JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IP Traceback Approach with Packet Marking and Logging System

Mr. Vantakula Leela Ruthvik*1, Mr. M. Somasundara Rao*2

[1]MCA Student, Department of Master of Computer Applications,
Vignan's Institute of Information Technology (A), Beside VSEZ, Duvvada Vadlapudi Post,Gajuwaka, Visakhapatnam-530049.

[2]Associate Professor, Department of Information Technology,
Vignan's Institute of Information Technology(A), Beside VSEZ,Duvvada,Vadlapudi Post,
Gajuwaka, Visakhapatnam-530049.

Abstract

Due to the widespread usage of the Internet in many different industries, network security challenges are becoming more and more prevalent and drawing public attention. But before launching an assault, attackers frequently disguise themselves by faking their own IP addresses. For this reason, numerous traceback strategies have been proposed by researchers to identify the origin of these attacks. To track IP addresses, certain packet logging techniques only need one packet. Others construct hybrid IP traceback techniques that require less storage but a longer search time by combining packet marking with packet logging. In this paper, we propose a new hybrid IP traceback scheme with efficient packet logging with the goals of achieving zero false positive and false negative rates in attack-path reconstruction and a fixed storage requirement for each router (under 320 KB, according to CAIDA's skitter data set) in packet logging. In addition, we censor attack behavior on a packet's upstream routers using the marking field. Finally, we simulate and compare our plan to other similar research in the areas of accuracy, processing, and storage demand.

Keywords: CAIDA's, Traceback IP, Router, Packet Logging.

1. INTRODUCTION

Due to the online's explosive growth, several online apps are being created for diverse user types. The impact of attacks grows more substantial as a result of Internet access's declining cost and growing availability through a variety of devices and apps. A distributed denial of service (DDoS) attack may be launched by knowledgeable attackers to interfere with a server's service. We may divide DDoS assaults into flooding-based attacks and software exploit attacks based upon how many packets must be sent to disable a server [10]. The primary characteristic of flooding-based attacks is the huge number of faked source packets used to deplete the victim's meager resources. Software exploit attacks are another sort of denial-of- service attack that target hosts by exploiting of their vulnerabilities. Core routers fail to determine the origin of packets since a majority of edge routers ignore the origin address of a packet. When a hacker wishes to prevent being monitored, they can spoof the source IP address in a packet. So, IP spoofing makes it difficult for hosts to fight against a DDoS attack. These factors have made creating a system to identify the true source of impersonation attacks a crucial issue in today's society. Burch and Cheswick provide a link test method employing the

UDP chargen service to impose an extra load on upstream lines in order to locate the true source of flooding-based attack packets. For it to locate the upstream router that the attack traffic flows through, the extra load may compete with the attack packets and delay the attack traffic. Bellovin et al. offer an iTrack system that uses the triggering packet to generate an ICMP packet with the router's forward and backward links. To retrace the attack path, the victim host gathers the ICMP messages. In order to identify the router or path information on the triggering packets, packet marking methodologies are created because earlier schemes required extra packets to trace the origin of attack packets.

Deterministic packet marking (DPM) and probabilistic packet marking (PPM) are two types of packet marking. In order to designate a border router's IP address on the passing packets, Belenky and Ansari suggest DPM trace back techniques. The identification field of an IP header, however, is insufficient to contain the entire IP address. Due to this, the border router computes 3 the IP digest and divides its IP into many chunks. The digest and a segment are then randomly selected and marked on the passing packets. The digest can be used by the destination host to put the various segments together once it has enough packets to do so. Savage et al., on the other hand, suggest a PPM approach with edge sampling that they refer to as FMS. The AMS scheme is suggested by Song and Perrig. The FIT approach is proposed by Yaar et al. The probabilistic pipelined packet marking (PPPM) scheme is proposed by Al-Duwari and Govindarasu. A useful packet labeling system is suggested by Gong and Sarac. These probability- based systems call for routers to assign a probability to the partial path information on packets that travel through them. In other words, a victim can recreate the entire attack path if it gathers enough tagged packets.

