International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 3 (March'2016)

LOCATING THE WISECRACKERS USING SPOOFER

B.Praveen Kumar,
Assistant Professor,
Computer science and engineering,
Velammal Institute of Technology,Chennai,India.

N.Haripreethi,
Student,
Computer science and engineering,
Velammal Institute of Technology,Chennai,India.

S.Shilpa,
Student,
Computer Science and Engineering,
Velammal Institute of Technology,Chennai,India.

B.Bharathi,
Student,
Computer science and engineering,
Velammal Institute of Technology,Chennai,India.

Abstract: In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. Many mechanisms have been introduced to find the real location of the spoofer, but the spoofer changes his IP address dynamically and thus finding the mother IP is difficult and it adds complication in finding the real location. The recent mechanisms find the last hit IP address of the spoofer. In this paper we propose a mechanism to find the mother IP address of the spoofer i.e. the original IP address with the help of the last hit IP address.

Key Words: Spoofing, IP trace back, DOS.

I.INTRODUCTION:

A **packet** is the unit of data that is routed between an origin and a destination on the Internet. An Intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system. When the data is sent by the sender the intruder tries to hack the data and thus there is a possibility of data being destroyed or changed and thus the sender may receive the false data. In a spoofing attack, the intruder sends messages to a computer indicating that the message has come from a trusted system. To be successful, the intruder must first determine the IP address of a trusted system, and then modify the packet headers, to that it appears that the packets are coming from the trusted system.

IP Spoofing[4] is one of the major tools used by hackers in the internet to mount denial of service attacks. DoS attacks can be classified into flooding attacks and software exploits [4]. In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. The most common kind of DoS attack is simply to send more traffic to a network address than the programmers who planned its data buffers [3] anticipated by someone. Although a DoS attack does not usually result in the theft of information or other security loss, it can cost the target person or company a great deal of time and money .A denial of service attack can also destroy programming files in affected computer systems.

It is hard to find the intruder who does such notorious activities in network because he uses some forge IP to conceal his own location and changes his IP dynamically and hence it is hard to find which is the real location of the intruder. In the proposed system we use the old trace back mechanism to find the last hit IP address. From the last hit IP address we use the spoofing detection algorithm to further investigate the last hit IP and thus it finds out the real IP of the intruder. The trace back mechanism which is used to find the last hit IP address is Packet marking algorithm [1]. The network path information is recorded to both, the routers and packets. The packet first traverses the network. The packet may traverse the network in different paths. At that stage a particular path traversed alone is taken into account and it is recorded, while the upstream portion of the traversed path is recorded at few intermediate routers. The routers consider the free space availability in the marking field and depending on that they record the path information. The information is written in to the packets when there is free space in the field else the routers compute and record the packet digests with the path information and then clear the marking field. Thus an IP Trace back approach is developed. This approach reduces the storage overhead of packet digests to one half and reduces the access time requirement for recording packet digests by a factor [1].

II.RELATED WORK

The denial of service (dos)[2] is a major threat in the internet. Previously the IP spoofing was used to trace the real location, by the attackers. But now it is impossible to determine the real location exactly as the spoofers keep changing their IP address dynamically. The trace Bach methods used are IP logging, IP marking and IETF ICMP Trace back (I Trace), called ICMP Trace back with Cumulative Path (I Trace-CP). It is often useful to learn the path that packets take through the Internet. This is especially important for dealing with certain denial-of-

service attacks, where the source IP is forged [5]. There are other uses as well, including path characterization and detection of asymmetric routes. There are existing tools, such as traceroute, but these generally provide the forward path, not the reverse. ICMP Trace back message [1] could be used to solve this problem. When forwarding packets, routers can, with a low probability, generate a Trace back message that is sent along to the destination [7]. With enough Trace back messages from enough routers along the path, the traffic source and path can be determined but the exact location of the spoofer still remains unfound.

There are security issues with the backscatter messages. The victim has to know the hop count from the routers to itself and the attacker must be capable of knowing the hop count from the victim to each router. The attacker finds it difficult to get the hop count as the tracing is done directly. There occurs possibility for the attackers to even send forged messages with the possible TTL values. Time to live (TTL) or hop limit [6] is a mechanism that limits the lifespan or lifetime of data in a computer or network. TTL may be implemented as a counter or timestamp attached to or embedded in the data. Once the prescribed event count or timespan has elapsed, data is discarded. In computer networking, TTL prevents a data packet from circulating indefinitely. But however the victim can find the forged backscatter messages.

