ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Detecting Spoofing Attack by Source using Path Information

Jyothi[1], Mr. Pavan Kumar V[2]

M Tech, Department of CSE, SCEM, Mangaluru, India [1]

Assistant Professor, Department of CSE, SCEM, Mangaluru, India[2]

Abstract: As there is a growth in internet usage, Systems have become more vulnerable to the attackers. Security verification is provided by the IP packets of Source IP Address. Hence the failure of the Security verification leads to increase in Denial of Service (DoS) attacks. Attacker spoofs the IP Address by randomising the 32 bit Source IP Address field in IP Header. To detect these kinds of attacks, IP Spoofing is introduced. Routers are used in Real Time Processing commonly. Attacks that occur within the organisation are difficult to detect the attack i.e. attacks in Intranet. To overcome this difficulty Route Based Information (RBI) is proposed which uses the packet information to detect the intruder. Source builds the dynamic path through which the packet has to be forwarded to the destination. When the interaction takes place the System's pings each other to check for the connection status. Once the connection status is checked the intermediate nodes acknowledges the Source by generating the 4 bit random number using the IP Address. Source verifies the IP Address of the Intermediate node with the path table. If IP Addresses are identical then it forwards the packet to the Intermediate node by referring the path table. When the node receives the packet, it obtains the address of next Intermediate node to whom the packet has to be forwarded. In case, if the IP Address doesn't match then the Source detects the attack and blocks the packet by displaying the Spoofed message.

Keywords*:* IP Spoofing, Intruder, IP traceback, Path table, RBI

I. INTRODUCTION

Today's Computing Environment provides more critical importance on Internet Security as people rely more on Internet. Online applications such as Public Services, Bank Transaction reckon on Internet. Transfer of information is done by using Client and Server Architecture. Therefore performance and efficiency of Server has to be maintained. DoS attacks are used by the Attackers to bring down the performance of the System. These attacks are detected and countered by IP Spoofing Techniques. IP Spoofing commonly refers to forging of Source IP Address when forwarding the packet [1]. Impact of this attack lead to unauthorized root access. After gain to the root access and taking over existing terminal and login connections, intruder can gain access to host.

Forbidding against DDoS attacks is most challenging task where the attacker Spoof the identity of the Source IP Address and thus elude traditional packet filters. Researcher to foil the DDoS attack can be divided into two categories: Route based and Host based. In Route based approach defence mechanism is installed inside the IP Router and thus Source of the attack is traced and corresponding traffic emerging from the Source is block. In Host based approach more motivation is required to deploy the defence mechanism in the single host. Here the Internet Server is protected to resist SYN cookies and Client Puzzle by using sophisticated Resource Management or by reducing Resource consumption of each Request. Initially the spoofed IP packets acts like a legitimate request by sharing the same resource and code path of the network processing.

Due to the Resource exhaustion by the spoofed IP packets, current approach couldn't provide availability service to the network. Further, many Host based services work at transport layer and above and couldn't stop victim Server from consuming the Resource [2]. Many techniques such as monitoring the packet, route filtering, packet filtering, hop count filtering, TTL based etc has been proposed to detect IP Spoofing attack.

Defending against DoS/DDoS attack is divided into 3 categories: preventive mechanism, reactive mechanism and source-tracking mechanism [3]. The organisation is provided with the fixed number of System's. The effective detection of the attack can be done at the source end by keep track of the path through which the packet has to be forwarded. Proposed scheme mainly focus on detection and tracking the original Source. In this paper, proposed method RBI (Route based Information) uses the Path Information for detecting the IP Spoofing attack. A protocol is design for Application layer, where Source generates a packet and defines a path for forwarding the packet to destination. Path table is maintained by the Source for forwarding the packet through the Intermediate node. As the packet moves the Source verify the IP Address in the path table. If the Address mismatch found with the Path table, then the Source notifies by displaying the Spoofing message.

The remainder of this paper are organised as follows: Section 2 summarises the related work based on IP Spoofing. Section 3 presents design methodology used by

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

proposed system. Section 4 discusses the result evaluation of this approach. Finally, section 5 concludes the work.

II. Related Work

Shashank Lagishetty et al. proposed DMIPS is two level filtering mechanism in which filtering is done within the network and outside the network [1]. Since the filtering is done in different levels, Server overhead is reduced. During the attack congestion is control.

N.Arumugam and Dr.C.Venkatesh proposed the IP traceback analysis method called extension of ant algorithm [3]. This approach validates the incoming packet by uses the flow information and hop count value before reaching the destination. No cryptography methodology is used. Shortest path is identified using pheromone intensity.

