© 2017 IJSRST | Volume 3 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Isolate Unauthorized Authentication and Block Data Transaction Using Agile IP Traceback

R. Lalith Kumar
PG Scholar, Department of Software Development & Management, VIT University, Vellore, TamilNadu, India

ABSTRACT

IP Traceback is a mechanism which is used to identify the origin of the packet on the internet. Since there are no authentications done for any IP address, there are many chances that IP address can be faked and used to perform harmful attacks to any host machines. There are many traceback methods implemented of which few are just used for investigation purpose and some for detection and prevention of these harmful attacks. The attacks are broadly categorized as passive in which only data is watched and active attacks in which the data is modified with purpose to corrupt or destroy the data. Passive attacks are very tough to find but it can be prevented. Active attacks are very tough to avoid but it's easy to detect. There are two types of service attacks which are Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. In DoS attacked only one system and one network connection is used to send packets to the system. These packets can be either TCP or UDP. By this way, it is possible to make the system inaccessible and hence all the applications available under the system is blocked. In DDoS attack it uses more number of system and many networks and hence blocks the server connections in a fast manner. Hence there is a need for a very fast processing algorithm to identify and block data transactions. This fast processing can be accomplished by Agile IP Traceback (AIT) which gives much better performance when compared to other algorithms.

Keywords: IP Traceback, Spoofing, Agile IP Traceback, Data transactions.

I. INTRODUCTION

Spoofing is an attack by which IP addresses are forged and used by hackers to access a network to gain information or even perform further operations. One big advantage of spoofing is the hacker's location can be hidden. There are several mechanisms by which the spoofed IP can be tracebacked and used for investigation purpose. These techniques help identify the path by which packets are transmitted but only after the entire operation gets completed. So hackers get all the necessary details and these techniques doesn't help in hindering these transactions.

Generally, attacker access the source using dynamic IP addresses which do not have ISP's, topology details and when dynamic IP address are used, the IP should be blocked from performing any transactions at the initial stage. The protocol that we use is called agile IP Trace back (AIT) which investigates the message triggered by spoofing traffic, and tracks the attackers based on public available information before any packets are being transferred.

II. TYPES OF INTERRUPTION

A. Snooping

Snooping is a process which is used to monitor and get the login id, password, pin, IP address by which general people's private matters can be accessed by third party member.

B. Spoofing

Spoofing involves faking of data such as creating duplicate IP address, user names and passwords and thus protected systems can be access with this faked information.

C. Phishing

There are various malicious reasons by which phishing is carried out. Usually normal user receives a link, mail with a trustworthy branding and makes the user to type personal information and later this information are used for various fraudulent activities.

D. Pharming

Pharming is a method which uses some software components to redirect a site to fake link through which personal information is fetched. Even when user enters a trusted website it redirects to some other fake site with lookalike of the original site.

E. Cookies

Cookies play a very important role in storing user details so that it helps fastening accessing the site. But this can be very dangerous as this will be misused by intruders to access user information very easily.

F. Spyware

This is a software which installed in a user's machine fetches the data and shares it to the intruders.

III. RELATED WORKS

[1] This paper plays an important role in investigation process where the origin and travelled path is identified. It proposes a novel cloud traceback system which focuses on deploying traceback services in networks of internet service provider. It uses token based authentication where the tokens are generated by a separate server.

[2] This paper deals with the security in TCP/IP protocol which is the most widely used protocol but has a number of loop holes which leads to attacks. This paper completely explains about the problems associated with TCP/IP protocol.

[3] Describes the Distributed Deniel of service (DDoS) attacks and the best methods to avoid them. The tools and techniques proposed in this paper are very well established in preventing the attacks.

[4] This paper briefly explains the Hash-based method to identify the origin of the IP packet as most of the current IP traceback mechanism are not very efficient in finding the accurate origin and these algorithms lag fastness. In hash based algorithm it populates audit trails for traffic and it helps in tracing the origin of the IP packet. This is very fast and space efficient.