Now is that instead of proposing another IP trace back mechanism to capture the intruder, Passive IP Trace back (PIT) mechanism is introduced. In this concept the routers generates an ICMP error message (named *path backscatter*). As the routers can be close to the spoofers, the path backscatter messages may disclose the locations of the spoofers. PIT exploits these path backscatter messages to find the location of the spoofers. In this, the list of IP address is obtained and the victim can seek help from the corresponding ISP to filter out the attacking packets. PIT is especially useful for the victims in reflection based spoofing attacks. The victims can find the locations of the spoofers directly from the attacking traffic. The probabilistic packet marking (PPM) algorithm [10] is used to solve the IP trace back problem. It is a used to discover the Internet map or an attack graph during a distributed denial-of-service attack.

The Distribute Denial of Service (DDOS) [8] is also a threat in today's internet. To determine the attacked packets to help the victim, the path identification DDOS scheme is used as a deterministic packet marking scheme. A new defense mechanism has been used which also detects the IP address of the spoofer on a per packet basis called as Stackpi. .pi refers to path identification.To determine the path traversed by the packets through the routers the Pi marking scheme has been used. The packet is marked deterministically by the routers along its path to the destination. When the packets travel along the same path it will have the same marking and thus the attack victim finds it easy because the victim has to identify only the Stackpi marks of attack packet to find out the packets being affected. The Stackpi marks can be used with source IP address to detect the spoofing. Thus the Stackpi serves several purposes like DDOS attacks, IP spoofing attacks and multicast spoofing attacks

Two new schemes have been proposed to improve the deployment performance namely Stack-based marking and write-ahead marking. The interaction between the Pi-enabled routers and legacy routers is eliminated by stack marking. The stack marking is however not applicable for all the situations as it tracks only the path of packets via few routers. Thus the attackers can shift between different Pi markings making it difficult for the victim. When a Pi enabled router is followed by a legacy router then we use write-ahead marking .During such cases the Pi-enabled router will mark itself as well as the next hop router.

III. ALGORITHM

Internet protocol (IP) is a network protocol operating at layer 3 (network) of the OSI model. It is a connectionless model, meaning there is no information regarding transaction state, which is used to route packets on a network. Additionally, there is no method in place to ensure that a packet is properly delivered to the destination. IP trace back is the ability to trace the IP packets to their origins.

The IP trace back problem is made very relevant because of the rising threat of cyber-attacks especially in DDOS. The Deterministic Packet marking (DPM) algorithm has no bandwidth and practically no processing overhead on the network equipment. Many number of simultaneous attacks can be determined using this approach. The processing is done by the victim. The DPM is capable of performing the trace back without revealing the topology of the provider's network which is a desirable quality.

The Flexible Deterministic Packet Marking (FDPM) provides more flexible features to trace the IP packets and it is capable of obtaining better tracing capability over other IP trace back mechanisms, such as link testing, messaging, logging, Probabilistic Packet Marking (PPM) and Deterministic Packet Marking (DPM) [6] .The FDPM is quite simple as it needs only small number of packets to compute the trace back and the manual work is also less. Thus this approach seems to be more powerful than the rest. This approach is also used in many security systems such as DDoS defense systems, Intrusion Detection Systems (IDS), forensic systems, and so on.

The IP trace back technique has two dimensions namely packet marking and packet logging. The IP trace back based on packet marking is called as PPM. In this, the packets are probabilistically marked with the path information partially as they are forwarded to the routers.Beacuse of this technique being probabilistic only the source of the traffic can be determined and not the exact path. In the packet logging the routers compute and store the digest when each packet is forwarded. The digest is a hash of the source IP address and is shorter than the IP address. It is also called as hash-based

approach and is capable of determining the individual packet to its source. But because of the digests the memory is more.

Marking procedure at router R:

for(each packet w received by the router)
{
generate a random number x between [0..1);
if (x < pm and flag=0) then /* router starts marking. flag 0 implies that the packet is not encoded previously */
write router's address into w.start and 0 into w.distance
else {
If (w.distance = 0) then
write router address into w.end and 1 into flag
} /* flag 1 implies that the packet has encoded an edge and no other successive routers should start encoding */
If (flag = 1) then
Increment w.distance by 1 /* w.distance represents the distance of the encoded edge from the victim V */
} }

A passive IP trace back (PIT)[1] that bypasses the deployment difficulties of IP trace back techniques is used.ICMP- the Internet Control Message Protocol (ICMP) is one of the main protocols of the Internet Protocol Suite. It is used by network devices, like routers. Backscatter is the reflection of waves, particles or signals back to the direction from which they came. PIT investigates Internet Control Message Protocol error messages (named path backscatter) triggered by spoofing traffic, and tracks the spoofers based on public available information (eg. topology).

