Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.429 – 432

RESEARCH ARTICLE

IP Trace Back Scheme for Packet Marking and Packet Logging Using RIHT

C. VAIYAPURI[1], R. MOHANDAS[2]
[1]SCHOOL OF COMPUTING SCIENCES, HINDUSTAN UNIVERSITY, CHENNAI, India
[2]SCHOOL OF COMPUTING SCIENCES, HINDUSTAN UNIVERSITY, CHENNAI, India

[1] *ramu.meet@gmail.com*; [2] *mohandas@hindustanuniv.ac.in*

Abstract— Internet Protocol trace back is the enabling technology to control the crime. Internet Protocol packet is to find the real source of Internet attacks, we must possess the capability of discovering the origin of IP packets without relying on the source IP address field. This capability is called IP trace back. IP trace back systems provide a means to identify true sources of IP packets without relying on the source IP address field of the packet header, and are the major technique to find the real attack sources. In this project we present an IP trace back system called Deterministic Packet Marking and with packet logging which provides [1] a defense system with the ability to find out the real sources of attacking packets that traverse through the network. While a number of other trace back schemes exist, we propose a new hybrid IP trace back scheme with efficient packet logging aiming to have a fixed storage requirement for each router in packet logging without the need to refresh the logged tracking information and to achieve zero false positive and false negative rates in attack-path reconstruction.

Key Terms: - DoS attack; DDoS attack; hybrid IP trace back; IP spoofing; packet logging; packet marking

I. INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company [1], and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions.

II. REVIEW OF THE EXISTING SYSTEM

A DDoS attack is an availability attack, for it is characterized by an explicit attempt from an attacker to prevent legitimate users from using the desired resources (CERT). Many institutes have reported DDoS attacks cause a huge amount of financial loss every year. DDoS attacks can cause the inability of information infrastructure to function, total stoppage or severe impairment of activity; therefore it can [3] result in threatening for life etc. The difficulty in solving the problem is first the DDoS tools are easy to get and use, thus even an inexperienced hacker can launch an attack effortlessly. The second reason is that it is difficult to separate unambiguously the attack traffic from legitimate traffic, and then filter out the attack traffic. Accurately separating and filtering attack traffic can provide maximum possible resources to legitimate users of the information infrastructure. The exiting packet marking can be put into two categories, deterministic packet marking (DPM) and probabilistic packet marking (PPM). These traceback schemes to mark a border routers' IP address on the passing packets. However, IP header's identification field is not enough to store the full IP address. In this section presents a comprehensive survey, mainly focused on the study of research methods for an IP trace [2]back system and then discusses the overview of various algorithms, concepts and techniques defined in different research papers.

A. Flexible Deterministic Packet Marking: An IP Trace back System to find the Real Source of Attacks

Xiang et al [1] proposed FDPM is suitable for not only tracing sources of DDoS attacks but also DDoS detection. The main characteristic of DDoS is to use multiple attacking sources to attack a single victim (the aggregation characteristic). Therefore, at any point in the network, if there is a sudden surge in the number of packets with the same destination address and with the same group of digest marks, it can be a sign of a DDoS attack. In FDPM, the marks in packets do not increase their size therefore no]additional bandwidth is consumed.

FDPM can maintain the trace back process when the router is heavily loaded, whereas most current trace back schemes do not have this overload prevention capability. A novel and practical packet marking trace back system, incorporating a flexible mark length strategy and flexible flow-based marking scheme, is proposed. Simulation and real system implementation show FDPM produces better performance than any other current trace back scheme in terms of false positive rates, the number of packets needed to reconstruct one source, the maximum number of sources that can be traced in one trace back process, and the maximum forwarding rate of trace back-enabled routers.

