Geographic Based Detection and Prevention of Spoofing Attack

V. Prabhu, D. Jaganathan

Abstract; Spoofing attacks remains one of the most damaging attacks in which an attacker can replace the original source address in the header with a new one to conceal their identity and location. Major spoofing attacks now a day's users face is the email spoofing attack in which the spoofer gets details from the email user they target and attack through the fake email sender with fake messages and viruses to attack the users system, mail list, etc. which causes a greater damage to the email user who have opened and responded to that mail unknowingly. To overcome these types of attacks in this project we are analyzing the email with spammed contents to check whether it is from the right person or not and the location from where the mail has been sent by doing this we can secure the E-mail communication as maximum as possible.

Keywords : Blind Spoofing, Email Spoofing, Geolocation, Header Analyzer, whois.

I. INTRODUCTION

1.1 Introduction of Domain

Cyber Security is the body of technologies process designed to protect networks, computer programs and data from attack, damage or both. Cyber security requires coordinated efforts from an information system.

Elements of cyber security include:

1. Application Security 2. Information Security 3. Network Security 4. Operational Security 5. End-User Education. One of the elements of cyber security is the quickly and constantly evolving in nature of security risks. This approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended for some less dangerous risks not protected against, such an approach is insufficient in the current environment in cyber security. Computer security is otherwise called as cyber security or IT security is the protection of information systems from theft or damage to the hardware, software and to the information on them from disruption or misdirection of the services they provide.

1.2 Paper Introduction

Spoofing attack is the unfamiliar attack in the cyber crime done in the internet which causes a great threat to the email users this may lead to a situation that the sensitive information of the users are hacked by the spammer in the internet. To make an awareness of this type of attack in the internet and safe guard themselves from this type of attack in mail.

1.2.1 Email Spoofing

The Email Spoofing is the one where the spoofer will attack the victim's mail by the following ways,

From - name/address Reply - name/address, return path – addresses and Source internet protocol address. The first three can be altered by changing the settings in the windows but the last one can also be altered but there must be more sophisticated user knowledge to make a false IP address truly. Rat ware program sometimes run massive built-in wordlists to create thousands of target email addresses, spoof a source email and blast the spoof email to those targets. Other times, rat ware program take illegally-acquired lists of email addresses and then send their spam accordingly. Other than rat ware program, mass-mailing worms are also found. Worms are self-replicating that act as a type of virus. In our computer, a mass-mailing worm will read your email address book. Then the mass-mailing worm will falsify an outbound message to appear sent from a name in your address book, and proceed to send that message to your entire list of friends. This not only offends the dozens of recipients, but tarnishes the reputation of an innocent yours. Some well-know mass-mailing worms include: Sober and Klez.

In computer networking, the term address spoofing or spoofing refers to the creation of headers with a forged source address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system. In a spoofing attack, the intruder sends mail to a person indicating that the message has come from a trusted recognized sender. To be successful, the intruder must first determine the email address of a trusted system, and then modify the mail headers to that it appears that the mail as come from the recognized sender. In essence, the attacker is fooling (spoofing) the distant computer into believing that they are a legitimate member in the network.

Types of Spoofing Attacks:

Blind Spoofing – This attack may take place from outside where sequenced and acknowledgement numbers are unreachable. Attackers send several packets to the target machine in order to sample sequence numbers, which is doable in older days.

Revised Manuscript Received on May 06, 2019

V. Prabhu, Assistant Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan, Dr. Sagunthala R&D Institute of Science and Technology, Avadi, India)

D. Jaganathan, (Assistant Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan, Dr. Sagunthala R&D Institute of Science and Technology, Avadi, India)

Non-Blind Spoofing – Non –Blind Spoofing is the type of attack takes place when the attacker is on the same subnet as the victim. The sequence and acknowledgement numbers can be calculating them accurately.

II. LITERATURE REVIEW

In the Internet more and more cyber-attacks are being performed. To overcome this IP Spoofing attack they have been inspired by the “Hop-Count Filtering” technique. Their algorithm is based on the idea that although an attacker can spoof the source IP address, the attacker cannot spoof the number of hops a packet traverses to reach the destination. Therefore, the algorithm first learns the IP to Hop Count (HC) mapping and stores the mapping in an IP2HC table. Once a packet arrives, it is compared to the HC stored for this IP. If the HC values match, then the packet is legitimate. Otherwise, the packet is discarded. The main strength of the HCF technique lies in its simplicity. This paper aims at proposing a variation of the HCF technique in order to enhance the accuracy of the HCF by including in the IP2HC table all valid HCs seen in the learning phase. This modification enhances the overall accuracy compared to the original HCF and its variations. This section provides a literature review of several methods that detect spoofed IP packets like Hop Count Filtering technique and Reverse Path Forwarding, Hop Count (HC) is defined as the number of hops a packet traverses as it moves from the sender to the receiver. HC is not sent in the IP packet but is rather inferred from the IP Time-to Live Field (TTL).

