Indian Journal of Science and Technology, *Vol 8(17), DOI: 10.17485/ijst/2015/v8i17/63910, August 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Mitigating IP Spoofing to Enhance Security in Multi-Agent based e-Learning Environment

K. Shyamala[1*] and Shantha Visalakshi[2]

[1]Dr. Ambedkar Government Arts College, Chennai - 600039, Tamil Nadu, India; shyamalakannan2000@gmail.com,
[2]Ethiraj College For Women, Chennai - 600116, Tamil Nadu, India; shan_shrivisa@yahoo.com

Abstract

Objectives: An important issue dealing with IP spoofing in the model of e-learning platform is studied to suggest mitigation techniques. **Methods/Analysis:** The paper proposing the wrapped up security does IP capturing at network level. This feature of IP capturing can be of no use when IP spoofing is carried out to disrupt the service. Studying IP spoofing techniques using tools such as n-map and by modifying the TCP and UDP headers using penetration testing tools reveals that IP spoofing can be used to disrupt the services offered by the e-learning systems. **Findings:** It is found that IP spoofing as observed is done in two ways. The first one is masking the IP using online IP masking tools and web sites. Offline tools such as TOR are also used to mask the IP. But it has been a great confusion learning the difference between the two methods of spoofing. The first method is actually masking IP which delivers the result of a request to the request initiator while spoofing does not send the response back to the initiator. Study reveals that this IP spoofing can be carried out in various methods which results in different types of attack scenarios and consequences. **Conclusion/Application:** This paper focuses on the techniques that are used to impersonate an IP. IP spoofing must be detected and blocked in order to provide e-learning as a service to authenticate users of the system which is analyzed in this paper.

Keywords: Distributed e-Learning, e-Learning, IP-Spoofing, Multi-Agent Co-Ordination, Security

1. Introduction

Every transfer of data across the internet involves capturing of IP address. A simple Google search involves tracking the IP of Google server back to the source system's IP. Since IP capture is accomplished in each and every point of transfer or exchange of data across the network, IP capture is easy to do and this can be added as a security feature to e-learning content retrieval system. This e-learning system proposed[1] captures the IP address of the registered user. When a user tries to retrieve the contents from the e-learning environment other than logging in from other IP address, the content delivery is prohibited. But there are chances that this IP captured from the registered users may be spoofed by unauthenticated users to gain access to the content of the e-learning system. Also it is better to improve the document based search techniques we need to incorporate class hierarchy methods[2]. The advanced AES algorithm coding formula can be embedded to produce secured transaction[3] in the distributed system by means of dynamic key generation for various information sets. To ensure the learning to be the lifelong process the system can be designed with pedagogical virtual agents who have the aesthetic value[4].

IP Spoofing can be achieved by intruding the end systems i.e. the source and the destination systems. The intruder captures the IP of the source machine and assigns its IP on the packets being sent to the destination machine, thus making the destination machine to believe the intruder to be the legitimate source machine that had sent the request.

The main aim of the intruder here is to establish a duplicate connection between itself and the destination

*Author for correspondence

machine to steal and gain access to access restricted data[5]. Normally, when there is a communication between two machines, let us say machine SRC and machine DST where SRC is the source machine and DST is the destination machine. The exchange of data is carried out as shown in Figure 1, Figure 2 and Figure 3.

This type of IP spoofing is done to impersonate and steal and gain access to data whereas when the aim is to do a DOS attack the Scenario will be as shown in Figure 4. The attacker spoofs the IP of the target and broadcasts ICMP Echo Requests to machines in a network. When all the machines respond to the target with ICMP Echo reply the victim or the server is brought down and faces a DOS attack. This attack is termed as Smurf attack.

IP Spoofing may be done with two intents[6] impersonation and for performing a DOS attack. DOS - Denial of Service attacks are done to bring down a server by flooding the server with TCP/SYN packets of ICMP Requests for which the server will not be able to respond. The impersonation attack is done to gain access or to capture traffic between two nodes on a network. The first type of attack is the one that has to be focused in this Learning and Content Management Systems since the impersonation may lead to piracy of the contents in the system.

