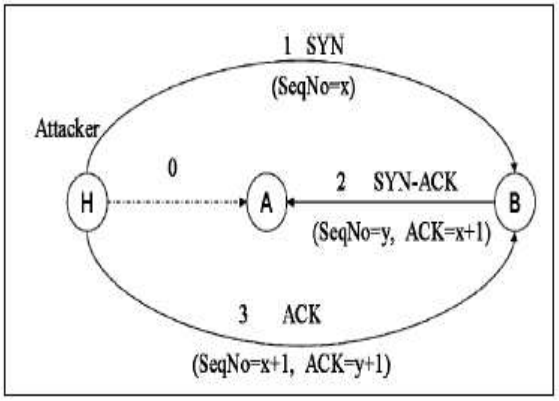

Figure 2. The process of IP spoofing attack[1]

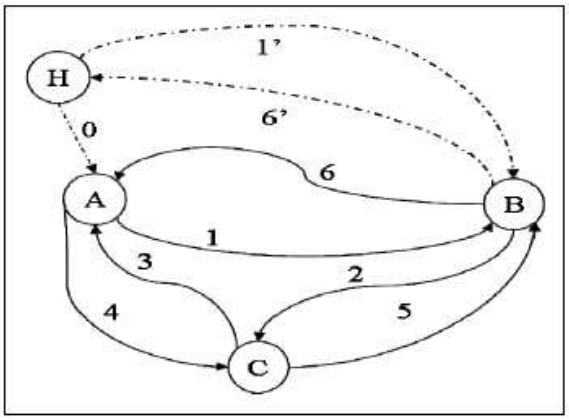

Figure 3. The model of traceroute[1]

1. Source node A sends normal access request to target node B, or attacker H sends request to victim node B by disguising IP address of A;
2. After node B receives the request, node B sends traceroute request to detection node C;
3. Node C traces the route information from node C to node A;
4. Node C gets traceroute result (reachable or unreachable);
5. Node C informs the traceroute result to node B;
6. If (host reachable) node B accepts the access of node A, else node B blocks the attacker;
7. If (IP spoofing) node B sends alarm information.

Figure 4. The process of traceroute[1]

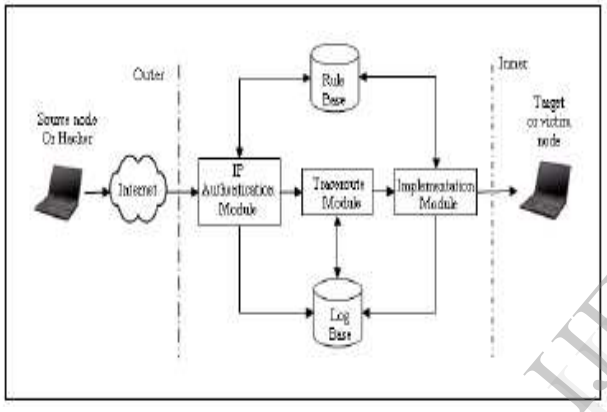

Figure 5. The architecture of system model[1]

1) IP Authentication Module

Based on trusted network architecture, only the trusted nodes can be accessed each other. This module is used to judge whether source host is a trusted node. The information of IP authentication includes node name, node IP address, hop count from itself to target node. When a node requests access, the information is compared with that of rule base. Only when the user pass the IP authentication, it is considered as an trusted node, Otherwise the user is considered as an node from outer site, then the other authentication method will be used.

2) Traceroute Module

In this module, he implement the traceroute from detection node to source node. If source host is trusted node, the result information of traceroute is "host reachable", otherwise, when IP spoofing attack occurs, the result information is "host unreachable". At the same time, the rule base and log base will be updated dynamically. The result of traceroute is sent to the implementation module.

3) Implementation Module

Implementation module receives the result from the above two modules, and implement it. If IP authentication is illegal or IP spoofing attack occurs, the node is blocked. Otherwise, source node is permitted to access destination node.

In order to further describe the method, the system flow chart of IP spoofing prevention method is shown as Fig. 6.

