The Improvement Scheme Based on SIPT

Jieying LAO
ZJUT Information Manger,
Zhejiang University of Technology,
Hangzhou, China
ljy@zjut.edu.cn

Zhilei SUN
ZJUT Information Manger,
Zhejiang University of Technology,
Hangzhou, China
szl@zjut.edu.cn

***Abstract*—Speedy IP Traceback method (SIPT) is deficient in monitoring and position attack sources, this paper puts forward an improvement scheme based on SIPT, it only marks two-three times for the packet on the key locations, and the propose also overload rarely used fields on IP packet header to store the checkpoint information, which can traceback the attack source use these marking information, which would help to attack path-reconstruction with a low false-positive rate as a guid.**

Keywords- Dos attack; attack source; path-reconstruction

I. INTRODUCTION

Vaarun Vijairaghavan etc proposes a Speedy IP Traceback method[1], this method is mainly trackback toward to the Dos attacker origin and protects the Legitimate hosts, its principle is that the client host sends data to others, first the packets traverse to the gateway router ,then the gateway router can get the communication source host of Mac address, gateway router will convert the 48 bit Mac address of the source host and the 32 bit the IP address of its own IP address into 16 bit by the efficient Hash making technique, and then insert 16 bit data to the packet header as a identification, which used as identification information to track back the attacker origin. After marked, the gateway router route the packet out; the intermediate router does nothing to the packet except route it normally.

SIPT method deploys the intrusion detection system server in the network environment of the key position, when the server detects the Dos attack happened, the server would capture the packets for analysis, and extracts the identification from the IP packets header, uses hash-table technique[2] to count the packets which from the same host. After a certain period of time, the server can maintain the number of packets from the same host.

We can use the records to know which host sends the big abnormal data flows, then the Dos attacker can be founded by using the identification information which includes the Mac address of the attacker host, because the Mac have been storied in the gateway router's MAC address table , use this method to trackback the Dos attacker origin and protect the Legitimate hosts.

SIPT method uses the making technique to mark the packet , converts the information of the communication source host of Mac address and the IP address of the gateway to the identification, and inserts the identification to the packets' header.

According to the identification information, the administrator can quickly position the source communication host by one packet ， but this method exists deficiencies: SIPT only can be used for attackers who send the anomalously large data flows, and the other situations will be hard to identify attackers, because the threshold of packet number is not easy to set. If the server capture the all data flows to analysis, that needs huge amounts of storage space, so this method is not easy to implement in reality, and the huge packets information does increase the administrators' work.

II. INTRODUCE THE IMPROVEMENT SCHEME BASED ON SIPT

The SIPT method needs the network manager involved in the work in personally, and judges the Dos attackers by the record of the number of packets from the same host, which stored in hash, and The SIPT is implemented only in small network area to monitor the Dos attack, because this method is need to use a large capacity of memory to handle and store packets' header In the large-scale network environment. This method would not work in the small data flow network environment .In order to make up the deficiency of the SIPT, this paper improves the algorithm, The boundary router marks the packets which traverse many times, and inserts the identification into the packets' header, when network attack happened, it can use the header information to trace back the attacker origin.

A. The improvement of SIPT based on autonomous system (AS) level

The current existing attack source tracking technology can be divided into two parts: attack-path reconstruction in inter-domain and intra-domain. The attack-path reconstruction in intra-domain(AS)level is superior to inter-domain for the current network environment, according to statistics[3] ,A topology distribution is shown in Figure 1, the AS could reach the others about 99% by 1-8 hop, this is far less than the number of hop on inter-domain level, but the attack-path reconstruction in AS level has the great challenge: when the packet reached its destination, the victim can't judge the packets from which AS in the network environment , although the

Published by Atlantis Press, Paris, France.

packet has its own IP address. When network attacks happen, accurate, quickly positioning to AS which traversed the attack packets, is the key for attack-path reconstruction on AS level.

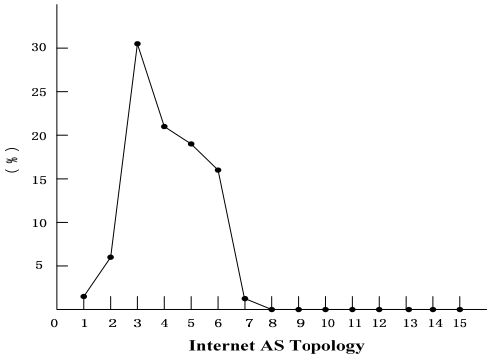

Fig 1 Internet AS Topology

In the current network environment, most ASes are located at the network edge relative to the core network. Generally, host in the client AS send the packet to others, first the packets traverse to the core AS, and after a series route toward to destination.

The improvement method this paper proposed, needs to use Border Gateway Protocol (BGP, Border Gateway Protocol) as a vehicle to distribute the deployment information, such as the ASes' Location information. ASes can communicate with each other with Border Gateway Protocol. By Using BGP Protocol, we can trace back to the AS which attacker belong to, and then use the improvement of SIPT method to locate the attacker.

