International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
SKRGC Since 2012

http://www.ijcsjournal.com Volume 6, Issue 1, No 01, 2018 ISSN: 2348-6600
Reference ID: IJCS-327 PAGE NO: 2171-2178

A NOVEL APPROACH TO DISCLOSE THE LOCATIONS OF IP SPOOFERS USING ICMP

Zarfin Rubaina.R, Ranjani.S, Swarna Lakshna.S, Roshini.G
P.BArun Prasad ME
Assistant Professor
Saranathan College of Engineering
arunprasad-it@saranathan.ac.in

Abstract— The system implementation mainly focusing disclosing the Locations of IP Spoofers from Path Backscatter using the passive IP trace back (PIT) that bypasses the deployment difficulties of IP trace back techniques. PIT investigates Internet Control Message Protocol error messages (named path backscatter) triggered by spoofing traffic, and tracks the spoofer's based on public available information (e.g., topology). In this way, PIT can find the spoofer's without any deployment requirement. This paper illustrates the causes, collection, and the statistical results on path backscatter, demonstrates the processes and effectiveness of PIT, and shows the captured locations of spoofer's through applying PIT on the path backscatter data set. These results can help further reveal IP spoofing, which has been studied for long but never well understood. Though PIT cannot work in all the spoofing attacks, it may be the most useful mechanism to trace spoofers before an Internet-level trace back system has been deployed in real.

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

1.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.

A number of notorious attacks rely on IP spoofing, including SYN flooding, SMURF, DNS amplification etc.A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system. The Smurf Attack is a distributed denial-of-service attack in which large numbers of packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. A Domain Name Server (DNS) amplification attack is a popular form of distributed denial of service (DDoS) that relies on the use of publically accessible open DNS servers to overwhelm a victim system with DNS response traffic.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
http://www.ijcsjournal.com Volume 6, Issue 1, No 01, 2018 ISSN: 2348-6600
Reference ID: IJCS-327 PAGE NO: 2171-2178

To capture the origins of IP spoofing traffic is of great importance. As long as the real locations of spoofers are not disclosed, they cannot be deterred from launching further attacks. Even just approaching the spoofers, for example, determining the networks they reside in, attackers can be located in a smaller area, and filters can be placed closer to the attacker before attacking traffic get aggregated. Identifying the origins of spoofing traffic can help build a reputation system for network, which would be helpful to push the corresponding ISPs to verify IP source address.

Spoofing is the action of making something look like something that it is not in order to gain unauthorized access to a user's private information. The idea of spoofing originated the discovery of a security hole in the TCP protocol. Today spoofing exists in various forms namely IP,URL and Email spoofing.

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.

2. 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

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 01, 2018 ISSN: 2348-6600
Reference ID: IJCS-327 PAGE NO: 2171-2178

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.

3.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

4. EXISTING SYSTEM

IP SPOOFING, which means attackers launching attacks with forged source IP addresses, has been recognized as a serious security problem on the Internet for long. By using addresses that are assigned to others or not assigned at all, attackers can avoid exposing their real locations, or enhance the effect of attacking, or launch reflection based attacks. IP traceback techniques are designed to disclose the real origin of IP traffic or track the path.

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.
- The real locations of spoofers are not disclosed
- Attackers cannot be deterred from launching further attacks
- Due to the challenges of deployment, there has been not a widely adopted IP traceback solution, at least at the Internet level

PROPOSED SYSTEM:

Instead of proposing another IP traceback mechanism with improved tracking capability, propose a novel solution, named Passive IP Traceback (PIT), to bypass the challenges in deployment. Routers may fail to forward an IP spoofing packet due to various reasons, e.g., TTL exceeding. In such cases, the routers may generate an ICMP error message (named path backscatter) and send the message to the spoofed source address. Because the routers can be close to the spoofers, the path backscatter messages may potentially disclose the locations of the spoofers. PIT exploits these path backscatter messages to

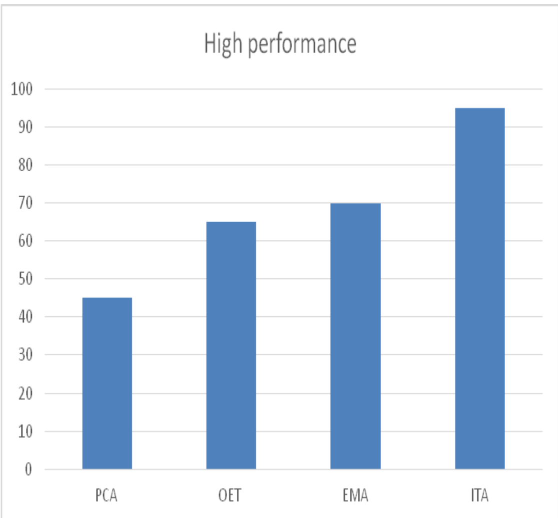
International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 01, 2018 ISSN: 2348-6600
Reference ID: IJCS-327 PAGE NO: 2171-2178