Jelena Mirkovic, Nikola Jevtic and Peter Reiher, proposed Clouseau System[4]. In this cooperation with other sites doesn't require protocol to change. Normal internet traffic is not affected and it's flexible to attack intended to subvert its operation.

Li et al. proposed SAVE Source Address Validity enforcement protocol that validates the true Source of the packet[5]. Prefix advertisements are generated by the Source and send to the Destination. Table is maintained at each Router that keeps track of the Source IP Address. Each Router runs SAVE protocol and verifies whether the packet has arrived from expected Interface.

Z. Duan et al. proposed IDPF (Inter Domain Packet Filters) in presence of selective announcements filters less spoofed packet than route based filters[6]. When the multiple incoming interfaces is marked it is difficult to detect in which interface is used by the Source.

Adrian Perrig et al. proposed StackPi where the Routers marked the packet deterministically in the path to the destination with the path fingerprints[7]. Since the victim identifies through StackPi marks of the packet, packet marking are given same to the packet that travel in same path.

Yunji Ma presented the methodology for detecting the Spoofing Attack by coordinating with the trusted adjacent nodes and the traceroute[8]. Trusted network is focused for preventing the Spoofing attack. Local Security System is executing since the mutual coopertion is taken place with the trusted adjacent nodes and traceroute.

Zhenhai Duan et al. developed the advanced scheme name IDPF(Inter Domain Packet Filtering) that uses the information of BGP(Border Gateway Protocal) route updates and is deployed in the border Routers in the network[9]. Drawback is subnet spoofing address is unhandle by this approach.

S. Savage et al. presented the approach that require both the victim and Network Admin[10]. As the packet arrive at the Router the packet is marked probablistically with partial path information. "Post-Morton" is performed by the attackers has the coressponding attack has been completed.

III. Design Methodology

The main objective of the proposed method RBI is to detect the Spoofing attack in Internal Network and to block the data transmission in Local Area Network. Initially, Source generates packet that has to be send to Destination through the Intermediate Node. Before the communication takes place the Source has to construct the path required for forwarding the data. The path table contains IP Address and is maintained by Source. According to the path table data will be forwarded to the destination(Figure 1). If the Attacker spoofs the IP Address, then the Source detects the Intruder by verifying in the Path table.

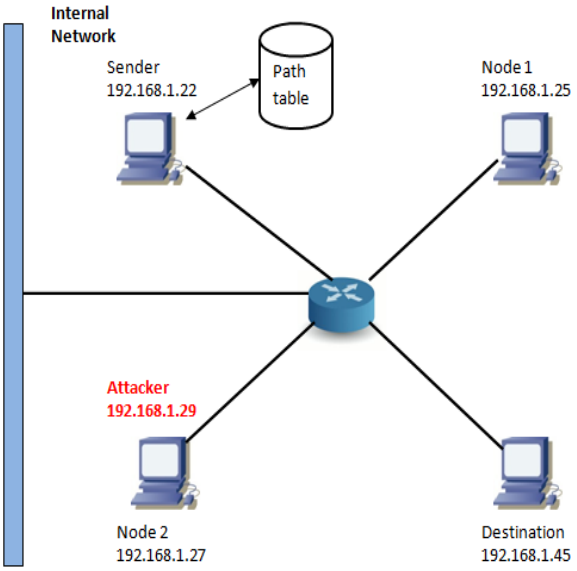

Fig. 1. System Architecture

Consider the scenario of internal network where the systems are connected using the Switch. The Sender 192.168.1.22 communicates with the Destination 192.168.1.45 through the Intermediate Nodes. There might be possible that the Intruder occurs within the network. i.e. Node 2 with the IP Address 192.168.1.27 may act has the Intruder and spoof the identity by 192.168.1.29. In order to detect such attack RBI scheme is used.

RBI consists four phases for Detecting IP Spoofing: Login Phase, Construction Phase, Verification Phase and Detection Phase.

1. Login Phase: Systems that involves in the organisation that uses the RBI scheme is provided with the login interface by which System IP Address is used to login the System. This address is automatically obtained by the System.

DOI 10.17148/IJARCCE.2015.4598

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

2. Construction Phase: During this phase, path is constructed by the Source in which the packet has to be forwarded through the Intermediate node. Path information is stored in the Path table. Path table contains the IP Address of the System and the Packet Identifier. Before the packet is forwarded to the next node, the Source has to look up the path table.
3. Verification Phase: The Source verifies the IP Address of the requested System with the path table. If the corresponding path matching is found then the packet will be forwarded to next node.
4. Detection Phase: Detection is performed by the Source for identifying the Intruder in the organisation. While the Source compares the path table and the IP Address of the requested node, if the path mismatch found then the spoofing has occurred and Source blocks the packet.