The receiver can estimate the HC by subtracting the received TTL value from the closest initial TTL value bigger than the received packet’s TTL. Usually, these initial TTL values are operating system dependent and are limited to few possibilities, which include 30, 32, 60, 64, 128, and 255. Therefore, guessing the initial TTL set by the OS is possible without explicitly knowing what the OS is, especially that the number of hops between two hosts is relatively limited. This is the case of most DoS attacks. Like HCF, our proposed algorithm has two phases, a learning phase and a filtering phase. In the learning phase, each destination creates a profile for each IP it communicates with. Unlike HCF, the profile is not only made of <IP, HC> but is made of <IP, HC-List>. In this manner, the destination can learn all the valid HCs seen from the source in case multiple routes with varying hop counts exist. This will enhance the performance of HCF by correctly classifying the legitimate traffic and thus lowering the false alarms rate. However, this leniency will come at the cost of lower attack detection rate since an attacker has more valid HC options to bypass this detection method.

In the filtering phase, the packet is considered legitimate if its HC belongs to the HC-list created in the learning phase. Otherwise, it is considered as an attack. The proposed model could be deployed in two forms. It can be deployed at end hosts to protect them from undetected IP spoofing attempts. It will be able to perform all the calculations since all the traffic will pass through it. In case of an attack, it can filter the traffic and thus protect end servers. However, the device will not be able to protect against DoS attacks that target the bandwidth of the Internet links used by the organization since that requires filtering from upstream Internet Service Providers. However, if all ISPs implement a similar solution, this limitation can be lessened.

In Internet, packets are transmitted using Internet Protocol (IP). It includes IP address of the sender in the data packet. Even though IP is the basis for Internet packet transmission, it does not provide any method for authenticating the source device. The lack of source authentication mechanism can pave a way to the attacker to forge the source address. The process of transmitting the data packets with forged source address is known as IP spoofing. IP spoofing is directly related to various networks malfunctioning like Distributed Denial of Service (DDoS). An ideal IP spoofing protection mechanism should fulfill the following properties -The spoofing protection mechanism should not depend on traffic characteristics for the attacker As the name implies, the solution is centered on end hosts where an end host identifies the spoofed IP packets. The solution of this type does not depend on the functionalities of router. They are easily deployable and do not need any modification in network infrastructure. However, this type incurs delay in detecting spoofed packet, as the packet has to reach the end host.

In the Internet, these solutions are deployed by the routers either at core of the Internet or at the edge of the Internet or at both. The solution is little difficult to deploy. However, it could be the efficient solution for it detects the spoofed packet before it reaches the end host. Their proposed solution for DDOS attacks is inefficient because of huge overhead involved in implementing the export policies to be followed by each node or AS. In order to provide the best solution that overcomes the abovementioned drawbacks, in this paper, we propose a Secure Verification Technique (SVT) for defending IP spoofing attacks. In this technique, each AS constructs Neighbor Authorization (NA) table using received route update messages. We defend the IP spoofing attacks using NA algorithm. This algorithm is triggered, when the source receive update message while transmitting data in the selected path. The NA algorithm authenticates the AS by tracing NA tables. Since, NA table plays an important role in authentication process, it must be transmitted securely. For this purpose, our technique uses RC-6 encryption algorithm to perform encryption in the network. Transmitting entire NA table will consequently incur more overhead. Hence, our technique uses arithmetic coding to compress and decompress the table. Here, the destination ID represents the IP address of destination, hop count is the length in terms of number of AS between the source and the destination and processor Id is the IP address of second to last hop AS towards destination. We include the predecessor ID in NA table so that the consistency and authenticity of the AS can be checked. When the source desires to transmit data to the destination, it will select the shortest path from the routing table. We assume that the initially selected path is short, secure and free of BGP threats. The NA algorithm is triggered, when the source router receives update message from any AS while transmitting data in the selected path. The source authorizes the update message by tracing the route in it. The tracing process detects the malicious router in the network and there by avoids network attacks such as black hole and hijacking. The number of attackers performing IP spoofing attack is varied from 1 to 5. The packet loss, packet delivery ratio, overhead and fraction of affected communications are measured for the two techniques.