Network level attacks include IP spoofing. Network level implementation device is the router and when the router is configured with proper Intrusion Prevention

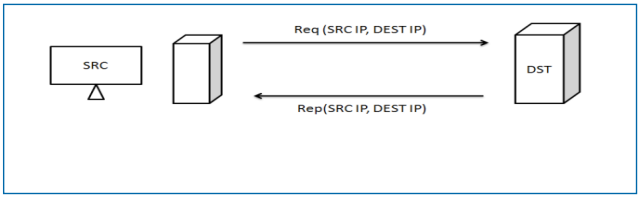

Figure 1. Common communication method.

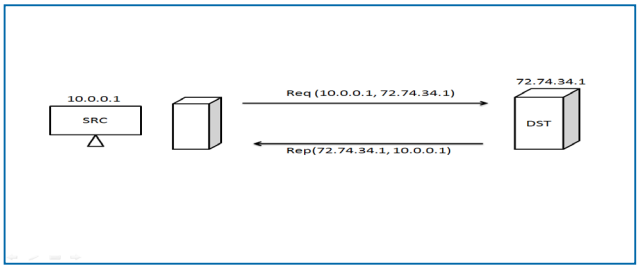

Figure 2. Normal communication between two machines.

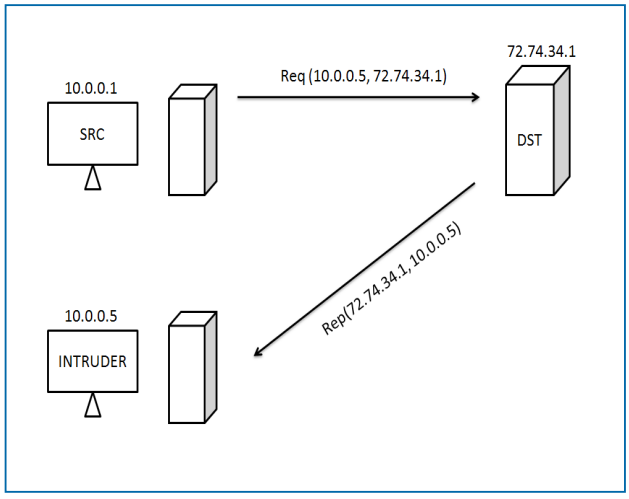

Figure 3. IP spoofing.

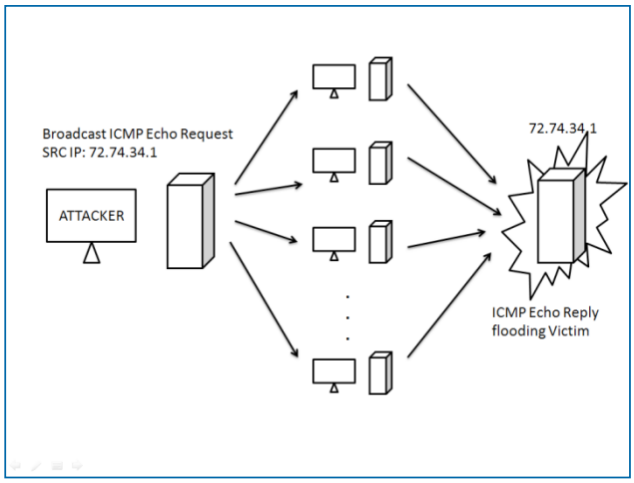

Figure 4. DOS attack using IP spoofing.

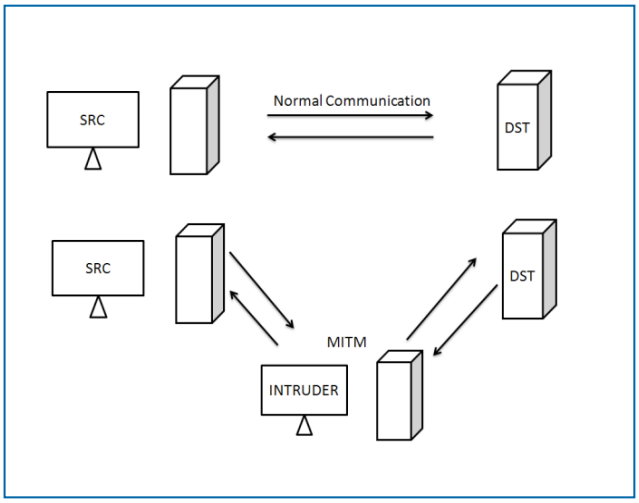

Figure 5. MITM attack.

