IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. V (Nov – Dec. 2014), PP 25-28
www.iosrjournals.org

"An efficient IP trace back using packetizing logging and pre shared key exchange"

Narendra Pradhan, Rajesh Kumar Sahu, Kamlesh kumar pandey.
Computer Science, S.S.College of Education Pendra Road/Bilaspur University, India
Computer Science, S.S.College Of Education Pendra Road/Bilaspur University, India
Computer science, MCRPV, Amarkantak Campus, India.

Abstract: *Here in this work we presented a hybrid model of packet marking and logging for the IP trace back for the node that wants to attack any node in the network. The main idea is to detect the DOS attacks in the network by employing the ip of the attacker node. Here we are implementing the packet marking and the logging for the homogenous and the heterogeneous network. Also here we are integrating the concept of pre shared key exchange on the routers to make the marking of the packets is easy and can increase the efficiency of detecting attacks in the network.*

Keywords: *Ip, Packetizing, Shared Key Exchange, Logging, Trace.*

I. Introduction

ATTACKS that use supply address spoofing represent a growing threat to the net infrastructure. Denial of Service (DoS) attacks and additional difficult version called Distributed DoS (DDoS) is that the commonest to require advantage of supply address spoofing. These attacks deny regular web services from being accessed by legitimate users either by blocking service utterly or by distressing it specified users become not curious about the service any longer (for example inflicting important delay in accessing associate airline reservation net site). In such attacks, the most objective is to overpower the victim whereas concealing attacker's identity. Today's web has witnessed many incidents that make sure the devastating impact of such attacks [1].

In order to defend web against DoS intrusion, an efficient method is to find the supply and eliminate the attack going down. Sadly, attributable to the anonymous access and non-state characteristics of web, there's no record regarding the transmission path of packets. Therefore, we tend to cannot get the packet supply simple from the supply address of the packet dependably.

In current cyber intrusion, Denial of Service and a few later forms become one in all the foremost threatening varieties. It absolutely was reported that (D)DoS traffic within the web increase variety of times in eight years from many many Mega-bytes in 2002 to a hundred Giga-bytes in 2010, in 2010 Worldwide Infrastructure Security Report, from Arbor Networks. many celebrated web firms, together with Yahoo, Amazon and CNN were brought down for hours [2].

The main idea behind packet logging is that routers record the state information of their forwarding packets locally. When the victim node suffers from intrusion, it can query the log-tables recorded in the routers and makes matching with the attack packet. In the recursive process, we can obtain the complete path in the end. The most representative method is SPIE (Source Path Isolation Engine). The two types have their own features: PPM incurs little overhead when routers mark packets in a low marking rate, but the victim needs a large number of packets to reconstruct the path to the source. It is more suitable for flooding DoS trace back, and does not have the capability to trace a single packet. While SPIE extracts the digests of packets and stores them in a space-efficient data structures known as bloom filter, which decreases the storage overhead and makes the packet logging scheme practical. It can trace small packets flows, even a single packet. However, it is still a challenging task for its practicality due to its remaining high storage overhead. Therefore, it is attractive to propose an effective IP trace back mechanism with the combination of the two trace back techniques, which is called a hybrid IP Trace back scheme [3].

1.1 Hybrid Internet Trace back

At present, HIT proposed by Gong Chao is the most representative. HIT borrows the main idea of packet logging, and records packet digests in every other router. The marking routers do not record digests, but write their ID information into some certain fields of IP header. It is efficient to reduce the huge storage overhead of SPIE. However, there are some drawbacks of HIT. Firstly, it may return incorrect path even the false source; then it still has a great demand for storage, which would limits its practicality [4].

1.2 Packet Logging Scheme

Introduced an idea to record packet state information in a router log, so as to reconstruct the attack path and get the attack source. This method can trace not only the flooding attack with a large number of packets, but also the single packet attack. It was thought to be impractical for its huge storage requirement. In order to reduce the storage overhead of log-based technology, log information needs a space-efficient manner. SPIE is proposed with the packet logging idea, so it has the ability to trace a single packet. In SPIE, routers do not store the whole packet, but the digest with bloom filter, which is famous for its space-efficiency. In this way, the condition of storage requirement has been greatly improved (down to 0.5% of the total link capacity per unit time) [5].