In computer networking, the term IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP 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 messages to a computer indicating that the message has come from a trusted system. To be successful, the intruder must first determine the IP address of a trusted system, and then modify the packet headers to that it appears that the packets are coming from the trusted system. In essence, the attacker is fooling (spoofing) the distant computer into believing that they are a legitimate member of the network. The goal of the attack is to establish a connection that will allow the attacker to gain root access to the host, allowing the creation of a backdoor entry path into the target system.

When the workstation requests a page from the web server the request contains both the workstation's IP address (i.e. source IP address 192.168.0.5) and the address of the web server executing the request (i.e. destination IP address 10.0.0.23). The web server returns the web page using the source IP address specified in the request as the destination IP address, 192.168.0.5 and its own IP address as the source IP address, 10.0.0.23.

Figure 1: Valid source IP address, illustrates a typical interaction between a workstation with a valid source IP address requesting web pages and the web server executing the requests.

IP Spoofing is one of the major tools used by hackers in the internet to mount denial of service attacks. In such attacks the attackers duplicate the source IP of packets that are used in the attack. Instead of carrying the original source IP of the machine the packet came from, it contains an arbitrary IP address which is selected either random fashion or particularly. The ease with which such attacks are generated made them very popular. There are at least four thousand such attacks happening every week in the Internet.In proposed system a concept is used which helps to trace back the mother IP address of the attackers who hack the sender's data.In proposed system a concept is used which helps to trace back the mother IP address of the attackers who hack the sender's data.

IV.PROPOSED SYSTEM

Instead of proposing another mechanism to trace the IP with improved features, we propose a technique that could help us in finding the attacker's mother IP at any situation. The first step could be creation of node. In communication networks, a node is either a connection point, a redistribution point, or a communication endpoint (e.g. data terminal equipment). The definition of a node depends on the network and protocol layer .A physical network node is an active electronic device that is attached to a network, and is capable of creating, receiving or transmitting information over a communications channel. A node is created using a particular IP address. Collection of nodes forms the network. Every node has a unique IP address and a name. When submitted the node is created.

After the creation of nodes, the files that ought to be shared is selected from the system environment. The selected file is going to communicate between a sender and a receiver. At first the selected file should be read from system path. The content is loaded in fixed path. Only when the files are selected it can be shared by the sender to the receiver. A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

There could be many reasons for a router in not transferring the packets such as TTL exceeding. Time to live (TTL) or hop limit is a mechanism that limits the lifespan or lifetime of data in a computer or network. When the limit is exceeded the packets get discarded. The intruder tries to hack the packet. An Intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system. In summary, this person attempts to violate security issues by interfering with system availability, data integrity or data confidentiality.

Now is that the data sent is hacked by the intruder and it known that attackers may use forged source IP address to conceal their real locations. The attackers change their IP address dynamically. As soon as the data is hacked by the intruder, the router sends an alert message to both the sender and receiver. Using this message the last hit IP address is known from which the original IP (mother IP) of the spoofer could be traced. And also after knowing the data being used by the intruder, sender and the receiver can change their kernel configuration so that the further packets are passed in a safer network.

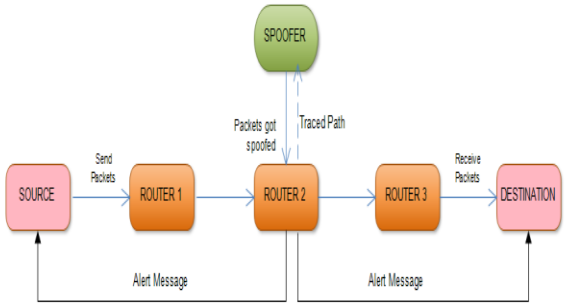

Figure 2: Architecture Diagram

V.RESULT EVALUATION

Tracing the IP address of the spoofer was very arduous in the beginning. Later on many algorithms were proposed to trace back the IP address, but each algorithm had its' own drawbacks. At each stage, certain technologies were used with advancement at each stages. In this paper, the advancement includes tracing back not only the attacker's IP (last hit IP) but also trace and find it's mother IP (original IP). The graph indicates the tracing back of the mother IP over a period of time drastically.