Other than IP trace back, another way of identifying attack packets is to have an ability to differentiate between attack packets and legitimate packets and filter those attacked ones. The reason for selecting IP Trace back is, it not only identifies the attack packets but also the location of spoofer's. IP Spoofing defense mechanism is of two types named Host-based solutions and Router-based solutions. A router implementing Spoofing Prevention Method (SPM) authenticates a packet by examining the secret key embedded into the packet. A source Autonomous System (AS) s, chooses upon a key calculated for every (s,d) pair, where d is a destination AS. When a packet reaches the destination d, the router ensures the secret key. A packet with the key is valid, and the packet without the key is spoofed. If the AS does not follow SPM method, there won't be any key associated with the packets.

Hence router cannot recognize the spoofed and nonspoofed packets. This section propose a mechanism called BGP-based AntiSpoofing Extension (BASE), which contains the features of Path Identification (Pi) and Distributed packet Filtering (DPF) . BASE (BGP based Anti-Spoofing Extension) which an anti-spoofing protocol is intended to achieve the incremental deployment properties which are necessary in todays Internet environment. BASE is used for preventing spoofers and can be adopted easily and deployed in real networks. In spoofers identification process, a value called "Marking" is calculated for these packets that use BGP update messages. It is distributed to routers where the value is checked against values in filter table. This method is called Packet Marking and Filtering in BASE. This method will detect more number of packets and, will minimize the computation overhead on the router. During spoofing attack, an attacker sends spoofed packets to the destination node to hide the identity of the attacker. Each node will have BASE filters and the role of a BASE filter. Each BASE filter has a Filtering Table F. If F can store only one marking value in each record, then it is called as one mark and if multiple marking values are stored, then it is called as multiple marks by default, BASE is multiple marks. In this case, it can store all likely marking values in the Filtering Table. In the distribution phase, when a BASE filter collects a marking value, it stored in its Filtering Table F. In the marking and filtering phase, when a BASE filter receives a packet (s,t), the filter forwards the packet to R(t) with a new mark mi only if mi1∑ F(s)otherwise it drops(s,t). The main motive of this system is to identify the IP spoofing attack using BASE mechanism in distributed network and differences between the various types of attack along with the reasons behind those attacks. In the distribution phase, BASE requires a small computation for creating marking values.

The marking values can be computed even before they are distributed through BGP update messages. This process occurs rarely, only when a BGP path changes or a new BASE-enabled node is deployed. Also, if some nodes sometimes need to inform their key values, then the marking values also need to be updated. Using PIT, the location of the spoofers is identified and it is analyzed that the spoofers are caught correctly to a great extent. Thus IP spoofing attack might be attained with improved performance result. Using a graph called X-graph, the overload of the router is evaluated and detection accuracy.

III. SYSTEM ANALYSIS

3.1 Existing System

The detection of spoofed or spammed email in the mailing list is difficult by the user and most of the email user's wont check the header. They just see the names and reply to the mail or just click any links that as been sent in that spoofed email. This creates a great loss to the users. They may lose their any sensitive information present in their system or mail. It is very difficult to identify that the user's mailbox as been hacked through a spoofed email.

In a spoofed mail the hacker can change the timings of the mail they send. The email users mostly use very weak password such as numbers, personal details as their password that could be easy for the hacker to hack and do whatever they want the may also change the reply path to same as your email address. They may also send unwanted email to your mail contacts with virus and spammed information. Due to the unawareness of this type of attacks, the email users are still victims to the hackers.

3.2 Proposed System

Let us consider a scenario, where in the user gets a mail from a recognized person with spammed contents or unwanted details of information not related to him. If the user need to check that whether the mail is originally from that recognized person means the possible ways are by contacting them through phone or any other mode of communication is used for verification. Instead of verify them directly the user itself can check the information of that mail he received.

First the users have to analyze the mail header received if he thinks that it is not from the legitimate sender. In the analyzer it will give all the information of that mail, i.e. from, to, reply to, return path, delay time, crested time, message id, SPF, etc. From that information we can easily identify the mail that is spoofed or it is from the recognized sender and also we can find the location of that spoofed mail by pasting the IP address of that spoofed mail service provider and verify who tried to steal the information.

IV. SYSTEM DESIGN

4.1. Description

Analyze the mail header you have received you think that it is not from the legitimate sender. In the analyzer it will give all the information of that mail, i.e. from, to, reply to, return path, delay time, crested time, message id, SPF, etc. From that information we can easily identify the mail that is spoofed or it's from the recognized sender and finds the location of that spoofed mail by pasting the IP address of that spoofed mail service provider and verify who tried to steal the information. By the geolocation positions of the latitude and longitude of the fake mail originally sent from.

4.2 Modules

1. User Authentication
2. Email Spoofing
3. Header Analyzer

4. Server IP Finder
5. Geolocation Finder

4.2.1 User Authentication

The User Authentication module is used to register and login into the websites if not registered they have to register by giving their user name ,password ,country , capcha this will be stored in the database server when ever user login into the site the details will be retrieved from the database. Then the user can access the site after logging in the user can send the information. If user need to change the password they can update and the updated information is again stored in the database.

