A Dedicated Setup to Recognize Spoofing in LAN/ Wi-Fi via IP Configuration

Bhuvana Natarajan
Student
Department of Information Technology
Jeppiaar Maamallan Engineering College, Chennai, Tamil Nadu, India

Nivetha Kuppusamy
Student
Department of Information Technology
Jeppiaar Maamallan Engineering College, Chennai, Tamil Nadu, India

Mrs. S. Nalini
Assistant Professor
Department of Information Technology
Jeppiaar Maamallan Engineering College, Chennai, Tamil Nadu, India

Abstract

In computer networks, it consists of policies and practises adopted to prevent and monitor unauthorised access. Networks can be both public and private where many of the counter attacks were practised. It is long known that IP spoofing or IP address spoofing is one of the major threats in communication protocol. IP spoofing is nothing but IP packets with forged source IP address, with purpose of concealing the identity of sender or impersonating an another computer system by forging the source address of packet header so it contains a different address, an attacker can make it appear that the packet was sent by a different machine .so that the IP spoofing comes into place. In existing, Passive IP trace back (PIT) that bypasses the deployment difficulties of IP trace back techniques. Though PIT cannot work in all the spoofing attacks and therefore we have proposed a novel idea, to restrict the Man in the Middle Attack (MITM) by providing inbound and outbound rules to avoid the challenges in operation. As long as the real origin of IP spoofing is not disclosed they cannot be deterred from launching further attacks. So the proposed solution ensures that the entity requesting for a service is an actual recipient by trace back the real identification of an attacker.

Keywords- IP Spoofing, Man in the Middle Attack (MITM), Inbound and Outbound Rules, Call Traceback

I. INTRODUCTION

Perfect demonstrating and assessment of computer networks rely on the availability of large datasets of Internet flows acquired from backbone links. Those data are needed to support several research tasks, including Internet traffic analysis, modeling of topological distribution, identification of security attacks, and validation of research results. Unfortunately, serious privacy and security concerns discourage the publication of such datasets. On the one hand, network flows carry extremely confidential information that should not be released for privacy reasons. For this reason we assume that the payload is removed from all packets. However, an adversary observing the source and destination IP addresses may associate an individual with the web sites that he/she visited, and thus he may infer private information such as political opinions, health issues, or religious belief. Similarly, Internet flows may reveal personal communications among specific individuals, such as e-mail exchanges and chat sessions among them. On the other hand, those datasets may also help an adversary to perform security attacks. For instance, observing the traffic of a target network, an adversary could identify possible bottlenecks to be exploited for several attacks. For these reasons, several techniques were proposed to sanitize network flows while preserving their utility. Early techniques were based on the substitution of the real IP addresses with pseudo-IDs. However, that method proved to be vulnerable to different kinds of attacks, based on the knowledge of network characteristics, or on the capacity to inject bogus flows in the monitored network. More recently, several techniques have been proposed to avoid the re-identification of IP addresses, based on the perturbation of other fields of the flows. However, those techniques do not provide any formal confidentiality guarantee, and it has been recently shown that they are prone to different kinds of attacks. Indeed, the computational costs and the memory requirements for obfuscating a large dataset could be strongly reduced by partitioning the dataset in smaller subsets and by running the theft process independently on each subset. With respect to our previous work, the original contributions of this paper consist in: 1) the identification of confidentiality traces: 2) a novel defense algorithm to apply –theft to incremental releases of network traces: 3) a theoretical proof of the confidentiality guarantees provided by the defense techniques. Our results show that our technique preserves the data quality in both the single and the incremental release.

II. LITERATURE SURVEY

A. Existing Work

There are a lot of IP trace back mechanisms proposed and a large number of spoofing activities are observed. Despite of previous work, the practical and effective IP trace back solution based on path backscatter messages, passive IP trace back (PIT) is proposed. This technique ensures with improved tracking capability, by identifying the commencement of the attack and their location only within its specific system, the real identity of an attacker is still mystery.

B. Proposed Process

In this project for tracing the real location of the attacker, Google API is used. Most probably the attacker prefers (MITM) to sniff the data on network connection. We have proposed a security measures to reduce the (MITM) with certain inbound and outbound rules in system configuration, Yangsiang[1] discussed the technique called FDPM it provides features to trace the DDOS attacking packets come from, and suspect intruder located. Main drawback is that this technique requires participating routers to log information about every packet passing by and huge number of packets required to identify the source, Shuivu[2] proposed a technique which creatively use IMEI number of mobile network for trace back the location of user of every possible attack in current mobile internet environment by single packet marking and shows demerit of performance bottleneck and reliability, Y.Bhavani[3] proceeded their work on enhancing the issue of probabilistic marking algorithm therefore It works by marking the packets and it contain only the partial information regarding the routers of attacking path and it requires more number of packets to get the complete information. So they proposed their work by reducing number of packets and time consumption possible to all attacks by using Chinese remainder theorem, Wanlei zhou[4] figured out a issue in dynamic deterministic packet marking algorithm. He made an innovative idea that rather than making every node of internet, he marked the involved attacked nodes to prevent the DDOS attacks in effective manner and shows demerit in scalability, L.Cheng[5]improvised a new scheme called opportunistic piggyback marking scheme. They demo that their design effective reduces the traceback completion delay and router processing overlay and increases the message delivery ratio compared with other approaches and also overcome the problem in et.al, Aqeel Sahi Khader[6]concentrated to prevent MITM in areas of different key exchange protocols especially diffie hellman key exchange protocol. In his proposed work the data are hashed and encrypted so that it will be so difficult to intercept and decrypt without appropriate keys.

