International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2494-9150 Vol-02, Issue 02, MAY 2016.

Packet Marking Based on Trace back Mechanism

[1]Prof. Anil V Turukmane, [2]Prof. Soniya N Madavi

[1,2]Assistant Professor, [1,2]P E S College of Engineering Aurangabad, Maharashtra, India.

[1]anilturukmane@gmail.com, [2]madavisoniya89@gmail.com

Abstract - The denial-of-service (DoS) attack has been a pressing problem in recent years. DoS defiance research has blossomed into one of the main streams in network security. Various techniques such as the pushback message, ICMP trace back, and the packet filtering techniques are the results from this active field of research. The probabilistic packet marking (PPM) algorithm attracted the most attention in contributing the idea of IP trace back. The most interesting point of this IP trace back approach is that it allows routers to encode certain information on the attack packets based on a predetermined probability. Upon receiving a sufficient number of marked packets, the victim (or a data collection node) can construct the set of paths that the attack packets traversed and, hence, the victim can obtain the locations of the attackers.

Keywords – Packet Filtering; Traffic Control; IP Trace back; DDoS Attack, Deterministic Flow Marking.

I. INTRODUCTION

The world has seen rapid advances in science and technology in the last two decades, which has enabled dealing with a wide spectrum of human needs effectively. These needs vary from simple day-to-day needs like paying electricity bills, booking train tickets, etc., to sophisticated needs like power grids for power generation and sharing. These technologies have taken human life into much higher levels of sophistication and ease. But in the middle of this phenomenon, the rise and growth of a parallel technology is startling – that of compromising security, thereby resulting in different effects detrimental to the use of technology. This includes attacks on information, such as stealing of private information, hacking, and outage of services. Media and other forms of network security literature report the possibility of the existence of underground anonymous attack networks which can effectively attack any given tar-get at any time. This only shows a possible shift in attack perspective in current days and in times to come – from wars causing physical damage and destruction to what is termed "information warfare", compromising of attacks mentioned above. The twist in the latter is that these attacks are mostly performed by attackers/networks who can conceal themselves.

While the range of attacks that can be performed on targets is as broad as the spectrum of constructive technology itself, this thesis deals with a particular class of attacks known as Denial of Service (DoS) attacks. Denial of Service (DoS) attacks are a class of attacks on targets, which aims at exhausting target resources, thereby denying service to valid users. The target resources could be in terms of space and/or time. For example, servers providing SSL service could be time-attacked by making them perform a lot of expensive cryptographic operations (public key decryption in this case) thereby preventing them from serving their genuine clients. Alternately, servers could also be space-attacked by exhausting their bandwidth or connection buffers with lot of bogus packets/requests.

1.1 Denial-of-Service Attacks

This dissertation studies denial of service (DoS) attacks in computer networks. The goal of these attacks is to prevent availability of network services from their legitimate users. This dissertation presents a structured view on possible attack and defense mechanisms, describes some new defense mechanisms, and provides new information on selecting and evaluating defense mechanisms. Defending against DoS attacks is network and computer security. As scientific disciplines, network and computer security are relatively new. Computer and network security were first studied in the early 1970s. There are many different types of DoS attacks and the number of them only increases with the release of newer protocols and network applications. In order to gain a better understanding of the most common DoS attacks, it is best to separate these attacks into two different categories: local and remote (or network based). These attacks can be further separated into two more subcategories that describe the overall goal of the attack: stopping critical services and exhausting system resources [3].

II. RELATED WORK

Providing networks with countermeasures against Denial of Service (DoS) attacks has become a pressing security issue in the Internet today. Network services get disrupted or become totally unavailable as malicious attackers flood a victim network with large amount of useless traffic. For accountability purpose and to thwart those attacks, it is essential to identify the source of these attacks, which is usually concealed using faked or spoofed IP addresses, and is known as the IP Traceback problem.

Packet marking is a traceback approach that calls for routers to mark packets along the attack path with self-identifying information. In Probabilistic Packet Marking (PPM) routers probabilistically decide whether or not to mark packets. A victim node relies on the amount of marked packet samples received to reconstruct the attack path. However, a fixed marking probability set for all routers in PPM has proved to be ineffective as marked packets from distant routers are more likely to be remarked by downstream routers. This entails a loss of information and leads to increase in the volume of packets needed to reconstruct the attack path. Enabling each router to adjust its marking probability so as to obtain equal samples of marked packets, in particular from the furthest routers would help in minimizing the time taken to reconstruct the attack path.

Dynamic schemes have been proposed for adjusting the marking probability, which can be derived by accurately estimating a router's position in the attack path. However, most schemes are highly dependent on the underlying protocols and require routers to have knowledge of distance information to the potential victim node. This adversely increases the router overhead and is time consuming for real-time packet marking scenarios.

In this work we propose an algorithm that dynamically set the value of the marking probability based on the 8-bit Time-To-Live (TTL) field in the IP header, which is a value that can be directly accessed by routers without external support. Our proposed scheme utilizes the variable TTL value as an estimate of the distance traveled by a packet and thereby its position in the attack path to derive the marking probability value. Our algorithm was simulated with a number of test cases using a user-friendly simulator that was developed to that effect. Results in terms of false positives, reconstruction time and number of packets needed for reconstruction have shown the efficacy of our dynamic scheme, which offers significantly higher precision with fewer overheads both at the router and at the victim in reconstructing the attack path. The main advantages of the proposed scheme reside both in its simplicity and low router overhead while offering comparable results with other dynamic schemes and outperforming static schemes at large attack distances.