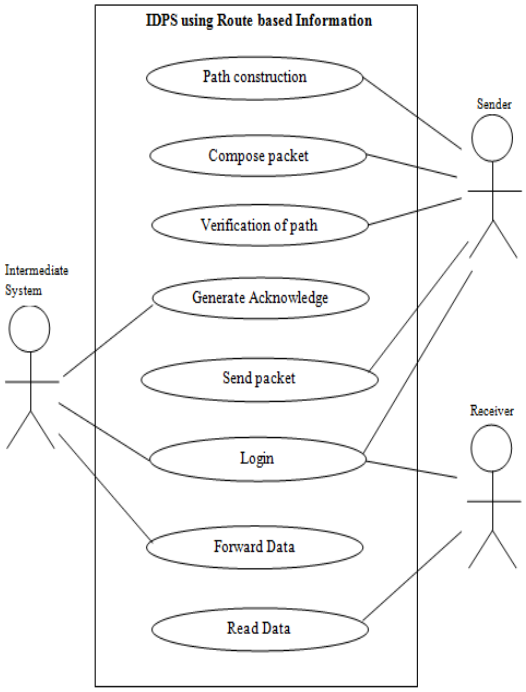

Fig. 2. Use case diagram for detection System

The working of the proposed system is as follows: Source logins to the System using the IP Address and constructs the path automatically. Path can be viewed only by the Source. The path information is stored in the path table. The Source has to ping with the corresponding next node. Pinging has to be performed to check the alive status of the system and send the packet. The alive status of the System generate the acknowledgement and forward to the Source. As the acknowledgement received, the source compares the IP Address of the node with the path table. If the IP Address is matching, then the Source forwards the packet. Otherwise the Source detects the Spoofing attack and blocks the packet with the message.

CONCLUSION

Detecting spoofing and preventing the intruder within the network or organisation has become the most challenging task for the researcher. For this purpose, RBI scheme is proposed. The proposed methodology focus on route information for detecting and preventing the intruder in the Intranet. Source maintains the path table through which the packet has to be forwarded to the destination. Each time the Systems has to ping each other. Acknowledgement is generated by the Intermediate node and is sent to the Source. Source then verify the IP Address in the path table. If the IP Address is identical then the data is forwarded. The unmatched status of the IP Address detects the spoofing attack.

REFERENCES

[1] Shashank Lagishetty, Pruthvi Sabbu, and Kannan Srinathan, DMIPS- Defensive Mechanism against IP Spoofing Attack, International Institute of Information and Technology, 2011.
[2] Sneha S. Rana and T.M. Bansod, IP Spoofing attack Detection using Route Based Information, International Journal of Advanced Research in Computer Engineering and Technology, vol. 1, Issue 4, June 2012.
[3] N.Arumugam and Dr.C.Venkatesh, A Dynamic Method to Detect IP Spoofing on Data Network Using Ant Algorithm, IOSR Journal of Engineering (IOSRJEN), October 2012.
[4] Jelena Mirkovic, Nikola Jevtic and Peter Reiher, A Practical IP Spoofing Defense Through Route-Based Filtering, 2007.
[5] J. Li and J. Mirkovic and M.Wang and P. Reiher and L. Zhang, SAVE: Source Address Validity Enforcement Protocol, Proceedings of INFOCOM, June 2002.
[6] Z. Duan and X. Yuan and J. Chandrashekar, Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates, Proceedings of INFOCOM'06, April 2006.
[7] A. Perrig, D.Song, and A.Yaar, StackPi: A New Defense Mechanism against IP Spoo_ng and DDoS Attacks, Technical Report CMU-CS-02-208, CMU Technical Report, February 2003.
[8] Yunji Ma, An Effective Method for Defense Against IP Spoofing Attack in Wireless Communications Networking and Mobile Computing (WiCOM), Recent Trends in Information Technology (ICRTIT), pp. 1-4, Sep. 2010.
[9] Zhenhai Duan, Xin Yuan, Jaideep Chandrashekar, Controlling IP Spoofing through Interdomain Packet Filters‖, IEEE Trans. On Dependable and Secure Computing, Vol. 5, No. 1, March, 2008.
[10] S.Savage, D.Wetherall, Anna Karlin and Tom Anderson, Network support for IP Traceback‖, IEEE/ACM Transactions on Networking, Vol. 9, No. 3, June 2001.