1.3 Packet Marking Scheme

Unlike packet logging scheme, in packet marking scheme, routers do not record packets digests, but write their ID information into IP header. When the victim gets sufficient packets, it can reconstruct the full attack path. Savage et al. proposed the classic probabilistic packet marking (PPM) method. PPM makes use of the Identification field as the marking space and stores the link information. It divides the IP address into eight fragments, 4 bits for each. This IP address fragment and the same offset fragment of the next router compose the edge fragment with 8 bits. The offset flag needs 3 bits for eight fragments, and the last 5 bits are enough to show the hop number. It is reported that few packets exceed 25 hops in the forwarding network when a router decides to mark a packet, it chooses a random fragment of its IP address, and records the fragment offset with the distance field set to 0. The advantage of PPM is that it needs no storage overhead for each router. But the drawbacks are also apparent. Victim needs a large number of packets to reconstruct the attack path, and PPM does not have the ability to trace a single packet [6].

1.4 Probabilistic Packet Marking Schemes

Probabilistic Packet Marking (PPM) is one stream of the packet marking methods. The assumption of PPM is that packets are much more frequent than the normal packets. It marks the packets with path information in a probabilistic manner and enables the victim to reconstruct the attack path by using the marked packets. PPM encodes the information in rarely used 16-bit Fragment ID field in the IP header. To reduce the data that is to be stored in 16 bits, the compressed edge fragment sampling algorithm is used. Although PPM is simple and can support incremental deployment, it has many shortcomings that can seriously prevent it from being widely used.

1.5 Deterministic Packet Marking Schemes

Another stream of packet marking methods, which does not use the above probabilistic assumption and stores the source address in the marking field, is in the category known as the deterministic approaches, such as Deterministic Packet Marking (DPM).The DPM scheme was modified to reduce false positive rates by adding redundant information into the marking fields. Unlike PPM, deterministic approaches only keep the first ingress edge router's information in the marks (but not the whole path). Moreover, they record marks in a deterministic manner (but not a probabilistic manner as in PPM).

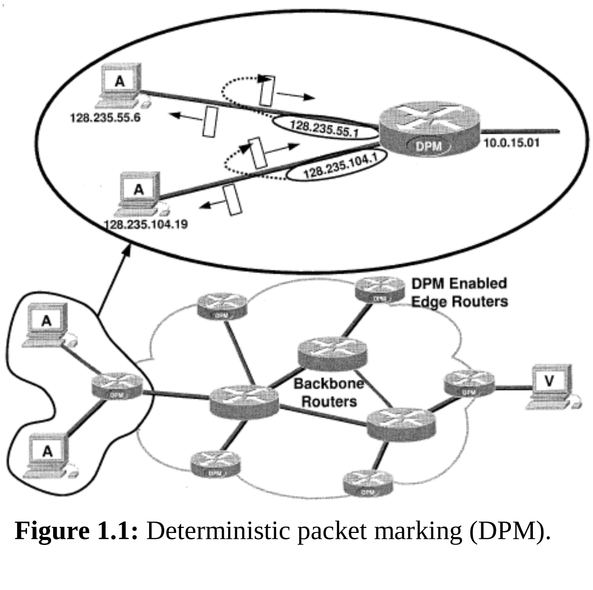

Figure 1.1: Deterministic packet marking (DPM).

II. Background And Motivation

2.1 Attack Trace back Problem

Let Ri1, Ri2,….,Rin be the ordered list of routers between attacker (Ai) and victim (V). This ordered list of routers defines the attack path for Ai. We call each of these routers involved in forwarding malformed packets to the victim, as an Attack Router. For any attack router Rij in the list, all routers between Rij and the victim are called the Predecessor List of Rij, while all routers between the attacker and Rij are called Successor List of Rij. The main objective of attack trace back problem is to identify the attack router connected directly to Ai (i.e., router Ri1 which has an empty successor list). In our view, this is equivalent to identifying the end point of a link list starting at the victim, where each element in the list represents an intermediate router along the path from victim to attacker as Multiple attackers' case corresponds to a tree of link lists rooted at the victim (V), where each leaf represents a link list end point.

The main assumptions made in our work are similar to those made in and with an exception that we do not necessarily assume that each attack source has to send numerous packets [7].

The imminent threats imposed by DoS attacks call for efficient and fast trace back schemes that enjoy the following features:

1. Providing accurate information about routers near the attack source rather than those near the victim.
2. Recognition and exclusion of false information injected by the attacker.
3. Avoiding the use of large amount of attack packets to construct the attack path or attack tree.
4. Low processing and storage overhead at intermediate routers.
5. Efficient collection of marking information stored at intermediate routers (if any).

III. Related Work

In 2006 by Al-Duwairi,, and G. Manimaran gives the concept about Tracing DoS attacks that make use of source address spoofing is an important and challenging problem and there are different scheme used ,The first scheme, called Distributed Link-List Trackback (DLLT), and for propagating marking The second scheme, called Probabilistic Pipelined Packet Marking (PPPM), use the concept of a "pipeline" for propagating marking information and at the destination end small amount of resources to be allocated at intermediate routers for packet logging purposes [1].