System and Intrusion Detection System impersonation or a DOS attack can be mitigated[7]. Ingress Filtering is one technique that can be used to mitigate IP spoofing attacks. This method proposes filtering of the data received at the destination where the data packets from the specified source are checked for its integrity and authenticity[8].

Tracing back to the source IP will yield better results in mitigating IP spoofing attacks. Trace back[8] is a method that traces the IP from which the data packets are received at the destination. This technique must be added to the router configuration which will dissipate packets from illegitimate source IPs.

2. Spoofing Attacks

2.1 Non Blind Spoofing

Non Blind Spoofing is done to attack a system in the same subnet. The attacker carries this out in order to capture the data flowing between the source and destination. Once the intruder spoofs the IP of the Victim and establishes a connection, this leads to a Session Hijacking. No matter whatever the security walls are built up once session is hijacked, then, all the data passing through the channel can be stolen and reproduced by the intruder. When our registered user and intruder are present in the same subnet and the IP of the user is spoofed by the intruder, the content retrieval system will be affected and the contents can be pirated[9] either using cookies or IP spoofing.

2.2 Blind Spoofing

This attack takes place outside the victim's subnet. The intruder probes the victim to get sequence numbers and fragment id's to capture the data by spoofing the IP. When this kind of attack is launched, the registered user's IP can be probed along with the IP ID or the Fragment ID or the sequence number that can be used to perform the attack and grab the content from the management system.

2.3 Man-in-the-Middle

This attack is launched by desynchronizing the communication between two machines and injecting packets by spoofing that allows the source to think the intruder to be the destination and the destination to think the intruder to be the source. This attack reveals all sensitive data passed between the two machines in the communication.

2.4 Denial of Service

When an intruder wants to bring down a server or a system to stop it from providing service, this type of attack is launched. The intruder chooses random IPs that is spoofed to send SYN packets to the victim that may be a system or a server. The victim at first replies to the SYN packets and when a large number of packets arrive flooding the server, the server becomes down unable to service the requests. [10]This is called as DOS attack.

3. Detecting IP Spoofing

Detection of IP Spoofing involves many techniques ranging from routing to non-routing methods. Each and every technique has its own way of detection of IP spoofing.

3.1 Routing Methods

Routing of a packet to its origination is possible which would help in detection of a IP spoofed packet entering the network[6] The process of disallowing the spoofed packets from getting into the network is called as *egress filtering*. This method filters the outbound traffic entering the network. The process of disallowing spoofed packets from getting out of our network is called as *ingress filtering*. This method filters the inbound traffic raising from the Internal IP to the NAT table and then to the External IP and being sent to the public network to reach the destination.

3.2 Non Routing Methods

Non Routing methods involve two kinds of ways of analyzing the network for IP spoofing attack. The first method is the Active method which will monitor the packets received by using net-log and verify and validate the origin of the packets. Whereas Passive method will just indicate that the network received a spoofed packet without any verification and validation.

3.3 TTL Probes

TTL is time to live which indicates the number of milliseconds a packet will be allowed to be circulated to reach the destination and upon whose expiration the

packet is discarded. The Probing of TTL will yield the result that can be compared with the spoofed packet's TTL. When found a mismatch in TTL of the original and the spoofed packet, the packet may be discarded.

3.4 Fragment ID Verification

Fragment ID or the IP ID is the one found in the header of a TCP packet. This ID gets incremented for each and every communication that is taking place between the source and the destination. When this ID is randomly increasing or decreasing, then the packets are termed to be spoofed and they may be discarded. There are also other methodologies such as Honey Pots, Caller ID Traceback, Active probing, topology based packet marking and so on. But these are the methods basically used for the detection of IP Spoofing Attacks.

