Asian Journal of Information Technology 10 (2): 51-54, 2011
ISSN: 1682-3915

Improved IP Trace Back Using Pre-Shared Key Authentication Mechanism

Jeevaa Katiravan and C. Chellappan
Department of Computer Science and Engineering, Anna University, Chennai, India

Abstract: Cyber crime is one of the major threats for IT security. Internet crime refers to criminal exploitation of the internet. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement etc. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. Existing mechanisms use Packet Marking technique to trace back the real source of attacking packets that traverse through the network. But this mechanism fails to provide solution in case of IP SPOOFING and Path failures. In this study, we propose a finest solution to trace back the real source using pre-shared key authentication between egress router and the attacker node.

Key words: IP trace back, DDOS attacks, security, IP spoofing, link failure, egress and ogress routers

INTRODUCTION

As researchers already know the importance of internet in the daily life, the measures that we need to take in order to get rid of security attacks through internet is also getting high. The internet plays a crucial role in keeping communication going, performing as an efficient and stable network for >1 billion users of it. As its user was creeping >1 billion the need to provide security to the data passed over network was also getting increased.

Data sent over the internet is of discrete packets which follows different channels in a sequence over time and rejoins at the final destination node. One of the major threats to the internet is DDOS attacks. It is one of the major cyber attacks currently we are facing. Cyber attacker's main aim is to obstruct the services provided by internet to its legitimate users.

This can be accomplished by exploiting vulnerabilities in network protocols, software and also by exhausting the consumable resources like bandwidth victim memory. With the increase in the internet bandwidth a variety of hacker tools to perform DDOS attacks also increases.

Hence, DDOS attacks are increasing at a rapid pace and becoming more and more vulnerable to IT Security. Lot of DDOS attacks are there. Some of the main DDOS attacks are described as follows:

Tear drop attacks: It involves sending of mangled ip fragments with overlapping, over-sized payloads to the target node. Because of this various operating systems may get crashed as a bug resides in TCP/IP fragmentation re-assembly code.

Phlashing attack: It is a permanent DDOS attack that damages victim system so badly that leads victim to re-install the operating system. It exploits security flaws that allow remote administration.

Reflected attack: This kind of attack involves sending forge request of some type to a large number of computers that will reply to the request.

ICMP flood attack: Defending (Xing and Wang, 2006). It is a smurf attack that floods DOS attack over the public internet. It depends mainly on network devices (which are not configured properly) that allow packets to be forwarded to the other hosts in the network. In such case, all the perpetrators will send large numbers of IP packets with the source faked to appear to be the address of the victim.

Peer to peer attacks: Here the attacker acts as a master instructing clients of large p2p file sharing, hubs to disconnect from their p2p networks and to connect to the victims website.

LITERATURE SURVEY

Already different methods have been proposed to transfer data securely over the internet. But none of them has provided a feasible solution to counter the DDOS attacks. Some of the existing mechanisms and their pit falls were discussed below. Packet marking technique (Akyuz and Sogukpinar, 2009) is an initial approach of tracing back source node in case of ddos attacks. But it failed in case of IP SPOOFING by the attacker node.

Corresponding Author: Jeevaa Katiravan, Department of Computer Science and Engineering, Anna University, Chennai, India

In the SYN agent model (Choi *et al*., 2010) the agent is used instead of the proxy server or firewall between the client and the server. The SYN-agent on the real server answer the client with SYN/ACK after receiving a SYN packet from the client side. If it is a SYN-attack, there should be no further ACKs. After a short time, the half-open TCP socket will be deleted from the agent. If it is a really connection request after the third time handshake packet arrived, the agent set the reserved bit in the TCP header to be 1 and route the packet to the real server.

EMDAF (Nagaratna *et al*., 2009) is encrypted based packet marking technique used as a solution for IP trace back in case of IP SPOOFING. But it involves 10% of routers communication in the process and also it adds certain load on the server to generate the encrypted key. PPM (Xing and Wang, 2006) is packet marking with distance based probabilities. In this approach packets probabilistically mark the packets they transmit. It uses node sampling in addition. Hop Count Based (KrishnaKumar *et al*., 2010) is one of the recent solutions proposed to counter DDOS attacks. In this method an assumption that systems in the current internet architecture are located max with a hop count of 255.

There were also few proposed solutions to counter DDOS attacks by using flexible deterministic packet marking technique from various research scholars. This packet marking technique is all about tracing back the attacker node using his ip address marked in the packet header before he transmits the packet in to the network. This approach has few limitations:

- While tracing back the path, it is not confined that network path may not fail
- When Attacker uses IP SPOOFING, this solution cannot trace back the original true source
- IP SPOOFING attacks were mainly of two types

Reflector attacks: Through this attack, attacker overwhelms the victim through network traffic by sending packets to the server using spoofed address (victim's address).

TCP SYN flooding: Integrated (Akyuz and Sogukpinar, 2009) here attacker initiates a TCP connection with a victim that never be completed hence resulting in the resource wastage of victim.

Proposed solution: The proposed solution mainly concentrates in defending these the second kind of attack as solution to first problem is already proposed in (Chandak and Ramasubramanian, 2005). This study (Zhou, 2008) overcome the initial limitation of previous proposals by constructing the back-up path

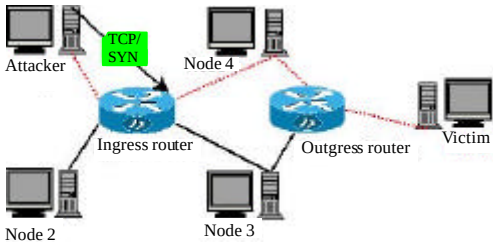

Fig. 1: Example network

Table 1: Notations used

Notation	Meaning
N_s	Sender node
N_d	Destination node
I_g	Egress router
O_g	Ogress router
H_{cs}	Hash code generated by sender
H_{cr}	Hash code generated by I_g
S_k	Shared key

using failure resiliency algorithm which is faster enough to construct alternative paths from sender node to destination node. The main concern is to over come IP spoofed attacks. Here is the solution that we propose. As we know that attacker can sends the packets to the victim through the network.