[5] Describes the Denial of Service (Dos) attack in brief and how internet is safe in preventing it. They propose a new concept called backscatter method where after a packet is being transmitted, it reflects a message based on which the origin of the IP can be found. This method mainly focusses on investigation where the IP is tracebacked after an attack.

[6] This paper uses two techniques, one is advanced marking method and authenticated marking method which helps the customer to track the spoofed IP packets. These methods use less network overhead and has high computational speed in restructuring the attacked path to prevent the Denial of Service attack. The authenticated marking method is used to provide efficient authentication of router marking so that it is not forged.

IV. ARCHITECTURE

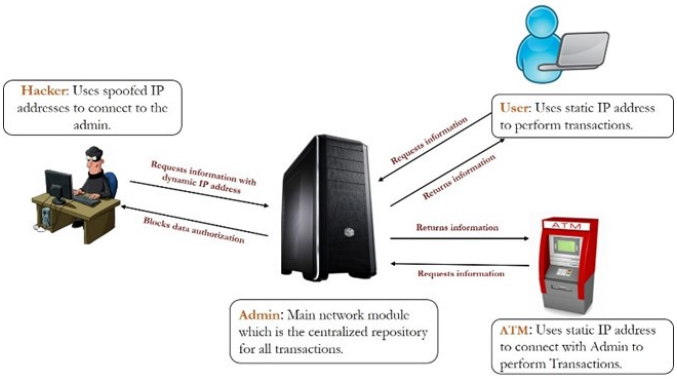

Figure 1: Architecture for IP Traceback

V. MODULES

- User module
- ATM module
- Hacker module
- Admin module

A. Admin Module

Admin module or the central hub through which other modules establish a connection and perform their required transactions. This module generally uses a static IP address and other modules are sub sectioned under this module. The purpose of this module is to

provide a centralized place where information for the system can be stored, retrieved, updated and accessed.

B. User Module

The purpose of this module is to authenticate users, provide message box for them. This module is created to centralize services related to users. This module helps update profile, perform general user transaction, authenticate and perform effective communication.

C. Hacker Module

Hacker module is a system which with its own IP address tries to access the admin module by dynamically updating its IP address to admin module and with forged authentication details; this module tries to perform transactions.

D. ATM Module

This is a physical module which helps users perform transactions and it has a communication between admin modules. This module is used to perform retrieval duties related to users. The purpose of this module is to provide the user interface and view functions for the system.

VI. PROBLEMS OF THE EXISTING SYSTEM

Internet is the most common medium that helps us in easy communication, transaction, gather information etc. As this seems to be an advantage but there are also disadvantages that the communication occurring through internet are not secured. There are number of protocols and security methods developed to safe guard this information but still the industry is getting better the negative side as well.

The protocols and algorithms used to secure and identify the intruders has both pros and cons. Every method used to safe guard the secure transaction has also a loop hole for the hackers to fetch the information. The base paper "FACT: A Framework for Authentication in Cloud-based IP Traceback" used the protocol Internet Control Message Protocol and the token algorithm is used to secure the authentication. ICMP protocol is mainly used in wide range of application including network forensics, security auditing, network fault diagnosis and performance testing.

It uses the concept of IP traceback where once a malicious transaction occurs; the spoofed IP address can be identified by this protocol. In order to secure the authentication, a token based login procedure is introduced where instead of username and password; tokens are generated from the traceback server. This method can be used only when either both the source and destination being used by an authorized user or destination controlled by the user. When both the source and destination are being controlled by the attacker, tokens can be generated by hackers and they can use the same to authenticate the system.

A. Disadvantages of existing system

- ICMP protocol can help only in investigation purpose and cannot identify and block the transaction before it occurs.
- Tokens are not effective method as hackers can bypass both source and destination server.
- Once the transaction occurs, it is not possible to revert back. Only traceback of IP address is possible.
- Not so efficient if there is heavy interaction between branches
- Data should be carefully maintained.

