AN IMPROVED IP TRACEBACK MECHANISM FOR NETWORK SECURITY

N.Srilakshmi[1], K.Rani[2]

[1] Student, [2]Asst. Professors, Department of CSE, VR Siddhartha Engineering College
srilakashmi57@gmail.com, beulahrani.cse@gmail.com

Abstract

IP traceback is amongst the main challenges that face the security of today’s Internet. Many techniques were proposed, including in-band packkhranits alert and outband packets each of them has advantages and disadvantages. Source IP spoofing attacks are critical issues to the Internet. These attacks are considered to be sent from bot infected hosts. There has been active research on IP traceback technologies. However, the traceback from an end victim host to an end spoofing host has never yet been achieved, because of the insufficient traceback probes installed on each routing path. There exists a will need to replace alternative probes in an effort to lessen the installation cost.

Recently a great number of technologies of a given detection and prevention have developed, but it is difficult the fact that the IDS distinguishes normal traffic that are caused by the DDoS traffic due to many changes in network features.

In existing work a whole new hybrid IP traceback scheme with efficient packet logging reaching to tend to have a fixed storage requirement for each router (CAIDA’s data set) in packet logging without the need to refresh the logged tracking information and then to achieve zero false positive and false negative rates in attack-path reconstruction. Existing hybrid traceback approach applied on offline CAIDA dataset which isn't suitable to realtime tracing. With this proposed work efficient hybrid approach for single-packet traceback to our best knowledge, our approach will reduces 2/3 of a given overhead in each of storage and how about recording packet paths, and to discover the time overhead for recovering packet paths is also reduced by a calculatable amount.

Keywords –*Attack, Trace back, LAN*

---***---

1. INTRODUCTION

A flooding-based Distributed Denial of Service (DDoS) attack is a very common way to attack a victim machine by sending a large amount of unwanted traffic. Network level congestion control can throttle peak traffic to protect the network. However, it cannot stop the quality of service (QoS) for legitimate traffic from going down because of attacks. Two features of DDoS attacks hinder the advancement of defense techniques. First, it is hard to distinguish between DDoS attack traffic and normal traffic. There is a lack of an effective differentiation mechanism that results in minimal collateral damage for legitimate traffic. Second, the sources of DDoS attacks are also difficult to find in a distributed environment. Therefore, it is difficult to stop a DDoS attack effectively.The internet rapidly develops on recent times and significantly influences increasingly more industry and business services. When popularity of the broadband, more houses are linked to the web Therefore, the difficulties of network security are actually. Currently, the primary threats of network security are coming from hacker intrusion, deny of service (DoS), malicious program, spam, malicious code and sniffer since there quite a few weaknesses within the original design of IPv4. The most common weakness is the idea that attackers could send IP spoofing packets and that is he likes to attack. Quite simply, the attackers modify the IP beginning with the true individual to another IP field. If these IPs are randomly generated then it is most more difficult to trace the fundamental cause of attacks from victims. Besides, the cunning attackers won't directly attack the targets. They could construct the botnet first then order them to attack the targets. However, it raises the damage grade of attack and tracing the attacks will be more difficult. The fact is, we are able to morally persuade the attackers or punish them by law after we obtain the way to obtain attacks. The process of searching source is called IP traceback. There are several practices trace attack source with the help of routers.

A Denial-of-Service (DoS) attack is characterized by an explicit attempt by an attacker to avoid legitimate users of a service through the use of the intended resources [1]. While launching their attacks, the attackers usually generate a huge volume of packets introduced to the target systems named victims, causing a network internet traffic congestion problem. Thus the legitimate users will be prevented from getting access to the systems actually being attacked. This paper specializes using an ground breaking marking scheme to defend against DoS attacks. Our company proposes a methodology, dependent on a packet discrepancy technique, to trace DoS attacks, especially glow attacks. Reflector attacks be owned by the category of the extremely serious DoS attacks. Unlike other DoS attacks, the number of attack packets served by the reflector attacker would be amplified persistently, flooding the victim's network. The attack packets reaching the victim are not direct from the attacker; they will be actually generated by some hosts regarded as reflectors. When such reflectors obtain the envelopes typically reflector attack, they might create persistently more packets with the use of a destination address of the victim.A distance-based rate limit mechanism is used by the traffic control component for dropping attack traffic at the source end. Instead of penalizing each router at the source end equally, the mechanism sets up different rate limits for routers based on how aggressively they are forwarding attack traffic to the victim. Therefore, a history of the drop rate in each router will affect the calculation of rate limit values in this mechanism. The focus of this paper is to present the distributed distance-based DDoS defense framework and the distance-based attack traffic control mechanism to detect and drop the attack traffic effectively.