To overcome the drawback of the existing system, the implementation of new system helps to detect the origin of attack, trace the real identity and accurate location of an attacker in tier-II autonomous system is possible.

III. PROBLEM DEFINITION

In computer networking, IP protocol is common protocol for sharing of resources from one person to another. Due to delay in network flow or network traffic issues, there is a sign of stealing the particular information or data from the source. In order to find the source from where the attack is actually happened we are proposing a solution for finding the real identification of Hackers that provides the exact details of attackers. The purpose of finding the real identity of hacker helps to reduce and safeguard the data from further attacks. So, it is important if the intimation of hacker is provided for the victim, it can be monitored and controlled from several counter attacks in a short period of time and investigation can be minimized.

IV. METHODOLOGY

Our prototype model of IP configuration and tracing the hacker location detected by the following steps:

- Complete setup is shown in the form of block diagram.
- The Google API detects the location of an attacker with the help of latitude and longitude position.
- The real identity of hacker details are sent through the server.
- The client IP address and other details are pre-saved in the server database.
- Whenever an attack has occurred the location is detected and a detail has been sent to pre-saved client.

A. Registration with AES Encryption

In the registration phase, the user details Client's name, IP-address, and a key string (password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server. After Client-Server registration protocol has completed, the server will have the following information in its memory, IP-address Port, Client's Name, Public Key of registered Client's and threshold value.

B. Threshold Value Formulation

We define a threshold value for each connection. Each time a packet is sending on a connection its threshold value is added. Sender can be either host or network based, as all interaction is typically performed over a network connection. One of the Packet or file is to be selected for the transformation process. The packet is sent along the defined path from the source LAN to destination LAN

.The destination LAN receives the packet and checks whether that it has been sent along the defined path or not using threshold values.

Threshold Value = IP Address of Client + Filename + Secure Key

C. Unauthorised Access –Hacker Zone

The node which is present in the different network or individual system accessing the data in the false name of a node which is present in the router network is called as hackers. The threshold value is not allocated to the hacker system. Monitoring Access module takes care of the data sending through the network using the threshold value. It accesses the database to check the validation for proper and improper user. It also monitors the hackers if anybody accessing the data, which does not belong to the network.

D. Accurate Call Traceback

Call trackback schema which is powered by intelligence along with the design of attack classifier. The output generated by the classifier generates a dynamic list of attacks, which are then queued in the proposed backscatter architecture built with network security to understand various approach of behavior and patterns of the attacker. The network administrator collects all such relevant information over the network itself allowing the inbound network connection from the attacker to do so. The system creates a call traceback to prevent the probability of vulnerable and hostile situation over the network even before the attack event is performed by the attacker.

E. Finding Hacker Location using Google API

Packet filtering is one defense against IP spoofing attacks. The gateway to a network usually performs ingress filtering a threshold value, which is blocking of packets from outside the network with a source address inside the network. This prevents an outside attacker spoofing the address of an internal machine. Ideally the gateway would also perform egress filtering on outgoing packets, which is blocking of packets from inside the network with a source address that is not inside. This prevents an attacker within the network performing filtering from launching IP spoofing attacks against external machines.