2.LITERATURE SURVEY

1. Introduction to IP traceback techniques: In the rapidly evolving landscape of computer networks and the Internet security challenges have become increasingly complex and cyber attacks are a constant threat. Among these challenges, the ability to trace the source of malicious network traffic or cyber attacks has emerged as a critical requirement for effective network defense and incident response IP trace back techniques place a pivotal role in addressing these need by enabling network administrators to trace the origin of unauthorized or harmful network activities back to their source. IP traceback refers to the process of identifying the source of network packets or data by analyzing the network path they traverse. This capability is invaluable in investigating and mitigating various types of cyber attacks, including distributed denial-of-service, (DDoS) attacks, spoof traffic and other malicious activities that can lead to network outages, data breaches or service disruptions.

2. Packet marking techniques: Packet marking involves embedding identifying information into packets as they traverse the network. This information can include router-specific details, timestamps and other data that aids in tracing the path taken by the packet. When a malicious packet is detected, routers or network devices that encounter the packet add their markings before forwarding it. At the destination, the markings are analyzed to reconstruct the path taken by the packet. Technique likes “hash based marking” and “probabilistic marking” fall under this category. IP traceback techniques offer valuable insights into understanding the source of network Attacks and identifying compromise systems. However, each approach has its strengths and limitations. And researchers are continuously working to improve their accuracy, scalability and effectiveness.

3. Packet logging techniques: Packet logging relies on routers and network devices storing information about packets they handle. Each router along the packets path maintains a log of packets passing through it. This log contains relevant information such as source and destination addresses, timestamps and positive. And possibly intermediate router information when 13 a malicious packet is identified, network administrators can retrieve the logged information from routers to reconstruct the packets path and trace its origin. IP drives back techniques offer valuable insights into understanding the source of network attacks and identifying compromised systems. However, each approach has its

strengths and limitations, and researchers are continually working to improve their accuracy, scalability and effectiveness.

4. Packet marking and logging integration for Ip traceback: Integrating packet marking and packet logging for IP Traceback involves combining the strands of both techniques to enhance the accuracy and efficiency of tracing the source of network packets. Here's you can integrate packet marking and login for an effective IP trace back solution. They are , Marking and logging strategy, Triggering trace back, Initial Marking analysis, Logging and verification, Hybrid traceback process, Adaptive strategies, Resource Management, Testing and Validation, Performance optimization, Documentation and Reporting.

3.EXISTING SYSTEM

We propose a trace back scheme that marks routers' interface numbers and integrates packet logging with a hash table (RIHT) to deal with these logging and marking issues in IP trace back. RIHT is a hybrid IP trace back scheme designed to achieve the following properties:

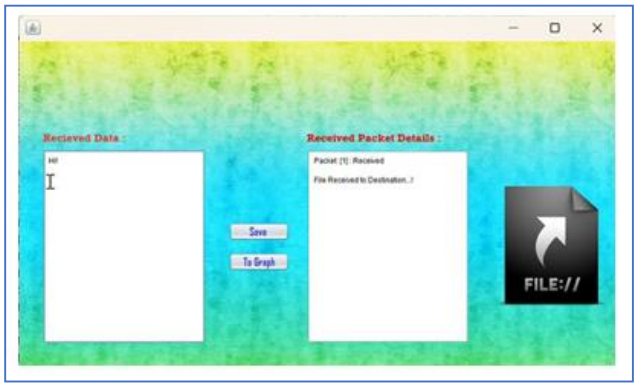
1. Our storage requirement for an arbitrary router is bounded above by the number of paths to the router, and thus every router does not need to refresh logged tracking information.
2. Our scheme achieves zero false positive and false negative rates in attack-path reconstruction.
3. We have higher efficiency in path reconstruction.
4. Our scheme can censor

