International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume3, Issue 8 (August '2017)

AN EFFICIENT METHOD FOR AUTHENTICATING IP ADDRESS USING ITS (IMPLICIT TOKEN SCHEME)

K.Gayathri,
M.Phil Scholar,
Department of Computer Science,
PRIST University,
Thanjavur,Tamilnadu,India.

T. Karunakaran,
Assistant Professor,
Department of Computer Science,
PRIST University,
Thanjavur,Tamilnadu,India.

Abstract: IP trace back plays an important role in internet cyber investigation processes, where the sources and paths of packets need to be identified the traversed path. It has a wide range of applications, including forensics network, auditing security, network fault diagnosis, and performance testing. Despite a plethora of research on IP trace back, the Internet is yet to see a large-scale practical deployment of trace back. While this makes the trace back service more available, regulating access to trace back service in a cloud- based architecture becomes an important issue. Consequently, we address the access control problem in cloud-based trace back. Our design objective is to check illegitimate users from requesting trace back information for malicious intentions such as ISPs topology discovery. To this end, we propose a temporal token- based authentication framework, called FACT, for authenticating trace back service queries. FACT embeds temporal access tokens in traffic flows, and then delivers them to end-hosts in an efficient manner. The proposed solution ensures that the entity requesting for trace back service is an actual recipient of the packets to be traced.

Keywords : IP trace back, marking based trace back, opportunistic piggyback marking, network forensics, Internet Service Provider (ISP), intrusion detection system

I.INTRODUCTION

A great amount of effort in modern years has been directed to the network security issues. In this paper, we tackle the difficulty of identifying the source of attacks. The device that generates the attacks may be a reflector, zombie, or a final link in a stepping stone chain. While identifying the device from which the attack was initiated as well as the person, behind the attack is a final challenge, we limit the difficulty of identifying the packets whose addresses may be spoofed source of the offending. Numerous solutions have been proposed for this problem. These solutions can be divided in two groups. The first group of the solutions depends on the routers in the network to send their identities to the destinations of definite packets, either encoding this information straightforwardly in seldom used bits of the IP header or by generating a new packet to the similar destination. The major limitation of this type of solutions is that they are paying attention only on flood-based (Distributed) Denial of Service {DoS) attacks and cannot handle attacks comprised of a small number of packets. The second group of solutions includes centralized management and logging of packet information on the network. Solutions of this type bring in a large overhead and are more complex and they are not scalable.

II. LITERATURE SURVEY

[1] Efficient Packet Marking for Large-Scale IP Traceback
Author proposed a new approach to IP traceback based on the probabilistic packet marking paradigm. Our approach, which we call randomize-and-link, uses large checksum cords to "link" message fragments in a way that is highly scalable, for the checksums serve both as associative addresses and data integrity verifiers. The main advantage of these checksum cords is that they spread the addresses of possible router messages across a spectrum that is too large for the attacker to easily create messages that collide with legitimate messages. Our methods therefore scale to attack trees containing hundreds of routers and do not require that a victim know the topology of the attack tree a priori. In addition, by utilizing authenticated dictionaries in a novel way, our methods do not require routers sign any setup messages individually.

[2] Practical Network Support for IP Traceback
This paper describes a technique for tracing anonymous packet flooding attacks in the Internet back towards their source. This work is motivated by the increased frequency and sophistication of denial-of-service attacks and by the difficulty in tracing packets with incorrect, or"spoofed", source addresses. In this paper we describe a general purpose traceback mechanism based on probabilistic packet marking in the network. Our approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs). Moreover, this traceback can be performed"post-mortem" after an attack has completed. We present an implementation of this technology that is incrementally deployable, (mostly) backwards compatible and can be efficiently implemented using conventional technology.

[3]FIT: Fast Internet Traceback

[9] E-crime is on the rise. The costs of the damages are often on the order of several billion of dollars. Traceback mechanisms are a critical part of the defense against IP spoofing and DoS attacks. Current traceback mechanisms are inadequate to address the traceback problem Problems with

the current traceback mechanisms: • victims have to gather thousands of packets to reconstruct a single attack path • they do not scale to large scale attacks • they do not support incremental deployment General properties of FIT: • IncDep • RtrChg • FewPkt • Scale • Local.