B. IP Trace back with Deterministic Packet Marking

Goodrich [2] proposed DPM is light, secure, scalable, and suitable for many types of attacks. Another modification to the basic approach will be aimed to address the fact that an IP source address can be changed by the attacker during the attack. Though the marks in DPM cannot be spoofed, frequent spoofing/changes of the source address with a different value by an attacker may void the DPM's effectiveness. This problem can be solved by making the destination rely only on the marks, which cannot be spoofed. By using a globally known hash function, the destination can verify that the two halves of the ingress address, received in the marks, do indeed belong to the same ingress address without relying on the source address of the packet. This solution will require sending additional marks with hash values, and will somewhat raise the expected number of packets needed for reconstruction of the ingress address.

C. Deterministic Packet Marking Based on Redundant Decomposition for IP Trace back

Jin et al [3] proposed a novel deterministic packet marking scheme for IP trace back against distributed denial of service attacks is presented. Besides the hash correlation functions, our scheme has a unique technique: redundant decomposition, which plays an important role in improving the recovery performance. Theoretical analyses, the pseudo code and the experimental results are provided.

D. Problem statement

A DDoS attack is an availability attack, for it is characterized by an explicit attempt from an attacker to prevent legitimate users from using the desired resources. Many institutes have reported DDoS attacks cause a huge amount of financial loss every year. DDoS attacks can cause the inability of information infrastructure to function, total stoppage or severe impairment of activity; therefore it can result in threatening for life etc.

The difficulty in solving the problem is first the DDoS tools are easy to get and use, thus even an inexperienced hacker can launch an attack effortlessly. The second reason is that it is difficult to separate unambiguously the attack traffic from legitimate traffic, and then filter out the attack traffic. Accurately separating and filtering attack traffic can provide maximum possible resources to legitimate users of the information infrastructure. The existing packet marking can be put into two categories, deterministic [3]packet marking and probabilistic packet[4] marking. These trace back schemes to mark a border routers' IP address on the passing packets. However, IP header's identification field is not enough to store the full IP address.

III. SOLUTION TO THE PROPOSED PROBLEM

The proposed project RIHT: An IP Trace back System to Find the Real Source of Attacks is to control Internet crime. IP trace back is the enabling technology to control Internet crime. IP trace back systems provide a means to identify true sources of IP packets without relying on the source IP address field of the packet [5]header, and are the major technique to find the real attack sources.

DPM can maintain the trace back process when the router is heavily loaded. DPM requires little computing power and adaptively keeps the load of routers in a low degree. DPM provides more features to trace IP packets than other packet marking schemes, and can obtain better tracing capacity. We propose a new hybrid IP trace back scheme (RIHT) for efficient packet logging aiming to have a fixed storage requirement according to the in packet logging without the need to refresh the logged tracking information. Also, the proposed scheme has zero false positive and false negative rates in an attack-path reconstruction.

A.RIHT Algorithm

RIHT provides more features to trace IP packets than other packet marking schemes, packet logging schemes, and can obtain better tracing capacity. The algorithm is as follows:

```
Marking procedure at router R, edge interface I;
for each incoming packet
let x be random number from(0,1)
if x<0.5 then
  write I0-15 into w.ID_field
  write ‘0’ into w.flags[0]
       else
           write I16-31 into w.ID_field
           write ‘1’ into w.flags[0]
Ingress address reconstruction procedure at victim V;
for each packet w from source Sx
if Ingress Tbl[Sx]==Nil then
create Ingress Tbl[Sx]
if w.flags [0]==’0’ then
    Ingress Tbl[Sx]0-15 : w.ID_field
else
Ingress Tbl[Sx]16-31 : w.ID_field
```

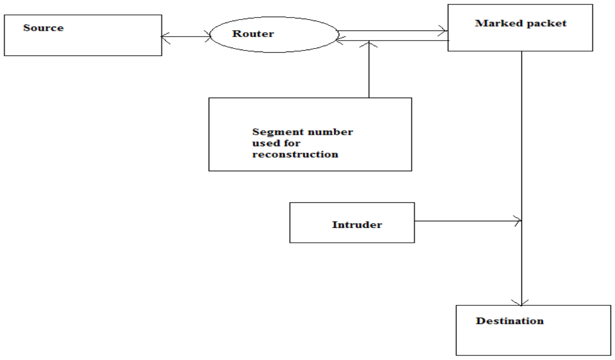

Fig 1: Design of RIHT

IV. FRAMEWORK OF RIHT ALGORITHM

The system has divided into three modules

Packet marking

IP Trace back

Reconstruction

A. Packet marking

This module is designed in such a way that when an IP packet enters the protected network, it is marked by the interface close to the source of the packet on a router. The source IP addresses are stored in the marking fields. The mark will not be overwritten by intermediate routers when the packet traverses the network**.**