In 2012 by Dong Yan, Yulong Wang, Sen Su And Fangchun Yang"in the field of Packet Marking and Logging "Tracing malicious packets back to their source is important to defend the Internet. There are two major kinds of IP trace back techniques, which have been proposed as packet marking and packet logging. In packet marking, it incurs little transparency. In packet logging, its needed storage space to record packet digests information and his capability to trace even a single packet. Therefore, it is a new idea to draw on both advantages to obtain the intrusion source and propose a precise IP trace back approach with low storage overhead, which improves accuracy and practicality greatly. [4].

In the field of Packet Marking R. Sravani, and J. Swami Naik in 2011 present a practical IP trackback system called Flexible Deterministic Packet Marking (FDPM) which provides a defense system with the ability to find out the real sources of attacking packets and finally In case of FDPM, the marks in packets do not increase their size; therefore, no additional bandwidth is consumed and overload prevention capability, FDPM can maintain the trackback process when the router is heavily loaded, whereas most current trackback schemes do not have this overload prevention capability [9].

In 2012 by Shih-Hao Peng et. All introduce A Probabilistic Packet Marking scheme and propose the LT Code IP Trace back scheme to reconstruct the attack graph and find the source of attacker and finally LTCIP is a reliable IP Trace back scheme, which can find the source of DDoS and avoid the attack [10].

Introduce an efficient Ip trace back in packet marking algo. In 2010 by Y.Bhavani and P.Niranjan Reddy propose a technique that efficiently encodes the packets than the Savage probabilistic packet marking algorithm and reconstruction of the attack graph and To conclude, our Efficient Probabilistic Packet Marking is an effective means of improving the reliability of original probabilistic packet marking [11].

Jeevaa Katiravan, C. Chellappan, and N. Duraipandian, in 2011 introduce the It Security concept there are different types of cyber-crime is major threat such as surrounding hacking, copyright infringement etc. and also problems of privacy when confidential information is lost or intercepted,

So here over comes this problem by using a pre shared key mechanism. This solution proves that even though attacker node changes its IP address but it can't change the pre shared key exchanged between it and egress router which is used for authentication [12].

References

[1]. Al-Duwairi,, and G. Manimaran,**"** Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback Bashee "IEEE. Volume 17, Issue 5, May 2006, Pages: 403 - 418.

[2]. Arbor Networks Inc., "2010 worldwide infrastructure security report," [EB/OL], http: //www.arbornetworks.com/report.

[3]. C. Gong and K. Sarac, "A more practical approach for single-packet IP trace back using packet logging and marking," IEEE Transactions on Parallel and Distributed Systems, Vol. 19 , pp. 1310-1324, 2008.

[4]. Dong yan, yulong wang, sen su and fangchun yang. "A Precise and Practical IP Trace back Technique based on packet marking and logging", published journal of information science and engineering 28, 453-470, 2012.

[5]. A. Snoeren, et al., "Single-packet IP trace back," IEEE/ACM Transactions on Networking, Vol. 10, pp. 721-734, 2002.

[6]. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP trace back," IEEE/ACM Transactions on Networking, Vol. 9,pp. 226-237. 2001

[7]. D. Song and A. Perrig, "Advanced and authenticated marking schemes for IP trace back," in Proc. of IEEE INFOCOMM 2001, April 2001.

[8]. Dong Yan, Yulong Wang, Sen Su And Fangchun Yang "A Precise and Practical IP Traceback Technique Based on Packet Marking and Logging", Journal Of Information Science And Engineering 28, 453-470 ,2012.

[9]. R. Sravani, J. Swami Naik "A Study on Flexible Deterministic Packet Marking: An IP Traceback System" Vol No. 9, Issue No. 1, 001 – 007, ISSN: 2230-7818, 2011.

[10]. Shih-Hao Peng, Kai-Di Chang, Jiann-Liang Chen, I-Long Lin, and Han-Chieh Chao "A Probabilistic Packet Marking scheme with LT Code for IP Traceback", International Journal of Future Computer and Communication, Vol. 1, No. 1, June 2012.

[11]. Y.Bhavani, P.Niranjan Reddy."An Efficient IP Traceback Through Packet Marking Algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010.

[12]. Jeevaa Katiravan, C. Chellappan, N. Duraipandian," Improved IP Trace Back Using Pre-Shared Key Authentication Mechanism**"** European Journal of Scientific Research ISSN 1450-216X Vol.50 No.1 , pp.99-109, 2011.