find the location of the spoofers. With the locations of the spoofers known, the victim can seek help from the corresponding ISP to filter out the attacking packets, or take other counterattacks. PIT is especially useful for the victims in reflection based spoofing attacks, e.g., DNS amplification attacks. The victims can find the locations of the spoofers directly from the attacking traffic.

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:



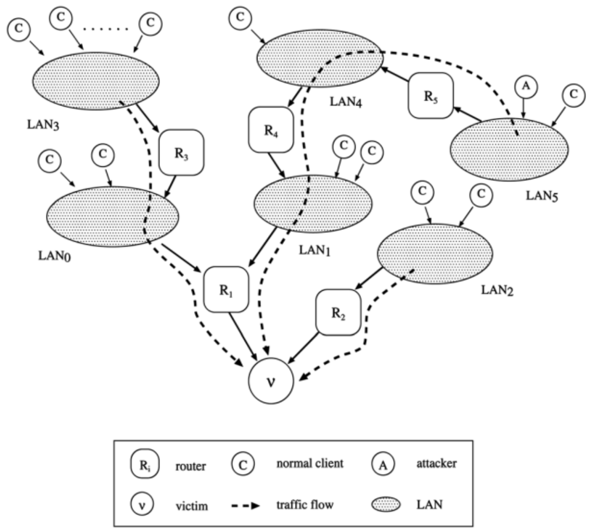
Related Work :

The related work can be categorized into two parts. The first one describes the existing IP traceback mechanisms, and the second one introduces IP spoofing observation activities.

IP Traceback:

IP traceback methods are developed to reveal the real origin of IP traffic or track the path. The existing IP traceback approaches can be classified into the following: packet marking, ICMP traceback, logging on router, link testing,Overlay and hybrid tracing. modify the header of packets to contain information of the packets. There are two types of packet marking schemes: probabilistic packet tagging [4], and deterministic supported by routers, it is challenging to enable packet marking in the network. Logging on router [6] involves routers keeping a history of all the packets it has forwarded. Attack path can be rebuilt from log on the router. In link testing scheme, the upstream of hop-by-hop attacking traffic is determined, while the attack is in progress.

5. IMPLEMENTATION



International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 01, 2018 ISSN: 2348-6600
Reference ID: IJCS-327 PAGE NO: 2171-2178

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.

6.Algorithm

one packet may take two hops to the victim site V whereas another packet may take 15. Therefore, it is impossible to preallocate a sufficient amount of space in the packet header. Another technical difficulty in recording the complete traversed path is that an attacker can potentially manipulate this path information to fill in false router identifications, in order to mislead the path analysis. Rather than record the complete path, probabilistic edge marking [14], [17] proposes to record only a traversed edge from the attacker to the victim site V in a probabilistic fashion. The marking algorithm uses some unused fields in the existing IP header to store three fields of information. The three fields are {start, end, distance} . The start and end fields store the IP addresses of the two routers at the end points of the marked edge while the distance field records the number of hops between the marked edge and the victim site V . When a victim site V is under a DDoS attack, it will send a marking-request- signal to a set of routers (i.e., all the routers which are within d ! 1 hops from V) requesting their participation in the probabilistic edge marking process. Each participating router will then mark each packet destined for V with probability p . In other words, whenever an IP packet addressed to V passes through a router in the enabled router set, the router, upon deciding the out-going edge of the packet through standard routing lookup, will mark the out-going edge in the packet's IP header with probability p . If marking is performed, the router records its IP address in the start field and sets the value of the distance field to zero. If the router decides not to mark the packet, the router needs to check whether the distance field of the packet is equal to zero or not. If it is equal to zero, the router records its IP address in the end field and then increments the distance field by one. If the distance field is not equal to zero, the router simply increments the distance field by one. Note that the mandatory increment of the distance field is crucial because it is used to minimize the probability of spoofing a marked edge. Under the marking method, any packet generated by an attacker will have a distance greater than or equal to the hop count between the victim site V and the attacker. Therefore, an attacker cannot forge any edge between itself and V . The probabilistic edge marking algorithm used by each participating router in the enabled set is illustrated in Fig. 1. By the property of the probabilistic marking algorithm, each traversed edge of an attack packet will have a different probability of being marked or unmarked. Let P m ð d Þ denote the probability that a victim site V will find an edge which is d hops away as a marked edge. In general, we have In other words, an edge which is d hops away from the victim site V will only be marked if a router connected to that edge decides to mark the packet and the remaining