2. LITERATURE SURVEY

In [2-3], Y. Kim et al. propose a path signature (PS)- based victim-end defense system. The system requires all routers to flip selected bits in the IP identification field for all incoming packets. Based on these marking bits, a unique PS can be generated for all packets from the same location. At the victim end, the defense system separates traffic based on PS of each packet and detects DDoS attacks by monitoring anomalous changes of traffic amount from a PS. Then, a rate limit value will be set up on this traffic. However, it is hard to detect DDoS attacks if PS diversity is much greater than real router diversity of incoming traffic. Moreover, it is possible that a PS has been changed after an attack has been detected. For this situation, collateral damage for the legitimate traffic cannot be avoided.

S.Saurabh and SaiRam[1] proposed packet marking and IP traceback mechanism called Linear Packet Marking which needs wide range of packets almost add up to range of hops traversed by the packet. Other IP traceback algorithm requires much high number of packets compared to this algorithm. A lot of them requires packets on the scale of a very large number packets. Yet as this scheme is able to do IP traceback using quite a few packets, it can be highly scalable i.e. it might work for highly DDoS attack involving a very large number attackers distributed across network. Secondly it may well be applied to low rate DoS attacks which could perform attack with very less range of packets. This framework is able to be incorporated by other traceback algorithms to scale back the volume of packets required for path reconstruction that may improve their performance too.

ADVANTAGES:

- With the recent increase e-crime using DoS/DDoS attacks, victims and security authorities need IP traceback mechanism that could trace back the attack to its source.
- This scheme requires a small number of packets hence it is capable of doing very well in situations of large scale DDoS attacks and in low rate DoS attacks.
- This procedure requires the attack to remain alive while performing traceback

DISADVANTAGES:

- IP traceback itself causes DoS attack while performing traceback.This method will not handle packets headers of IPV6 but generated extra traffic for traceback.
- It entails wide range of hard drive storage and hardware changes for packet logging due to which it is not really practically deployable.
- Unfortunately current proposals for IP traceback mechanism has problems with various drawbacks like need for thousands of packets for performing traceback and the in-ability to handle highly distributed and scaled DDoS attacks.

The overlay-based distributed defense framework [4] detects attacks at victim end. During source finding, the traceback technique SPIE (Source Path Isolation Engine) is used. To control attack traffic at the source end, it combines the history of a flow into rate limit calculation by defining a reputation argument. A spoofing DDoS attack can make the flow-based rate limit algorithm ineffective.

Ninglu and Yulongwang [2] proposed as Tracing the paths of IP packets returning to their origins, known as IP traceback is a crucial step up defending against Denial of Service (DoS) attacks employing IP spoofing. In log-based single-packet IP traceback, the path information is logged at routers. Packets are recorded through routers toward the path toward the destination.

DDoS attack occurs by a lot of zombie PCs. Zombie PCs are distributed all over the world. Therefore, when an attack occurs, then the attack traffic is transmitted via backbone network of the target system's country. So, if backbone network is monitored and analyzed, DDoS attack would be detected earlier than current DDoS prevention systems. It can make damages be minimized and also effective to prevent IP spoofed attack packets. For this, attack detection and prevention system has to offer more than tens of Gbps performance.

Probabilistic Packet Marking:[3] It can be defined to be the most famous packet identification techniques. In these particular methods, the packets are marked with the router's Internet protocol address which actually they traversed or the trail edges from which the packet is being transmitted. Marking the packets when using the router's address is the very best approach when compared onto the two alternatives provided here, where if a packet dissipates of affected with any attack, the source router address can be fetched and send back to the actual router. Now the router checks the packets and retransmits the packet towards the actual destination. Using this implementation, an accuracy of 95% is possible to actually see the actual attack path. Second approach considered in probabilistic bundle marking is edge marking and here the IP address of two nodes will be needed to mark the packets. This approach definitely is much complicated compared to marking the IP address of a given router, where much state information of a given packet is required inside the former case. There are few techniques to reduce the state detail required in this case plus they are also discussed here. A basic XOR operation can be executed between them nodes which typically make up the edge.

In order to react effectively against DDoS attack, all the processes for information gathering, analysis and defense rule generation have to be automated. Furthermore, based on these analysis results attack detection and prevention processes also have to be automated. The IDDI is located in the center of whole network. In this position, lots of information could be gathered, so with the information zombie PCs, C&C servers and agent distribution systems also have to be detected. Beyond current visualization tools, it has to be able to show the network traffic and security status in real-time. IDDI also can give direct information about security environment to administrator.