4.2.2 Email Spoofing

The Email Spoofing is the one where the spoofer will attack the victim's mail by the following ways,
The email is spoofed by following ways:
1. FROM- name/address 2. REPLY- name/address 3. RETURN PATH- addresses 4. SOURCE IP address
The first 3 can be altered by changing the settings in the windows but the last one can also be altered but there must be more sophisticated user knowledge to make a false IP address truly. Rat ware programs will sometimes run massive built-in wordlists to create thousands of target email addresses, spoof a source email, and then blast the spoof email to those targets. Other times, rat ware programs will take illegally-acquired lists of email addresses, and then send their spam accordingly. Other than rat ware programs, mass-mailing worms are also found. Worms are self-replicating that act as a type of virus. In our computer, a mass-mailing worm will read your email address book. Then the mass-mailing worm will falsify an outbound message to appear sent from a name in your address book, and proceed to send that message to your entire list of friends. This not only offends the dozens of recipients, but tarnishes the reputation of an innocent yours. Some well-know mass-mailing worms include: Sober and Klez.
In computer networking, the term address spoofing or spoofing refers to the creation of headers with a forged source address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system. In a spoofing attack, the intruder sends mail to a person indicating that the message has come from a trusted recognized sender. To be successful, the intruder must first determine the email address of a trusted system, and then modify the mail headers to that it appears that the mail as come from the recognized sender. In essence, the attacker is fooling (spoofing) the distant computer into believing that they are a legitimate member in the network.

4.2.3 Header Analyzer

All emails has a header block in which the sender, receiver address and the subject of that mail information is given. The header in a email helps to know the information about that email and to identify it is original or untrusted people works to gather our personal information. Also give the timings in how much delay the mail is sent to the receiver.

4.2.4 Server IP Finder

Whois is a query and response protocol so its widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. It is used for a wider range of other information. It stores and delivers database content in a human-readable format.

4.2.5 Geolocation Finder

Geolocation is the identification or estimation of the real-world geographic location of an object, such as radar source, mobile phone and Internet-connected computer terminal. Its involves the generation of a set of geographic coordinates and is closely related to the use of positioning systems, but its usefulness is enhanced by the use of these coordinates to determine a meaningful location of street address. IP address location data can include information such as country, region, city, postal / zipcode, latitude, longitude and time zone. Further deeper data sets can determine other parameters such as domain name, connection speed, ISP, language, proxies, company name, US DMA/MSA, NAICS codes and home/business.

V. CONCLUSION AND FUTURE WORK

5.1 Conclusion

Hence, we try to dissipate the mist on the location of spoofers. In this proposed system to track spoofer's location with publicly available information. and to make the email users aware of email spoofing attack by having this software for analyzing the mail header of the fake mail received in the mailing list and report it to spam or the user can themselves find from which location the spammed mail is sent.

5.2 Future Work

As further improvements towards the project, we can provide authentication in the mail server itself. The mail server can filter the spammed mails based on message ID only so we can analyze that the mail is from the registered mail service provider.

REFERENCES

1. Alwar Rengarajan, Rajendran sugumar, and Chinnappan Jayakumar. (2016) "Secure Verification Technique for Defending IP Spoofing Attacks".
2. S.Swarna Latha, J.Bhavithra. (2016) "Detection and Prevention of IP Spoofing using BASE Mechanism".
3. Kevin Benton, L. Jean Camp, Tim Kelley, and Martin Swany. (2015) "Filtering IP Source Spoofing using Feasible Path Reverse Path Forwarding with SDN".
4. E-Mail Phishing - An open threat to everyone.(2014) "Gori Mohamed .J, M. Mohammed Mohideen, Mrs.Shahira Banu. N".
5. Ayman Mukaddam, Imad Elhajj, Ayman Kayssi, Ali Chehab. (2014) "IP Spoofing Detection Using Modified Hop Count".
6. Bingyang Liu, Jun Bi. (2014) " Toward Incentivizing Anti – Spoofing Deploying".
7. Abhishek Kumar Bharti, Manoj Chaudhary. (2013) "Detection of Session Hijacking and IP Spoofing Using Sensor Nodes and Cryptography".
8. Sharmin Rashid, Subhra Prosun Paul. (2013) "Proposed Methods of IP Spoofing Detection and Prevention".
9. Young –Hyun Chang, Kyung-Bae Yoon, Dea-Woo park. (2013) "A study on the IP Spoofing Attack through Proxy Server and Defence Thereof".
10. S.G. Bhirud, Vijay Kumar. (2011) "Light Weight Approach for IP- ARP Spoofing Detection and Prevention.