Marker Technique and its Application in the Source Address Recognition Research

Zhu Zhiyu
Network Information Center
Changsha University,
Hunan, China
373211023@qq.com

Duan Huiliang
Network Information Center
Central South University of Forestry and Technology
Hunan, China
105925041@qq.com

***Abstract*—SPi is an end system of validation technique, in which routers mark packets, and end system performs filtering. we construct the simulation with various network topologies to verify the effectiveness and the filtering accuracy of the SVA architecture. The simulation results show that, SVA can respond quickly to the source address forgery attack, and has a better filtration.**

Keywords-source address validation, SPi, SVA

I. Introduction

DoS attacks occur frequently because of the current Internet is designed to forward packets based on destination address, and does not provide any source address authentication mechanism, which for an attacker to fake identities of others offer the possibility of cyber-attacks, it weakens the defense mechanisms on the one hand the detection and filtering of attacks reported capacity, and enhancing the attack damage and increases the difficulty of positioning the source of attacks.

II. Introduction to Marking Mechanism

Tag mechanisms belong to the source address of end system validation techniques. To mark the packets by the router, end system to perform filtering function.

Routers need additional tags you want features to mark each message you receive and forward, to be completed at the end system the following features：

1.Send probe messages to the source message, and based on the reply message to accelerate the path to learn, ability to quickly judge the message source address real address.

2.Direct confidence-building tables based on active learning results. Increases based on probability, imprecision of thresholds of a passive learning, provide support for follow-up to dispose of the message.

III. System Design

SVA（Source Validation Architecture）contains both the source address back-end system validation technologies also include source address validation technology. SVA architecture composed of subsystems and port hosts the common by routers, routers subsystem provides two optional authentication mechanisms, Active SPi and OAuRPF, this article is intended to discuss Active SPi mode.

A Router subsystem key algorithm

The labeling process is divided into two steps: one is to mark the local fill router ID field, the second is the next hop information in advance on the message transfer paths marked in the message. Five functions of the TCP/IP protocol stack defines righteousness, can be achieved through these functions check of the data packets and custom handling operations. The algorithm pseudo code is as follows：

```
    Gets the IP address of the interface tmp=get_dev_ifaddr (in)；
    Gets the number of the interface index=in->ifIndex；
    Judgment message w is in the message is a message
    If w is the message{then   To index as an index table look-up to see if there is a corresponding table entries
    if   There is a corresponding table A[i]
      then
           if tmp = A[i].dev_ip
             A[i].dev_ip_mark fill in the message ID field
           Else
          {A[i].dev_ip_mark = markingbits(tmp)
           A[i].dev_ip_mark fill in the message ID field }
    Endif
Else{
   A[i].index = in->ifindex,A[i].dev_ip =tmp,A[i].dev_ip_mark = markingbits(tmp)
    A[i].dev_ip_mark fill in the message ID field }
                Endif
                }
}
Else
    else{
     To index as an index table look-up to see if there is a corresponding table entries if There is a corresponding table A[i]
    { then   if tmp = A[i].dev_ip
          A[i].next_mark fill in the message ID field
```

© 2012. The authors - Published by Atlantis Press

```
    Else
  {
       published gets its direct-attached router interface IP address next_ipA[i].next_mark = markingbits(next_ip)
A[i].next_mark fill in the message ID field
  }
endif}
       else
       {A[i].index = in->ifindex
       A[i].dev_ip =tmp
         published gets its direct-attached router interface IP address next_ip
       A[i].next_mark = markingbits(next_ip)
         A[i].next_mark fill in the message ID field }
       Endif
}
Endif
```

B Filter the end host subsystem module design and realization

In this prototype system, end system filter function implemented in the kernel, and by building in the kernel TCP request message, proactively validate the legitimacy of the message source. Validation and filtering of messages should be completed before the data packet is submitted to the local application.

IV. Experimental Analysis of Programmes and Results

A Experimental

Tis article mainly for studies of source address spoofing attacks within the domain, so we assume that the current OSPF routing protocols are running on all routers within a domain. Example shown in Figure 1, eth0 connected to the true source of our host, eth1 connected to the destination host, carrying out active authentication and packet filtering features, nod1-2 of their attacker, on which you are running the forged source address message sending programs.