V. TOPOLOGICAL DIAGRAM

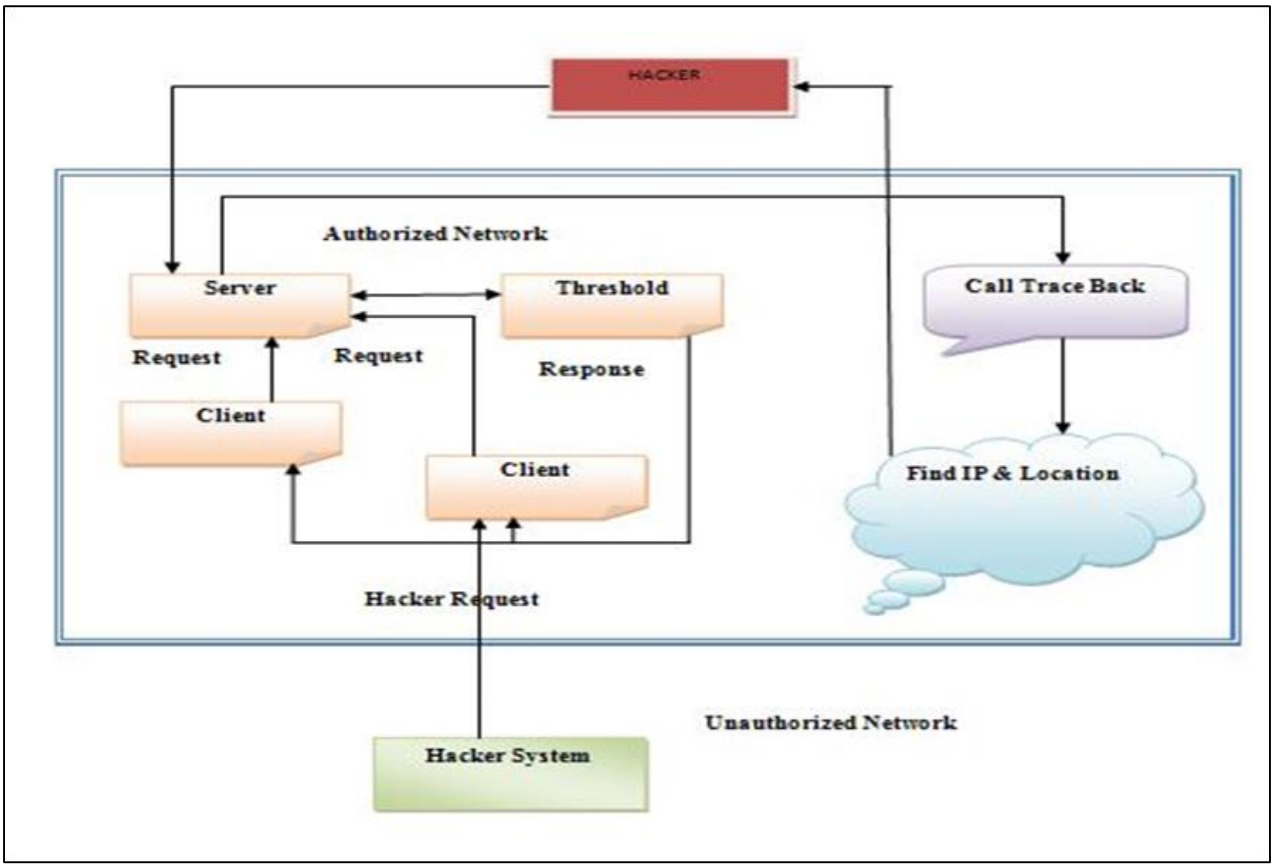

Fig. 1: Network topology showing hacker identity

In fig1 illustrates the setup to identify the exact location of hacker by tracing the spoofed IP address in client –server system.

VI. FUTURE SCOPE

The future enhancement is based upon with some extensions of implementing several security measures to prevent this MITM. As consideration deploying the own traceback system is meaningless and cost effective so this demerit can also be deployed in the future. Despite of previous work, the tracking capability can be increased and reduction on time delay made to identify the real source of an attack much faster. Our idea had practically deployed only for a small organisation rather than it can also be done for a large IT organisation.

VII. CONCLUSION

In this project, we addressed the certain inbound and outbound rules. Thereby these rules are specifically done with some changes to prevent this Man-In-Middle Attack(MITM).we have formally proved the confidentiality guarantees provided by this new technique and experimentally evaluated that our idea is practically deployed in Tier-II autonomous system. By tracing the spoofed IP address the real origin of source, IP address, port number, port type, location details can be identified accurately. Results showed that our technique preserves the network issues of threats with security and improved tracing capabilities and also supported for any kind of attacks.

REFERENCES

[1] Yang Siang, Wanleizhou, Minviguo, "FLEXIBLE DETERMINISTIC PACKET MARKING: An IP Traceback system to find the real source of attacks", IEEEsecurity and policy, (vol: 20, no 4, pp 567-580),2009.
[2] Shui,Keshavshood, Yongxiang," An Effective and feasible traceback scheme in mobile internet environment", IEEE communications letters(Volume 18,issue 11),2014.
[3] Y.Bhavani, R.Sridevi,"IPtraceback through modified Probablistic Packet Marking algorithm using Chinese remainder theorem", (Volume 6, issue 2), 2015.
[4] Shui yu,wanlei zhou,Song guo,"Afeasible IP Traceback through ,"dynamic deterministic packet marking", IEEEtrans on computers (Volume 65, issue 5), 2016.
[5] Long Cheng, D.M.Divakaran, VL.Lthing "Opportunistic piggyback marking for IP Traceback",IEEEtrans on info forensics and security (Volume 11,issue 2),2016.
[6] Aqeel Sahi Khader,david lai,"preventing man-in-the-middlw attack in diffie hellman key exchange protocol", telecommunication(ICT)22nd international conference,2015.