Egress router is the one directly connected to the attacker node. So, obviously attacker needs to forward his packet through egress router.

So, we assume to provide secured authentication between attacker and the egress router. This authentication mechanism includes pre shared key which we consider to be one of the finest secured wireless authentication mechanism as in Fig. 1. The process of authentication involves the parameters shown in Table 1.

Initially the sender node need to get registered with the egress router in order to send its packets through the network and later using pre shared key mechanism it gets authenticated by egress router (I_g). This key is assigned by the router to all the nodes uniquely who was in the domain of router. The sender node encrypts its initial packet with this key and sends as a TCP/SYN packet to the ingress router. This makes the burden of authenticating further packets coming from the same sender node to be reduced. This process involves the following steps:

- N_a--->I_g: Sender node sends the request using TCP/SYN (encrypted with pre-shared key given by the router) to the ingress router Hc
- I_g --->N_a: Egress router now checks for authentication of sender node by decrypting the TCP/SYN packet using pre-shared key and sends acknowledgement to sender node

- N_a --->I_g: Further packets from the same sender in that session no need to be authenticated as we have used TCP/SYN packet as an authentication packet initially
- I_g --->Nb: Now Ingress router forwards these packets into the network to the destination node

Algorithm 1

Required: N_a, I_g , H_c, S_k, Network shown in Fig. 1.

Assumption: Sender node has already registered with the router and got the pre-shared key.

Process:

- Sender node sends a request to egress for sending data packets to destination node using the function sendPacket (req)
- Egress router now will send challenge response acknowledgement to sender node chaAck ()
- Now sender node will send the new packet encrypted with pre-shared key to the ingress router. This packet need to be a TCP/SYN packet making sure that further authentication of packets is not required in that session for the same node

ADVANTAGES

We have considered few parameters to make the proposal to be defined as one of the finest solutions to trace back source node as follows:

If the sender node is considered to be an attacker node and targets destination node with reflector attacks then the ogress router fails back to trace the original source of packets in case of IP SPOOFING.

But through the mechanism we can over come this problem. Though the sender node changes its IP it can't change the pre shared key generated by its egress router.

This makes the sender node not to sent data packets again to the same victim using different IP. If it tries to do, it will get easily identified with its pre-shared key (Table 2).

Table 2: Performance comparison

Parameters	Pre-shared key
Routers usage in network	Less
Messages involved in authentication	Less
Security level	High
Packets required to re construct the path	Less
Expected no of false positives	0.3

We planned to simulate this paradigm using NS2 by implementing the algorithm 1. In order to calculate the accuracy of a trace back mechanism against large DDOS attacks, we have used the number of false positives. This false positive rate is affected by the number of attackers.

CONCLUSION

Methods to defend IP spoofed DDOS attacks are not yet proved completely. Lot many new proposals getting evolved with slight modifications and security advances.

The proposal 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 cant change the pre shared key exchanged between it and egress router which is used for authentication.

So, the attacker node can't target the victim using IP Spoofing mechanism. The future enhancement is to implement this idea in Mobile Adhoc Networks (Xiang and Li, 2006).

REFERENCES

Akyuz, T. and I. Sogukpinar, 2009. Packet marking with distance based probabilities for IP traceback. Proceedings of the 1st International Conference on Networks and Communications, Dec. 27-29, Chennai, pp: 433-438.

Chandak, A. and S. Ramasubramanian, 2005. Dual-link failure resiliency through backup link mutual exclusion. Proceedings of the 2nd International Conference on Broadband Networks, Oct. 3-7, Boston, MA. USA., pp: 258-267.

Choi, Y.S., J.T. Oh, J.S. Jang and J.C. Ryou, 2010. Integrated DDoS attack defense infrastructure for effective attack prevention. Proceedings of the 2nd International conference on Information Technology Convergence and Services (ITCS), Aug. 11-13, Cebu, pp: 1-6.

KrishnaKumar, B., P.K. Kumar and R. Sukanesh, 2010. Hop count based packet processing approach to counter DdoS attacks. Proceedings of the International Conference on Recent Trends in Information, Telecommunication and Computing, March 12-13, Kochi, Kerala, pp: 271-273.

Nagaratna, M., V.K. Prasad and S.T. Kumar, 2009. Detecting and preventing IP-spoofed DDOS attacks by Encrypted Marking Based Detection and Filtering (EMDAF). Proceedings of the International Conference on Advances in Recent Technologies in Communication and Computing, Oct. 27-28, Kottayam, Kerala, pp: 753-755.

Xiang, Y. and Z. Li, 2006. An analytical model for DDOS attacks and defense. Proceedings of the International Multi-Conference on Computing in the Global Information Technology, August 2006, Washington, DC. USA., pp: 66-66.

Xing, F. and W. Wang, 2006. Understanding dynamic denial of service attacks in mobile Ad Hoc networks. Proceedings of the Military Communications Conference, Oct. 23-25, Washington, DC. USA., pp: 1-7.

Zhou, W., 2008. Keynote III: Detection and traceback of DDOS attacks. Proceedings of the 8th IEEE International Conference on Computer and Information Technology, July 8-11, Sydney, New South Wales, pp: 3-3.