B. The improvement scheme based on SIPT of marking technology

SIPT method of the marking technology inserts the attacker identification information in IP packet header, the improvement scheme based on SIPT still uses this packet-marking technique, uses IP header of unused fields, such as identification, flag and Fragment offset. According to the literature[4] shown that in the current network environment, the packet is divided into fragment probability less than 0.25%. In addition, the IP optional field also is rarely used. In this improvement of SIPT method, using IP header fields which does not often use to Store marking information, we rewrite the field of 16-bit ID field named HSIPT, 3 12-bit subfields named HAS1, HAS2 and HASC, 2 4-bit HD1, HDC to store AS length information. In addition, still need 1-bit field as a Flag to judge whether the packet traverses the core AS.

C. *The process of packet marking*

When the packets traverse to the Special router, the router uses the packet-marking techniques, the marking information as a checkpoint to help the reconstruct the attack path. The specific marking process is as follows:

(1) When the client host sends the packet to the others, the packet traverses to the gateway router firstly(the client connected to gateway router directly), the gateway router would know the client Mac address and its own IP address, once we know both, we can trace back the attacker. Before the marking, the gateway router needs to judge the income packet which is whether come from the client host or directly connected to itself, if it was, the gateway router inserts marking information into the IP header; if not route the packet normally. The marking information is data link connection that includes the client's Mac address and the gateway router's IP address, the router converts the data link connection into 16-bit marking information.

(2) When the marked packet leaves local AS, routes forward to the core AS directly, the boundary router in core AS will mark the packet second times. First, the boundary router converts the packet's local AS's number into 12-bit identification information, inserts this identification into HAS1field, inserts the core AS's number into HASC, obtains the distance between the core AS and packet's local AS based on BGP Protocol, inserts the distance into HDC, and sets the flag to 1.If the marked packet route forward the client AS, not core AS, the boundary router in client AS also marks the packet second times as core AS's, The only difference is that the boundary router in client AS needs to judge the packet whether route forward to the core AS based on the BGP Protocol or not.

a) If necessary, the boundary router obtains the distance between the its own AS and the core AS which the packet will route forward to based on BGP Protocol, and puts the distance into HD1.When the marked packet traverses to the core As, the boundary router marks the packet the third time, inserts the local AS's number into HASC,gets the distance between its own AS and the AS which the packet's destination belong to, inserts the distance into the HDC, and sets the flag to 1;

b) If not, the boundary router gets the distance between its own AS and the AS which the packet's destination belong to based on BGP Protocol, inserts the distance into the HDC, sets the flag to 0,and routes the packet as usual

When the Victim start attack path-reconstruction, according to the value of Flag firstly, known that the packet whether traversed the core AS, and traceback to the AS which the attacker belong to based on the BGP protocol, distance, the AS number, finally uses the SPIT's marking information, such as the gateway router's IP address and the attacker's Mac address to locate the attcker.

III. SIMULATION EXPERIMENT

In order to verify performance of the improvement scheme based on SIPT， we make the corresponding experiment. This method in attack path-reconstruction Performance compared with ASEM algorithms.

Published by Atlantis Press, Paris, France.

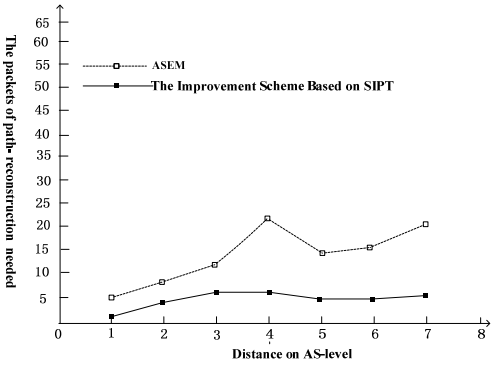

Fig 2 simulated experiment

As shown in Fig 2, the improvement scheme based on SIPT has greater advantages than ASEM[5] in attack path-reconstruction, because the improvement scheme based on SIPT ignores some router-level attack path. The AS-level attack path is far less than the number of routers, so the attack path- reconstruction on AS-level is more efficient.

IV. CONCLUSION

This paper introduces the SIPT method, according to deficiencies of the SIPT method in position attack sources and then puts forward an improvement scheme based on SIPT, redefining the optional field if IP packet header store the checkpoint information, which can traceback the attack source more efficient than other methods.

REFERENCES

[1]Vaarun Vijairaghavan,Darshak Shah,Pallavi Galgali,Amit Shah,Nikhil Shah,Venkatesh Srinivasan,“Marking Technique toIsolate Boundary Router and Attacker”,Computer,vol 2,pp.54-58.Feb 2007.

[2] LAUFER R P,VELLOSO PB,DUAKRTE O C M B.Generalized Bloom Filters[R].Coppe/UFRJ, Tech Rep GTA-05-43,2005.

[3] Masayuki Okada,Yasuharu Katsuno,Akira Kanaoka and Eiji Okamoto,“32-bit AS Number Based IP Traceback”.IEEE Computer Society Washington,DC,USA,pp.628-633,July 2011.

[4] Stefan Savage,David Wetherall,Anna Karlin,Tom Anderson, “Practical network support for IP traceback” ,ACM, Newyork , USA.pp.295-306,2000.

[5] Zhiqiang Gao and Nirwan Ansari,“A practica and robust inter-domain marking scheme for IP traceback”,Computer Networks,vol 3,pp.732-750,2007.

Published by Atlantis Press, Paris, France.