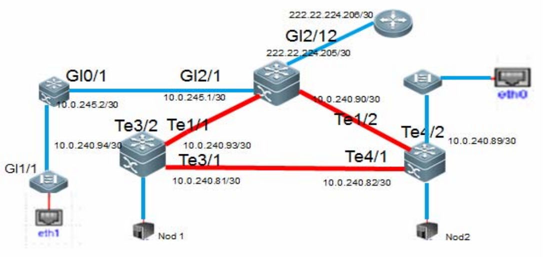

Figure 1 network topology diagram

B Analysis of the results

Throughout the testing process we need to change the router configuration to changing network topology, adjust the tag number and distribution of the router number, location of the attacker and message sending rate, the source host and the attacker, on the effectiveness of Active SPi validate and filter accuracy.

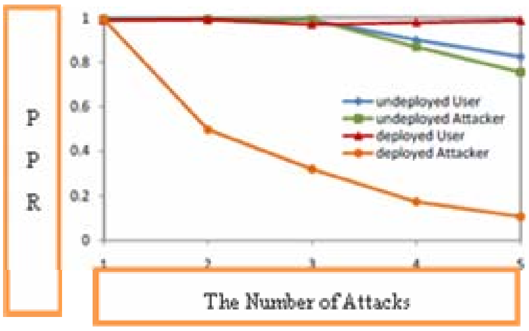

Figure 2 user message 1000pps, attacking message 300pps

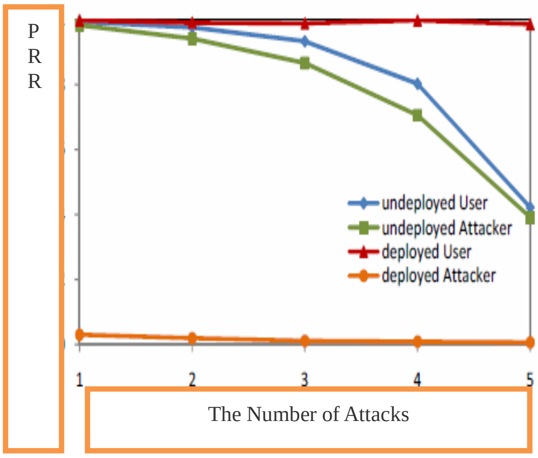

Figure 3 message 1500pps user, attack messages 200/300/500/700/1000pps

By the above test results, as can be seen：

（1）Whenever you deploy an Active SPi, user messages and attack packet receive rates are relatively high, and with the increase in the number of attackers on your network, packet receive rates both declined, probably because of an end system processing power saturation.

（2）After you deploy Active SPi, the user message receive rate has improved, attacking message receive rate declined significantly, with the increase in the number of attackers on your network, a legitimate user packet receive rate change more smooth, and attack packet receive rate the overall rendering of the first rise after declining trend.

We have the following analysis:

(1) After you deploy an Active SPi legitimate user packet receive rate has improved, this is due to Active SPi mechanisms use active learning methods, fundamentally guarantee the legitimacy of the received message. With increase of network attackers, causing congestion in the network, therefore legitimate user packets receive rate decrease.

(2) After you deploy Active SPi mechanism, the attacker packet receive rate after rising curve rendered the overall downward trend. Attacks on the network throughput time, and with the increase in the number of attackers, difficult for reply packets to reach the victims-end system on the source side, victims-end system can identify the current attack traffic, so throw it away.

SUMMARY

Ensure the authenticity of the packet source address. Forged source addresses of the existing defense technology cannot solve real perfect address the problem. But some of these improvements you might close the final objectives of the program.

REFERENCES

[1] Kunihiro Ishiguro. Quagga- A routing software package for TCP/IP networks.http://www.quagga.net

[2] Hal Burch, Bill Cheswick. Mapping the Internet[J]. Computer. 1999, 32(4): 97~98.

[3] Xin Liu, Xiaowei Yang, Yanbin Lu. To filter or to authorize: network-layer DoS defense against multimillion-node botnets [J]. SIGCOMM Comput. Commun.Rev. 2008, 38 (4): 195~206.

[4] Heejo Lee, Minjin Kwon, Geoffrey Hasker, *et al*. BASE: an incrementally deployable mechanism for viable IP spoofing prevention [C]. Singapore: ACM,2007.

[5] Abraham Yaar, Adrian Perrig, Dawn Song. Pi: A Path Identification Mechanism to Defend against DDoS Attacks[C]. 2003.

[6] Wang Haining, Jin Cheng, G. Shin Kang. Defense Against Spoofed IP Traffic Using Hop-Count Filtering[J]. Networking, IEEE/ACM Transactions on. 2007,15(1): 40~53.