VII. PROPOSED ALGORITHM

Hackers switches from malicious IP to the vendor's IP to perform authentication to the vendor application and when IP traceback methods are used, the original source IP address of the hacker is identified and based on the general information such as the ISP, topology, security settings, the IP address can be identified if its spoofed.
AIT is used to perform IP traceback; it is very different from existing IP traceback mechanisms. AIT is inspired by a number of IP spoofing observation activities. Thus, the related work is composed by two parts. The first is to identify spoofed IP, and the second is to block transactions with that IP.

NAME: Agile IP Traceback (AIT)

INPUT: set of host names.

OUTPUT: Original IP or Spoof IP.

START

Declare H; where H=host names

Find host names of the request and assign to H;

With H

Declare E; where E=host entries

Find host entries of host names and assign to E;

With E

Declare A; where A=IP Address

For each (A in E)

If (A exists in dataset)

Then

Return true;

Else

Return false;

End

End

STOP

A. Advantages of proposed system

- Spoofed IP's are blocked before any transactions could occur.
- Once an IP is identified as fake, data authorization to that IP is permanently blocked.
- Fast processing than ICMP.
- This technique is very efficient if there is heavy interaction between branches.
- We can store the data normally and efficiently.

VIII. EXPERIMENTAL RESULTS

A. Requirements

TABLE 1
PARAMETER REQUIREMENTS

Parameter	Value
User ID	Customer preferred names
Password	Customer preferred password
PIN	Four digit number