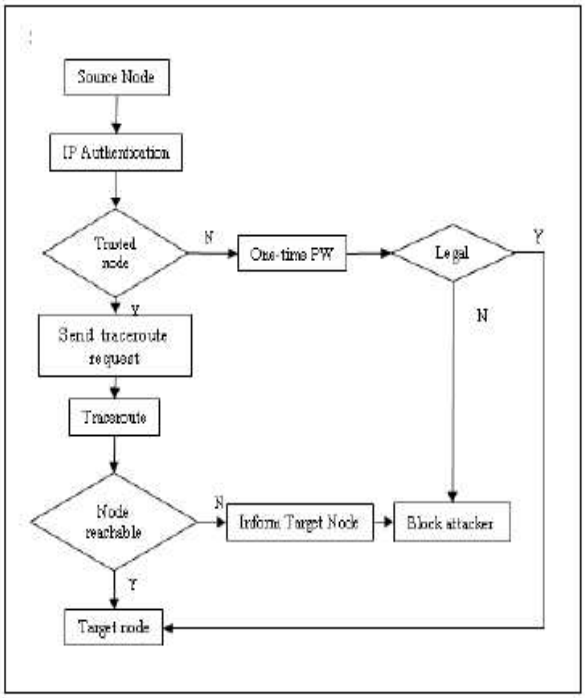

Figure 6. Flow chart of prevention system[1]

III. Detection And Defense Against DDoS Attack With Ip Spoofing

In this ,an author [3],provides an framework for detecting the DDoS attack and dropping the spoofed packets. By analyzing the number of hops that packet gone through before reaching at the destination, The legitimacy of a packet can be find out. Attacker can forge any field in the IP packet including TTL, but he cannot control hop count. By generating an IP to Hop-Count mapping table and inspecting it, spoofed packets can be identified.

According to author[3], HCF *(Hop Count Filter)* is used to classify legitimate and spoofed packets with little collateral damage. HCF technique causes delay in critical path of packet processing in the kernel because of enormous IP2HC mapping table[3], such type of overhead is reduced by identifying the attackers in learning state and then drop spoofed packets in filtering state. It is observed

that the CPU overhead can be reduced by implementing it in Linux kernel in terms of interrupts.

IP packets can easily be forged by means of raw socket programming, wherein construct the IP packet and fill the bogus values of each field of IP packet. Source IP address also can be spoofed with less effort. This kind of forging is associated with Distributed Denial of Service attacks, which blocks server's resources to legitimate client by exhausting victim [5] [6] [7]. DoS attack widely use IP spoofing, such as smurf attack [8].

Based on location of installation of defense mechanism author[3] specify are two approaches, which can be implemented: Router based and Host based.

1) Router Based approach:

This approach uses ACL (access control list) to block private IP addresses on downstream interface. Additionally, this interface should not accept addresses with internal range as the source (as this is a common spoofing technique used to circumvent firewalls). On the other hand upstream interface restricts source addresses outside of networks valid range, which prevents sending of spoofed traffic to the Internet [9].

2) Host Based approach:

The host-based approach protects server either by using sophisticated resource-management schemes or by significantly curtailing the resource consumption of each request to withstand the flooding traffic.

Most of present host-based solutions work at the transport layer and above, and cannot prevent the victim server from consuming CPU resource in servicing interrupts from spoofed IP traffic. It is observed that at the high speed, incoming IP packets generate many interrupts and can drastically slow down the victim server.

The fundamental idea behind this scheme is to make use of that information from packet which attacker can not forge. And this inbuilt information is number of hops packet takes to reach its destination [10] [11].

In this scheme author[3] proposed technique in which it first calculating and capturing the correct HOP count and then it apply HOP count filtering

3) A HOP count Filtering

In this scheme traceroute utility is specially used to calculate hop-count for particular IP address. Then IP2HC mapping table is formed. This scheme is a outline of the HCF technique to identify spoofed packets, assuming that IP2HC mapping table is accurate. For each packet reached to the terminal, hop count has to be calculated. Extract the source IP address S and final TTL *Tf* value from arrived IP packet. Initial TTL *Ti* could be found from *Tf,,* then subtract *Tf* from *Ti* to find Hop-count *Hc*. While inspecting IP2HC mapping table, the source IP address provides the index to retrieve the correct Hop-count from table. If this value matches with the calculated Hop-count then packet is classified as not spoofed. If Hop-count differs then HCF will drop that packet [3].

IV. Interdomain Packet Filtering

Interdomain packet filetring scheme is proposed by Z. Duan, X. Yuan, and J. Chandrashekar [12] .IDPF associates each source with a set of feasible neighbors (previous hops). A neighbor N is feasible for source x if N advertises a route to x to this filter. In [12], Duan et al. assume that route advertising rules are based on relationships between ASes [13]. IDPF was proposed as an altruistic defense with a recommended vertex cover deployment [12].

Normalized strength of the IDPF filter is: $\text{strength}_F = \sum_{p \in IP_{rout}} NF(p)/|IP_{rout}|^2$, where NF(p) is the number of source IPs whose previous hop does not exist in the feasible neighbor set of p. Well-connected nodes are good candidates for strong filters because of the diversity of their neighbors and the prevalence of peer relationships that limit the size of the feasible neighbor set.