4. How to Prevent IP Spoofing

Cross-validation is a technique that disallows packets entering into the victim's system. This technique first validates the IP address from which the packet is coming by verifying it with the list of the IANA (Internet Assigned Numbers Authority) and then fetches the bogus IPs and compares with them[8]. Then ICMP Echo requests probing the IP ID and TTL of the source are sent in order to check the authenticity of the IP Origin. Apart from these basic filtering and validations, we can modify the core routing structure without changing its originality and implement an algorithm that will disallow IP spoofed packets from entering into the system[11]. In addition to these the system can be even deployed with the emerging integrating technology called Honey-pot[12] to keep track of Malware analysis and Intrusion detection.

5. Future Work

Changing the core routing structure, that will do multiple validations and disallow the IP Spoofed packets entering the network needs an algorithm that must be developed without any change in the core routing technologies. When this is implemented in the multi-agent e-learning environment, the security gets enhanced. Extensive Implementation of the system architecture proposed[1] can be effectively implemented in cloud environment[13] to ensure the 24/7 data availability for the convenient cum secured way of learning to the e-learners. As the system architecture[1] comprises of many agents for providing service, they can be very well configured on virtual clusters[14] in cloud data centers to establish trust-worthy relationship between two entities. Hence, the entire process will be clearer and transparent to both user and cloud service provider perspective.

6. Conclusion

By using lossless compression techniques one can avoid IP spoofing attacks. Implementing an algorithm that would avoid source address authentication, use cryptographic authentication and change the core routing structure without modifying its originality but allow multiple validations to authenticate packets from an IP a multi-agent based content retrieval system can be implemented to achieve a secure e-learning content retrieval and management system.

7. References

1. Shantha VU, Shymala K. Multi-Agent Co-ordination In Distributed E-Learning Environments: Providing Access Permissions. IJET. 2013 Apr-May; 5(2):1306–10. ISSN: 0970–4024.
2. Manickasankari N, Arivazhagan D, Vennila G. Ontology based Semantic Web Technologies in E-learning Environment using Protege. INDJST. 2014 Oct; 7(6);64–7. e-ISSN: 0974-5645.
3. Abhinivesh M, Garg M, Acharya KDP. Secured Transaction for Distributed Service System. INDJST. 2015 Jan; 8(2):160–4. e-ISSN: 0974-5645.
4. Ramachandiran CR, Jomhari N. A case study on e-learners Perception and Kansei Experience towards Pedagogical Virtual Agents. INDJST. 2015 Jun; 8(11):1–10. e-ISSN: 0974-5645.
5. Bremler-Barr A, Hanoch L. Spoofing Prevention Method. 2005 Mar. p. 536–47.
6. Rana SS, Bansod TM. IP Spoofing attack detection using Route Based Information. International Journal of Advanced Research in Computer Engineering and Technology. 2012 Jun; 1(4):285–8. ISSN: 2278-1323.
7. Rashid S, Paul SP. Proposed Methods of IP Spoofing Detection & Prevention. IJSR. 2013 Aug; 2(8):438–44. ISSN: 2319-7064.
8. Yu F, Lee D. Internet Attack Traceback Cross-validation and Pebble Tracing. Waltham, MA: IEEE; 2008. p. 378–83. ISSN: 978-1-4244.
9. Upadhyay V, Kumar R. Detecting and preventing IP spoofed attack by hashed encryption. IJECBS. 2011 Jul; 1(2):753–5. ISSN: 2230-8849.

10. Stone R. Center Track: An IP overlay network for tracking DoS floods. Proceedings of USENIX Security Symposium; 2000 Jul. p. 199–212.
11. Kumar AB, Choudhary M. Detection of session hijacking and IP Spoofing using sensor nodes and cryptography. IOSR-JCE. 2013 Jul-Aug; 13(2):66–73. e-ISSN: 2278-8727.
12. Sathish V, Khader SA. Deployment of proposed Botnet Monitoring platform using Malware analysis for distributed environment. INDJST. 2014 Aug; 7(8):1087–93. e-ISSN: 0974-5645.
13. Durai Raj M, Manimaran A. A study on security issues in cloud based e-learning. INDJST. 2015 Apr; 8(8):757–65. e-ISSN: 0974-5645.
14. Uddin M, Mamom J, Alsaquor R, Shah A, Zaidi M. Mobile agent based Multi-layer Security Framework for cloud data centers. INDJST. 2015 Jun; 8(12):1–10. e-ISSN: 0974-5645.