Future work includes fine-tuning the derivation of the dynamic marking probability to further improve performance at larger attack distances and a study of its applicability and performance in IPv6 networks.

III. THE PROPOSED DEFENSE SYSTEM

One of the major open problems in network security today is Distributed Denial of Service (DDoS) Attacks. In a DDoS attack, the attacker sends vast amounts of traffic from a large number of systems that are controlled by him/her to a victim network or system. The result is that the victim's resources become overloaded and it cannot process the requests of legitimate users, thus any services that this system provides become unusable. One of the main difficulties in the detection, and prevention of DDoS attacks is that the incoming packets cannot be traced back to the source of the attack, because (typically) they contain invalid or spoofed source IP address. For that reason, a victim system cannot determine whether an incoming packet is part of a DDoS attack or belongs to a legitimate user. DDoS attack is a major source of Cyber-attack [1]. The attacker tries to hide its identification by spoofing the IP Address. Current IP traceback mechanisms can be mainly classified into four categories [2]. These are packet marking, Debugging, Link Testing and Messaging. Packet marking mechanisms mark the identification of the routers in the IP packets. Marking mechanism such as Probabilistic Packet Marking Mechanism (PPM) and Deterministic Packet Marking (DPM) mechanism rely on packet marking for identification of attackers. In PPM, all routers mark the packet using some probability. The victim reconstructs the path back to the source using the bit encoding by each routers. PPM mechanism can also uses TTL value in the packet to identify the source of malicious packets. DPM marks the packet with fixed probability. It uses the identification of ingress routers while marking the packets. SIT (Speedy IP traceback).uses MAC address for marking in the IP packet [3]. This is based on the assumption that the MAC address may not be spoofed by the user since it changes from one hop to other. So, MAC address of source is marked in the packet which can later easily traced. But, MAC address copying is violation of privacy. It is also subject to spoofing.

One marking mechanism uses checksum to encode the IP Address and Traffic filtering mechanism at ingress router to drop the spoof packets at ingress interface [4].

Link testing methods include input debugging [5] and controlled flooding methods [6]. The main idea is to start from the victim to locate the attacker from upstream links by testing the possible routes and then finding the attack path. This technique has limitations when there are branching in the network as it increases the overloading of the network. When the Network Traffic is quite heavy, this technique is not

Feasible to use. If the victim is receiving significant attack traffic, then this technique is less effective.

Another traceback technique is Messaging. Bellovin [7] proposed ICMP messages to traceback the source of attacker. ICMP messages are sent to find the source of forged packets. But, the limitation of this technique is that generally routers do not allow to exchange of ICMP messages. Also, when the network traffic is very high, this generates additional traffic.

3.1.1 Basic assumptions

The assumptions that will be used in this paper are largely borrowed from [7] and are the following:

- The attacker may generate any packet
- The attacker knows that he is being traced
- The attacker knows the traceback scheme
- Routing is stable most of the time
- Routers are not compromised
- Routers are both CPU and memory limited

The first three assumptions mean that the proposed marking scheme cannot contain any weaknesses that could be exploited by the attacker. The attacker can craft any kind of packet, even packets that bear such markings that could circumvent traceback or filtering of his/her packets. The fourth assumption dictates that we expect most of the packets from a specific source that have the same destination, to follow the same path. Efficiency of this marking scheme can be degraded if the assumption is not true, but success of the scheme is not compromised.

IV. CONCLUSION

In this work, have implemented and evaluated the proposed system most interesting point of this IP trace back approach is that it allows routers to encode certain information on the attack packets based on a predetermined probability. Upon receiving a sufficient number of marked packets, the victim (or a data collection node) can construct the set of paths that the attack packets traversed and, hence, the victim can obtain the locations of the attackers.

REFERENCES

[1] A. Yaar, A. Perrig and D. Song "SIFF: a stateless Internet flow filter to mitigate DDoS flooding attacks", IEEE Symp. Security and Privacy, Berkeley, pp. 130–143, May 2004.

[2] Y. Chen, S. Das, P. Dhar, A. El Saddik and A. Nayak, "Detecting and preventing IP-spoofed distributed DoS attacks" International Journal of Network Security, vol. 7, no. 1, pp. 69–80, July 2008.

[3] M.S. Fallah and N. Kahani, "TDPF: a traceback-based distributed packet filter to mitigate spoofed DDoS attacks", Security and communication networks, Wiley Online Library, DOI: 10.1002/sec.725, Feb. 2013.

[4] R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network", Technical report, ACIRI and AT&T Labs Research, Feb. 2001.

[5] Snort network intrusion prevention and detection system, Accessed 28 October 2013,

[6] Internet Control Message Protocol, Accessed 28 October 2013, http://en.wikipedia.org/wiki/Internet_Control_Message_ Protocol/

[7] The CAIDA "DDoS Attack 2007" Data set, Accessed 28 October 2013,.

[8] The CAIDA Anonymized Internet Traces 2012 Data set, Accessed 28 October 2013, http://www.caida.org/data/passive/passive_2012_dataset.xml/