ADVANTAGES:

- A single-packet traceback approach in accordance to routing path.
- The main design goal is to conserve the single-packet traceability and, at the same time, reduces the storage overhead and minimizes the total number of routers that must be queried during the traceback process.

DISADVANTAGES:

- Bandwidth overhead is amazingly high while tracing the attack origin.
- may not trace the attack while it is over i.e attack should remain active until such time as the trace is completed.

Vijayalakshmi M and Mercyshaline [3] proposed as DDoS attacks have been carried out along at the network layer, for instance ICMP flooding, SYN flooding and UDP flooding that happen to be called Network Layer DDoS attacks. The proposed Filtering technique performs filtering close to the way to obtain the attack driven by information filed by the injured individual. This is complemented by the proactive traffic shaping mechanism to stop network overload before detection happens in the victim. This method detects flooding network attacks, flooding and non flooding application layer attacks.

ADVANTAGES:

- This method greatly reduces the magnitude of the attack traffic and improves the probability of survival regarding a legitimate flow.
- Quite simple to trace ip source address. Very easy to trace router's path
- .Simple checksum is made use of instead of hash function calculations which decrease the time and byte consumption of IP header fields.

DISADVANTAGES:

- Doesn't detect other type of attacks except dos.
- Overhead while recording packets in network and make use of layers.
- Found medium number of false positive outcomes.

Okada M,Katsuno[4] Y Proposed as , the large collection of packets that considers the autonomous system (AS) level of the world wide web topology distribution is calculated. The attack path tracing time is assumed to remain an index based on the expected wide range of collection packets, and the best marking probability is presumed. For estimating best marking probability, PPM (Probabilistic Packet marking)method uses only Identification field of IP header The strategy is constructed according to the following considerations.
a. The tactic fails to influence other communications.
b. The method is as efficient as possible.

ADVANTAGES:

- Compatible with existing protocols Support for incremental implementation
- Allows post packet analysis
- Insignificant network traffic overhead
- Compatible with existing routers and network infrastructure.

DISADVANTAGES:

- Resource incentive in regards to processing and storage requirements.
- Sharing of logging information among several ISPs gets to logistic and legal issues.
- Less Suitable for distributed denial of Service attacks

Khan z and Akram N[5] proposed as a new IP traceback technique. This new IP traceback technique will work on single packet IP traceback. Single packet IP traceback means it requires only one packet to start the traceback procedure. Secondly it eliminates the need of any marking technique. Proposed work designed a marking technique in which a 16 bit ID is allocated to each ISP. As soon as ISP receives a packet from any attached end user it adds its 16 bit ID to the identification field of IP header. Since the size of the ISP ID and IP identification field is same so we don't need any other efficient packet marking technique. 16 bits are embedded into 16 bit field.

ADVANTAGES:

- It is easy to implement
- It has low processing and no bandwidth overhead
- It is suitable for a variety of attacks [not just (D) DoS
- It does not have inherent security flaws.

DISADVANTAGES:

- Since every router marks packets probabilistically , some packets will leave the router without being marked
- It is too expensive to implement this scheme in terms of memory overhead
- One important assumption for PPM to work is that DOS attack traffic will have larger volume than normal traffic.

CONCLUSIONS AND FUTURE SCOPE

In this paper existing approaches and its drawbacks are identified and analyzed. An advantage of implementation without structural change of the existing network by eliminating the existing IP traceback system's disadvantage of implementation difficulty on internet environment Also, the high expanding features by using the agent have a potential of being implemented on large size network in the future.

In conclusion, the active security system utilizing IP traceback technology could be contributed for safer and better reliable internet environment by effectively protecting the intentional internet hacking. In future realtime ip traceback mechanism is developed and identified within the network.

REFERENCES:

[1]. Saurabh S, SaiRam A.S Linear and Remainder Packet Marking for fast IP Traceback COSMNET, fourth international journal 2012.

[2]. NingLu;Yulong wang a novel approach for single packet ip traceback based on routing path parallel and distributed systems 20 international conference 2012.

[3]. Mercy Shaline and Vijayalakshmi M IP traceback system for network and application layer attacks Recent trends in Information Technology, 2012.

[4]. Okada M, Katsuno Y 32-BIT as number based ip traceback (IMIS) 2011 fifth International conference.

[5]. Khan ,Z.S;Akram N; secure single packet ip traceback mechanism to identify the source (ICITST)2010