B. Screen Shots of experiment

Figure 2: Login screen for authentication

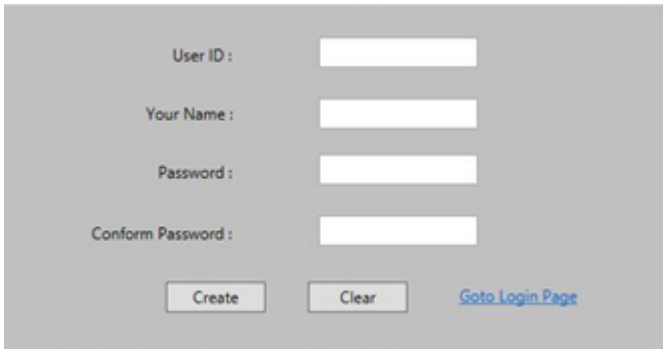

Figure 3: New user registration page

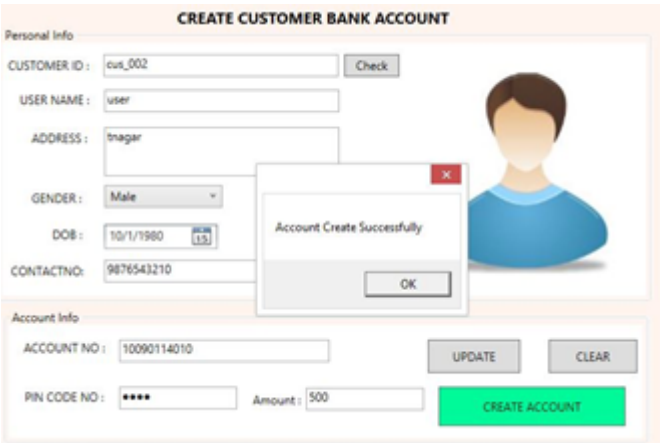

Figure 4: Account creation page for customer

Figure 5: ATM module for customer

Figure 6: Pin authentication for ATM module

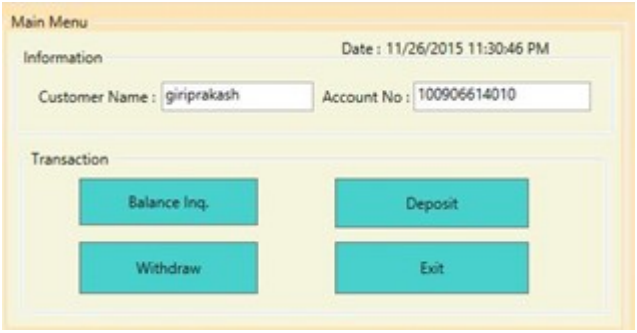

Figure 7: Main menu for Customer

Figure 8: Home page for hacker module

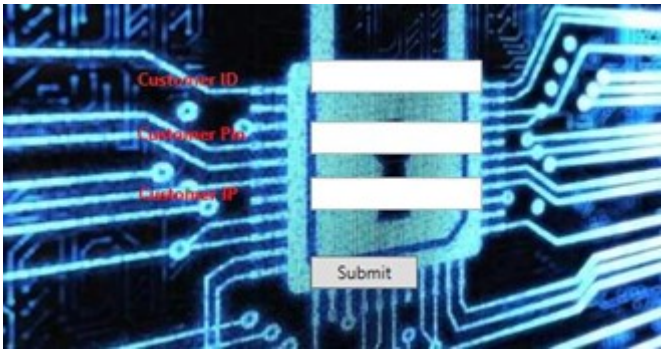

Figure 9: Input screen for hacker module

Figure 10: Withdrawal screen for hacker module

Thus from the above screenshots, when the hacker tries to perform any data transaction, it is blocked by the algorithm as the IP address for the hacker is not authorized. By this way many unwanted data transfer can be controlled. This algorithm is very fast in computing the result and thus is far superior in IP traceback mechanism.

IX. CONCLUSION

The proposed algorithm gives better results in analysing the root node and identifying its authenticity with the general information and when identified to be a malicious IP, it is then blocked and further data authorization is completely blocked. Agile IP traceback can be very fast in identifying the information of the requestor which helps the destination to prevent illegal data transaction.

Agile IP traceback only reads the information of the requestor to identify fake IP addresses which makes it fast and efficient. This method doesn't allow packet transmission to take place as the identification and blocking of falsified IP address takes place before packet transmission.

The computational time to identify the IP address and process it to authenticate is very easy and quick as the AIT algorithm is placed in the start of the process and helps load the results much faster than any other algorithms developed so far.

In some cases, when the algorithm implementation is placed after few routers, it may delay the processing speed and results in fast data access by hacker. Agile IP traceback gives better results in identifying falsified IP address and block its transactions.

X. REFERENCES

[1] Long Chengy, Dinil Mon Divakarany, Aloysius Wooi Kiak Angz, Wee Yong Limy, Vrizlynn L. L. Thing, "FACT: A Framework for Authentication in Cloud-based IP Traceback", IEEE 2016.

[2] S. M. Bellovin, "Security problems in the TCP/IP protocol suite," ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48, Apr. 1989.

[3] Stephen M. Specht, ICANN Security and Stability Advisory Committee, "Distributed denial of service (DDOS) attacks," SSAC, Tech. Rep. SSAC Advisory SAC008, Mar. 2006.

[4] Alex C. Snoeren, "Hash-Based IP Traceback", BBN Technologies, 2007.

[5] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," ACM Trans. Comput. Syst., vol. 24, no. 2, pp. 115–139, May 2006.

[6] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback," in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 2. Apr. 2001, pp. 878–886.

[7] Virandra Patil, Pritish Deshpande, Mahesh Talekar, Swapnil Tapkir, Dhanajay khade, Prof.Nitin Hambir, "Spoofer location detection using passive ip traceback", MJRET 2016.

[8] Shweta vincent, j. Immanuel john raja, "A Survey of IP Traceback Mechanisms to overcome Denial-of-Service Attacks".

[9] Vijayalakshmi Murugesan, Mercy Shalinie, Nithya Neethimani, "A Brief Survey of IP Traceback Methodologies", 2014.

[10] Wikipedia, "IP_traceback" https://en.wikipedia.org/wiki/IP_traceback.

XI. AUTHOR'S PROFILE

Lalith Kumar is an PG Scholar in Department of Software Development & Management at VIT University, India. He obtained his bachelor's degree in computer science and engineering from SNS college of engineering, afflicted to Anna university. His area of interest lies in security in network and Cloud Computing. He has published two international journals in the area of scheduling in grid computing.