B.IP Trace back

After all the segments corresponding to the same router address have arrived at the reconstruction point, the source IP address of the packets can be reconstructed. In order to [4]keep track of the set of IP packets that are used for reconstruction, the identities showing the packets coming from the same source must be included. The reconstructed packets will be forwarded by the router to the server by the authenticated client's IP address.

C. Reconstruction

Reconstruction is the process of getting back the packet and sending them one by one by denial of service. This helps in construction[5] of improper packets and also helps in avoiding further the loss of packets. The FDPM involves in the number of the number of the packet count of the reconstructed packets.

V. RESULTS AND DISCUSSION

By this proposed system we avoid DDOS defence attack in the network. It provides the reliable and guarantees delivery of packets and controlling the communication overheads in the network. RHIT provides innovative features to trace the source of IP packets and can obtain better tracing capability than others. DPM can maintain the trace back process when the router is heavily loaded. DPM requires little computing power and adaptively keeps the load of routers in a low degree. RHIT provides more features to trace IP packets than other packet marking schemes, and can obtain better tracing capacity [5]compared to other techniques used in the project.

The requirements specification is a technical specification of requirements for the software products. It is the first step in the requirements analysis process it lists the requirements of a particular software system including functional, performance and security requirements. The requirements also provide usage scenarios from a user, an operational and an administrative perspective. The purpose of software requirements specification is to provide a detailed overview of the software project, its parameters and goals. This describes the project target audience and its user interface, hardware and software requirements. It defines how the client, team and audience see the project and its functionality.

VI. CONCLUSION

A new hybrid IP trace back scheme (RIHT) for efficient packet logging aiming to have a fixed storage requirement in packet logging without the need to refresh the logged tracking information. Also, the proposed scheme has zero false positive and false negative rates in an attack-path reconstruction. Apart from these properties, our scheme can also deploy[6] a marking field as a packet identity to filter malicious traffic and secure against DoS/DDoS attacks consequently, with high accuracy, a low storage requirement, and fast computation, RIHT can serve as an efficient and secure scheme for hybrid IP trace back.

REFERENCES

[1] H. Farhat (2006), "Protecting TCP Services from Denial of Service Attacks," Proc. ACM SIGCOMM Workshop Large-Scale Attack Defense (LSAD '06), pp. 155-160, 2006.

[2] M.T. Goodrich (2002), "Efficient Packet Marking for Large-Scale IP Trace back," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS '02), pp. 117-126, 2002.

[3] G. Jin and J. Yang(2006), "Deterministic Packet Marking Based on Redundant Decomposition for IP Trace backs," IEEE Comm. Letters, vol. 10, no. 3, pp. 204-206, 2006.

[4] Y. Kim, J.Y. Jo, and F.L. Merat (2003), "Defeating Distributed Denial of-Service Attack with Deterministic Bit Marking," Proc. IEE Global Telecommunications Conf. (GLOBECOM '03), pp. 1363-1367, 2003.

[5] Y.K. Tseng, H.H. Chen, and W.S. Hsieh (2004), "Probabilistic Packet Marking with Non-Primitive Compensation," IEEE Comm. Letters, vol. 8, no. 6, pp. 359-361, 2004.

[6] H. Wang, C. Jin, and K.G. Shin(2007), "Defense against Spoofed IP Traffic Using Hop-Count Filtering," IEEE/ACM Trans Networking, vol. 15, no. 1, pp. 40-53, 2007.