III.PROBLEM STATEMENT

End-to-end encryption and authentication mechanisms, such as TLS, do not solve any of the above issues, since they are agnostic to which path the packet takes. A stronger approach is needed, which enables routers and destinations to perform source authentication and path validation. The major signature of flooding-based attacks is a huge amount of forged source packets to exhaust a victim's limited resources. Another type of DoS attack, software exploit attacks, attacks a host using the host's vulnerabilities with few packets (e.g., Teardrop attack and LAND attack). Since most edge routers do not check the origin's address of a packet, core routers have difficulties in recognizing the source of packets. The source IP address in a packet can be spoofed when an attacker wants to hide himself from tracing. Therefore, IP spoofing makes hosts hard to defend against a DDoS attack. For these reasons, developing a mechanism to locate the real source of impersonation attacks has become an important issue nowadays

IV.EXISTING SYSTEM

The internet is the global media organization which can able to access by number of user. The existing research work used cannot able to track the ip hackers. Since the number of mechanism which involved can able to contain high computational cost. The information of the particular device can able to easily track by the hackers and intruders. Perhaps, the methodology is very sensitive and can easily broke by the attackers. The features which was related to the network can able to assume and the attacks cannot able to rectify by the user. Users can be linked to their locations, and multiple pieces of such information can be linked together. The LBS is a convenient process so the Adversary may easily access the user private information and location services.

Demerits

- Can be inferred from a user's whereabouts. This could make user the target of blackmail or harassment.
- A stalker can also exploit the location information.
- Misuse their rich data by, e.g., selling it to advertisers or to private investigators.
- Low privacy of a user.

V.PROPOSED SYSTEM

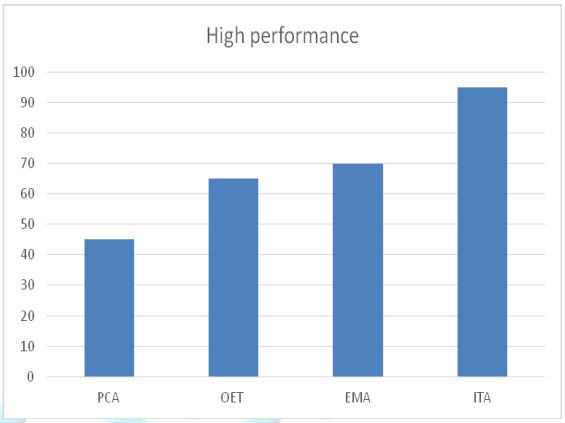
The proposed research work will mainly focus on the user privacy and security. The thesis proposed a method called implicit token scheme, which can able to protect the IP address. A novel antispoofing method, which provides continuous deployment incentives. It drops an outbound packet whose source address does not belong to the local server.

The packets which are dropped may sometimes cause lots of problems. So, the main contribution of this research is to safeguard the IP address from spoofer. For this reason, the research focused on a proposed method to hide the IP address. Since the internet is very large global communication medium, the user should hide the IP address. So the Adversary not entering the during communication between user and LBS.

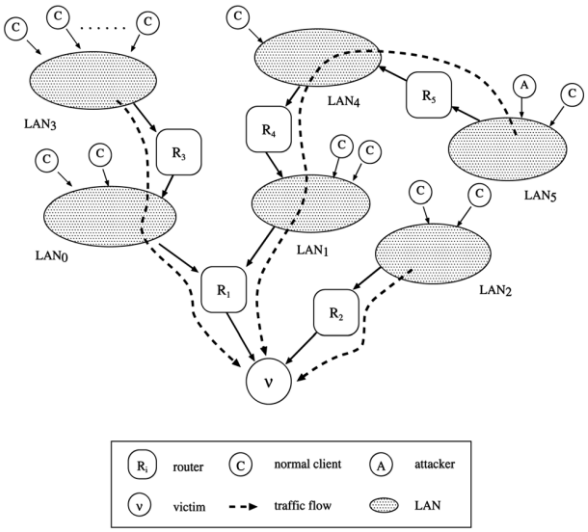
Merits

- The System is attached to the information and protected with the digital signature.
- Malicious users cannot mislead others into receiving fake information, because messages are digitally signed by the LBS.
- A user's query becomes hidden from the server due to Mobi Crowd protocol.
- To provide high security and less time processing.