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
SKRGC Since 2012
http://www.ijcsjournal.com
Reference ID: IJCS-327
Volume 6, Issue 1, No 01, 2018
ISSN: 2348-6600
PAGE NO: 2171-2178

routers along the same path decide not to mark this packet (thereby overwriting any old mark). Let P u ð d Þ be the probability that a victim site V will not find an edge which is d hops away or closer as a marked edge. We have This happens when all the routers along the path to V decide not to mark the packet. Fig. 2 illustrates the set of marked and unmarked edges collected by the victim site V under a simple linear network topology. In the example, V can collect four types of packets. The first three types are marked packets with edges ð R 3 ; R 2 Þ , ð R 2 ; R 1 Þ , and ð R 1 ; ÀÞ , respectively. The last type of packet that can be received by V is the unmarked packet. V , upon receiving packets, needs to first filter out those unmarked packets since they do not carry any information useful in the attack graph construction. For all the collected marked packets, the victim site V needs to execute the graph construction algorithm, shown in Fig. 3, to construct the attack graph. To illustrate the attack graph construction algorithm, let us consider a network which has a tree-like topology as depicted in Fig. 4. In the figure, the routers are represented by 1. R i Path and the 1: R 3 victim ! R 2 ! site R 1 is ! represented V , by V . Packets passing 2. Path through 2: R 4 ! the R 2 ! routers R 1 ! V will , be marked by the probabilistic 3. Path 3: edge R 7 ! marking R 6 ! R algorithm 5 ! V , and shown in Fig. 1. At the 4. end Path of the 4: R measurement 10 ! R 9 ! R 8 period, ! V . the victim site V will have It is received important a to number point out of that packets the following with the advantages marking of classification the probabilistic shown marking in Table 1. algorithm: V uses these marked packets to create an attack graph based on the attack graph construction algorithm in Fig. 3. From the above example, the attack graph contains four linear paths, which are: 1. Path 1: R 3 ! R 2 ! R 1 ! V , 2. Path 2: R 4 ! R 2 ! R 1 ! V , 3. Path 3: R 7 ! R 6 ! R 5 ! V , and 4. Path 4: R 10 ! R 9 ! R 8 ! V .

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;
  }
}
```

7. SYSTEM MODEL

Proxy Switcher

Proxy Switcher allows to automatically execute actions, based on the detected network connection. As the name indicates, Proxy Switcher comes with some default actions, for example setting proxy settings for Internet Explorer, Firefox and Opera. Automatic change of proxy

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 01, 2018 ISSN: 2348-6600
Reference ID: IJCS-327 PAGE NO: 2171-2178

configurations (or any other action) based on network information:

Sql Injection Attack

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

Passive IP Traceback

The Distributed Denial of Service (DDoS) attacks are launched synchronously from multiple locations and they are extremely harder to detect and stop. Identifying the true origin of the attacker along with the necessary preventive measures helps in blocking further occurrences these types of attacks. The issue of tracing the source of the attack deals with the problem of IP traceback.

8. CONCLUSION AND FUTURE WORK

The proposed system try to dissipate the mist on the locations of spoofers based on investigating the path backscatter messages. Passive IP Traceback (PIT) tracks spoofers based on path backscatter messages and public available information. Specified how to apply PIT when the topology and routing are both known, or the routing is unknown, or neither of them are known. An effective algorithm is used to apply PIT in large scale networks and proofed their correctness. Demonstrated the effectiveness of PIT based on application. The proposed system showed the captured locations of spoofers through applying PIT on the path backscatter dataset. These results can help further reveal IP spoofing, which has been studied for long but never well understood.

In this project a new technique, backscatter analysis is presented, for estimating denial-of-service attack activity in the Internet. Using this technique, we try to dissipate the mist on the actual locations of spoofers based on investigating the path backscatter messages. In this, project Passive IP Traceback (PIT) is proposed, which tracks spoofers based on path backscatter messages and public available information. The future enhancement will focus on the proxy switcher , in that the browser identifies if the user spoofs the IP address.

We proved that, the effectiveness of PIT based on deduction and simulation. We showed the captured locations of spoofers through applying PIT on the path backscatter dataset.

9. 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.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 01, 2018 ISSN: 2348-6600
Reference ID: IJCS-327 PAGE NO: 2171-2178

[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.

[6] 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.

[7] 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.

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