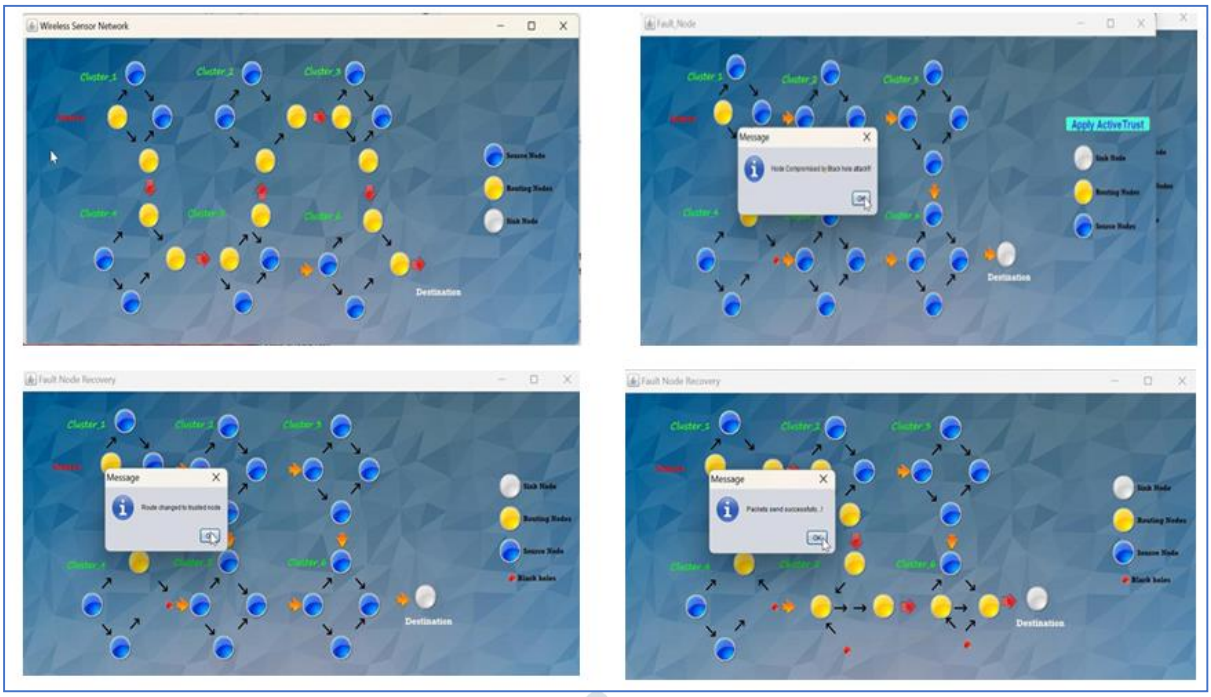
4. PROPOSED SYSTEM

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 a marking field as a packet identity to filter malicious traffic and secure against DoS/DDoS attacks. However, adversaries often hide themselves by spoofing their own IP addresses and then launch attacks. For this reason, researchers have proposed a lot of trace back schemes to trace the source of these attacks. Some use only one packet in their packet logging schemes to achieve IP tracking. Others combine packet marking with packet logging and therefore create hybrid IP trace back schemes demanding less storage but requiring a longer search.

5. EXPERIMENTAL RESULTS

Home Page:





6. CONCLUSION

The propose a new hybrid IP traceback scheme 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 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 traceback. An efficient traceback scheme is necessary to identify the sources of DoS attacks which impose an imminent threat to the availability of Internet services. The work presented in this paper adopts a hybrid traceback approach in which packet marking and packet logging are integrated to achieve the best of both worlds (i.e., small number of attack packets to conduct the traceback process, and small amount of resources to be allocated at intermediate routers for packet logging purposes).

7. REFERENCES

[1] B. Al-Duwari and M. Govindarasu, "Novel hybrid schemes employing packet marking and logging for IP traceback," IEEE Trans. Parallel Distributed System., vol. 17, no. 5, pp.
403–418, May 2006.

[2] A. Apple-by, Murmurhash 2010 [Online]. Available: http://sites.google. com/site/murmurhash/

[3] A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," IEEE Commun. Lett., vol. 7, no. 4, pp. 162–164, Apr. 2003.

[4] A. Belenky and N. Ansari, "Tracing multiple attackers with deterministic packet marking (DPM)," in Proc. IEEE PACRIM'03, Victoria, BC, Canada, Aug. 2003, pp. 49–52.

[5] S. M. Bellovin, M. D. Leech, and T. Taylor, "ICMP traceback messages," Internet Draft: Draft-Ietf-Itrace-04.Txt, Feb. 2003.

[6] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in Proc. USENIX LISA 2000, New Orleans, LA, Dec. 2000, pp. 319–327.

[7] CAIDA's Skitter Project CAIDA, 2010 [Online]. Available: http://www.caida.org/tools/skitter/

[8] K. H. Choi and H. K. Dai, "A marking scheme using Huffman codes for IP traceback," in Proc. 7th Int. Symp. Parallel Architectures, Algorithms Networks (SPAN'04), Hong Kong, China, May 2004, pp. 421–428.

[9] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distributed System., vol. 19, no. 10, pp. 1310–1324, Oct. 2008.