Experimental Result:



VI.IMPLEMENTATION



Most of current single packet traceback schemes tend to log packets' information on routers. Most current tracing schemes that are designed for software exploits can be categorized into three groups: single packet, packet logging and hybrid IP traceback . The basic idea of packet logging is to log a packet's information on routers. The methods used in the existing systems include Huffman Code, Modulo/ Reverse modulo Technique (MRT) and MOdulo/REverse modulo (MORE). These methods use interface numbers of routers, instead of partial IP or link information, to mark a packet's route information. Each of these methods marks

routers' interface numbers on a packet's IP header along a route. However, a packet's IP header has rather limited space for marking and therefore cannot always afford to record the full route information.

VII.ALGORITHM

Output : ipaddress changed as various name

GET the packet
SET packet as pkt
FOR EACH packet pkt
IF pkt in TOKEN THEN
Forward the packets with ipaddress
ELSE IF check cookies (pkt) is equal to TRUE THEN
Forward pkt without ipaddress
ELSE
Hide ipaddress
END

Algorithm: Edge Marking Procedure at router R

```
for (each packet w targeted to the victim site V) {
  generate a random number x between [0..1);
  if (x < p) { /* router R needs to mark the pkt*/
    write R into w.start and 0 into w.distance;
  }
  else { /* router R doesn't need to mark */
    if (w.distance == 0) {
      write R into w.end;
    }
    increment w.distance;
  }
}
```

VIII. SYSTEM MODEL

- ✓ Intra-AS Structure: A trace back server is deployed in each trace backdeployed AS. Traffic flow information collected at trace backenabled routers will be exported to internal cloud storage which is managed by the trace back server in each AS for long-term storage and analysis. Routers may independently sample the traffic or collect the traffic flow in a coordinated fashion.
- ✓ Trace back as a Service: Trace back-enabled ASes expose their trace back services in the trace back coordinaton
- ✓ Inter-AS Logical Links: To maintain inter-AS logical relations, and achieve efficient trace back processing and high incremental deploy ability

IX. CONCLUSION AND FUTURE WORK

In this work, we first presented the cloud-based IP trace back architecture, which possesses several favorable properties that previous trace back schemes failed to satisfy simultaneously. We then focused on the access control problem in the context of cloud-based trace back, where the objective is to prevent illegitimate users from requesting trace back information for ill intentions. To this end, we proposed the FACT, an enhanced user authentication framework which ensures that the entity requesting for the trace back procedure is an actual recipient of the flow packets to be traced. Evaluation studies based on real-world Internet traffic datasets demonstrated the feasibility and effectiveness of the proposed FACT. Privacy is perhaps the most significant long-term challenge facing the successful roll-out of location-based experiences. Monitoring a user's location and transmitting this to other users, or storing it centrally, has the potential to seriously compromise individual privacy. Solutions are likely to rely in a mixture of technical, social and perhaps even legal mechanisms. Technical mechanisms for handling privacy will involve the careful choice of location-sensing technologies (e.g. preferring those that run only on the user's local device), along with mechanisms for controlling disclosure, backed up with appropriate security mechanisms.

X. REFERENCES

[1]. Aloysius Wooi Kiak Ang, Wee Yong Lim, and Vrizlynn L. L. Thing "FACT: A Framework for Authentication in CloudBased IP Traceback," IEEE Transactions on Information Forensics And Security, Vol. 12, No. 3, March 2017.

[2]. T. H.-J. Kim, C. Basescu, L. Jia, S. B. Lee, Y.-C. Hu, and A. Perrig, "Lightweight source authentication and path validation," in Proc. SIGCOMM, 2014, pp. 271-282.

[3]. Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An IP traceback system to find the real source of attacks,"IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 4, pp. 567-580, Apr. 2009.

[4]. S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS attacks using entropy variations," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 3, pp. 412-425, Mar. 2011. [5] L. Cheng, D. M. Divakaran, W. Y. Lim, and V. L. L. Thing, "Opportunistic piggy-back marking for IP traceback," IEEE Trans. Inf. Forensics Security, vol. 11, no. 2, pp. 273-288, Feb. 2016.

[5]. H. Tian and J. Bi, "An incrementally deployable flowbased scheme for IP trace-back,"IEEE Commun. Lett., vol. 16, no. 7, pp. 1140-1143, Jul. 2012.

[6]. G. Yao, J. Bi, and A. V. Vasilakos, "Passive IP trace back: Disclosing the locations of IP spoofers from path back scatter,"IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 471-484, Mar. 2015.

[7]. H. Zhang, J. Reich, and J. Rexford, "Packet traceback for software defined networks," Princeton Univ., Princeton, NJ, USA, Tech. Rep. TR-978-15, 2015