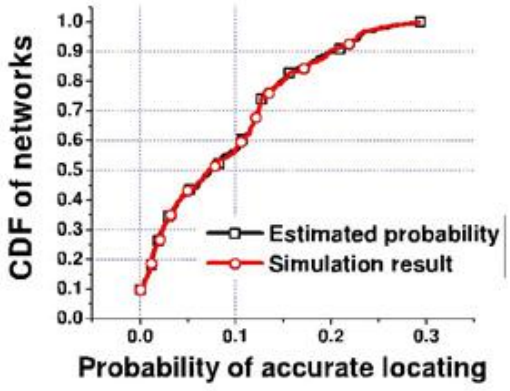

Figure 3: Probability of accurate tracing

VI.CONCLUSION

In this paper, we have proposed a methodology to detect not only the attacker's IP(last hit IP) but also trace and find it's mother IP(original IP). We try to dissipate the mist on the actual locations of spoofers based on investigating the path backscatter messages. In this method the tracing can be done despite the topology and routing remaining unknown.In the existing system, backscatter message detects only the last hit IP address (one of the multiple forged IP's) thus the avoidance of the intruders hacking the data becomes difficult. In proposed system the last hit IP address of the intruders are further investigated and the mother IP address is thus found. This technique can also be used for tracing multiple packets.

VII. REFERENCES

[1]. Disclosing the Locations of IP Spoofers From Path Backscatter Guang Yao, Jun Bi, Senior Member, IEEE, and Athanasios V. Vasilakos, Senior Member, IEEE March2015

[2]. H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in Proc. LISA, 2000, pp. 319–327.

[3]. R. P. Laufer et al., "Towards stateless single-packet IP traceback," in Proc. 32nd IEEE Conf. Local Comput. Netw. (LCN), Oct. 2007.

[4]. H. C. J. Lee, V. L. L. Thing, Y. Xu, and M. Ma, "ICMP traceback with cumulative path, an efficient solution for IP traceback," in Information and Communications Security. Berlin, Germany: Springer-Verlag, 2003.

[5]. A. Yaar, A. Perrig, and D. Song, "FIT: Fast internet traceback," in Proc. IEEE 24th Annu. Joint Conf. IEEEComput. Commun. Soc. (INFOCOM), vol. 2. Mar. 2005.

[6]. Passive IP Traceback: Disclosing the Locations of Man in the Middle from Path Backscatter AmanShekhar, Krishan Yadav, Krishna Yele, Utpal Chirag, Ms. Santhi K. Guru.

[7]. M. D. D. Moreira, R. P. Laufer, N. C. Fernandes, and O. C. M. B. Duarte, "A stateless traceback technique for

identifying the origin of attacks from a single packet," in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2011.

[8]. M.-H. Yang and M.-C. Yang, "Riht: A novel hybrid IP traceback scheme," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 789–797, Apr. 2012.

[9]. A. Mankin, D. Massey, C.-L. Wu, S. F. Wu, and L. Zhang, "On design and evaluation of 'intention-driven' ICMP traceback," in Proc. 10th Int. Conf. Comput. Commun. Netw., Oct. 2001.

[10]. AN EFFICIENT IP TRACEBACK THROUGH PACKET MARKING ALGORITHM, Y.Bhavani, P.Niranjan Reddy

[11]. S. Bellovin, M. Leech, and T. Taylor, ICMP Traceback Messages, Internet Draft -BellovinItrace-04.txt, Feb. 2003.

[12]. M. Adler, "Trade-Offs in Probabilistic Packet Marking for IP Traceback," J. ACM, Mar. 2005.

[13]. M. T. Goodrich, "Efficient Packet Marking for Large-Scale IP Traceback," in Proc. of ACM CCS 2002, Nov. 2002.

[14]. D.X. Song and A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," Proc. IEEE INFOCOM '01, Apr. 2001.

[15]. Tao peng, Christopher Leckie and KotagiriRamamohanarao. Adjusted probabilistic packet marking for IP traceback. In Proceedings of Networking 2002 Pisa, Italy, May 2002.

[16]. Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An iptraceback system to find the real source of attacks," Parallel and Distributed Systems, IEEE Transactions on, vol. 20, no. 4, pp. 567–580, 2009.

[17]. C. Labovitz, "Bots, ddos and ground truth," NANOG50, October, vol. 5, 2010.

[18]. W. Caelli, S. Raghavan, S. Bhaskar, and J. Georgiades, "Policy and law: denial of service threat," in An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks, pp. 41–114, Springer, 2011.

[19]. A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, "Hash-based iptraceback," in ACM SIGCOMM Computer Communication Review, vol. 31, pp. 3–14, ACM, 2001.

[20]. A. Belenky and N. Ansari, "Iptraceback with deterministic packet marking," IEEE communications letters, vol. 7, no. 4, pp. 162–164, 2003.