The IDPF per-packet cost consists of the lookup of the packet's previous hop in the feasible neighbor set (<8 ns). The storage cost is about six times higher than RBFs and HCFs because multiple feasible neighbors must be recorded for each parameter table entry. If the average number of neighbors is 280, and each neighbor's feasibility is indicated by a single bit, we need 35 bytes for parameter values plus 5 bytes to store a prefix for each table entry. IDPF is vulnerable to the same attacks as RBF: path-all, subnet-all, replay-all, and replay-fix. Additionally, IDPF is also vulnerable to possible-path-all attack, since it will fail to filter packets from attackers that lie on a different path than the source but arrive from a feasible neighbor.

IDPF's parameter table values change when a change in end-to-end routing leads to a change in feasible neighbor sets. The frequency of false positives at an IDPF filter should be higher than at an RBF filter but smaller than at an HCF filter. An attacker cannot influence the feasible neighbor sets of spoofed packets thus false negatives due to guessing are zero[12][4].

V. Network access control and its management by using ARP spoofing in the various windows environment

It is important to analysis the network access control and managing it using ARP spoofing in various windows environment. The author[14] analyze Network Access Control and Management as a solution to the problem of extremely inefficient IP address management. He focus on the ARP protocol action process and policy changes brought about by the change in Windows versions. Ultimately on realizing and proposing additional policies or control methods accordingly. This will help in making securing IP/MAC address utilization clarity, elimination of disorders arising from IP address conflicts, provision of a convenient interface for prompt IP assignment, blocking of unauthorized disclosed IP usage and swift actions against any impediments alongside Network Management Systems possible.

VI. Conclusion

This survey analyze the various defense techniques used for controlling of IP spoofing, imparting a major role in improving network security. With the growth of network scale, now a days network administrators dissipate large amounts of time and costs to manage network addresses (IP/MACs), so network access control and IP, ARP management also studied. But still now a day IP address is hacked, these scheme doesn't provide full controlling over IP spoofing to improve maximum network security. So it is required to propose a new techniques which specially focus on IP-MAC address binding to control IP spoofing as MAC address is unique through out the world.

REFERENCES

[1] Yunji Ma, " An effective method for defense against IP spoofing attack", WiCOM – 2010 / IEEE pages(s): 1 - 4

[2] L. Garber, "Denial-of-service attacks rip the Internet," IEEE Computer, vol. 33, pp. 12–17, April 2000.

[3] I.B.Mopari, S.G .Pukale, M.L.Dhore, " detection and defence against DDoS attack with IP spoofing" 2008/ IEEE ,pages(s): 1-5

[4] Z. Duan, X. Yuan, and J. Chandrashekar, "Controlling IP Spoofing through interdomain packet filters," IEEE, Jan-March 2008, volume:5, Issue:1 , page(s):22-36

[5] TCP SYN flooding and IP spoofing CERT advisory CA -2000-21, ,'http://www.cert.org/advisories/CA-2000-21.html".

[6] US-CERT Vulnarability Note- 539363 DOI, www.kb.cert.org/vuls/id /539363

[7] CERT Advisory CA-200-2 IDoS vulnerability DOI,http://www.cert.orgladvisories/CA-2000-21.html

[8] Cheswick, H. Burch, and S. Branigan, "Mapping and visualizing Internet," in Proc. USENIX Annu. Technical Conf., 2000, Pages(s): 1-12.

[9] K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internet," in Proc. ACM SIGCOMM, 2001, Pages(s): 15-26.

[10] Cheng Jin and Kang G. Shin "Defense Against Spoofed IP Traffic Using Hop-Count Filtering" *IEEE/ACM* Trans. Networking, vol.15 No. I, Feb 2007.

[11] A. Hussain, J. Heidemann, and C. Papadopoulos, "A framework for classifying denial of service attacks," in Proc. ACM SIGCOMM 2003, pp.99-110.

[12] Z. Duan, X. Yuan, and J. Chandrashekar, "Constructing Inter- Domain Packet Filters to Control IP Spoofing Based on BGP Updates," Proc. IEEE INFOCOM, 2006.

[13] F. Wang and L. Gao, "On Inferring and Characterizing Internet Routing Policies," Proc. Internet Measurement Conf., Oct. 2003.

[14] Janghun Bae, Seongjin Ahn, Jinwook Chung, "Network Access Control and Management using ARP Spoofing in Various Windows Environment" IEEE 2011,Page(s):1-10

[15] Jelena Mirkovic and Ezra Kissel, "Comparative Evaluation of Spoofing Defenses", *IEEE transactions on dependable and secure computing, vol. 8, no. 2, March-April 2011*