International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 01 | Jan -2017 www.irjet.net p-ISSN: 2395-0072

A SURVEY ON OPPORTUNISTIC PIGGYBACK MARKING FOR IP TRACE BACK

Suraj Patil[1], Prof: Parth Sagar[2]

Department of Computer Engineering RMD Sinhgad School of Engineering, Pune

---

Abstract - *IP trace back is a solution for attributing cyber attacks, and it is also useful for accounting user traffic and network diagnosis. Marking-based trace back (MBT) has been considered a promising trace back approach, and has received considerable attention. However, the trace back message delivery problem in MBT, which is important to the successful completion of a trace back, has not been adequately studied in the literature. To address this issue, we present the design, analysis, and evaluation of opportunistic piggyback marking (OPM) for IP trace back in this paper. The OPM distinguishes itself from the existing works by decoupling the trace back message content encoding and delivery functions in MBT, and efficiently achieves expedited and robust trace back message delivery by exploiting piggyback marking opportunities. Based on the proposed OPM scheme, we then present the flexible marking- based trace back framework, which is a novel design paradigm these DoS attacks is that attackers use incorrect IP or spoofed IP addresses in the attack packets features for practical deployment of IP trace back. Through the numerical analysis and the comprehensive simulation evaluations, we demonstrate that our design effectively reduces the trace back completion delay and router processing overhead, and increases the message delivery ratio compared with other baseline approaches.*

Key word: IP trace back, marking based trace back, opportunistic piggyback marking, network forensics.

I. Introduction

Denial-of-service (DoS) attacks pose an increasing threat to number of IP trace back techniques have been proposed in the marking based trace back (MBT) approach. Even more concerning, automatic attacking tools such as Tribal Flood Network (TFN), TFN2K, Trinoo, DDoS attacks And real DDoS attacks are often mounted from hundreds or even thousands of hosts. the attack packets and hence disguise the real origin of the attacks. Due to the stateless nature of the Internet, IP trace back is a difficult problem to determine the source of these spoofed IP packets, which is called the IP trace back problem.

While a number of IP trace back techniques are in the marking based trace back (MBT) approach has received considerable attention. The basic idea of MBT is that routers convey their trace back messages (e.g., the identity information) to the end-hosts by marking on passing packets. Accordingly, an end host can construct a graph of network paths traversed by these marked packets regardless of source IP trace back address spoofing. It is obvious that applying packet level marking all the time on all traffic flows is unnecessary and it suffers the scalability problem which overloads routers by marking each passing packet, trace back mechanisms are activated in a reactive manner, e.g., triggered by attack detection systems when any abnormal traffic flow is detected.

In this paper we have surveyed on various types of Load balancing methods. Section II of this paper deals with literature survey and Section III conclusion of the paper.

II. LITERATURE SURVEY

Chao Gong [1] proposes to develop a hybrid IP trace back approach based on both packet marking and packet logging. Legitimate users from accessing that resource Semantic attacks exploit some specific feature or implementation bug of operating systems or routers to disable the services with one single or a few packets. An IP trace back approach that can track an individual packet is a must for defending against semantic DoS attacks. In order to keep consistent with the literature, we term a packet of interest an attack

packet. [2] The destination of an attack packet is a victim, the network path traversed by an attack packet is an attack path, and the output of IP trace back process is an attack graph composed of one or more possible attack paths for an attack packet. The basic idea of IP trace back approach based on packet marking is that the router marks packets with its identification information as they pass through that router. The mark overloads a rarely used field in IP packet header, i.e., 16-bit IP identification field. The identification of a router could be 32-bit IP address hash value of IP address or uniquely assigned number [3] In the last two cases, the length of identification information is variable and could be less than 16 bits. Since the marking space in packet header is too small to record the entire path, routers mark packets with some probability so that each marked packet carries the information of one node in the path. [4] The length of router identification and the implementation of marking procedure, the router may only write part of its identification information into the marking space. While each marked packet represents only a small portion of the path it has traversed, the whole network path can be reconstructed by combining a modest number of such packets. This kind of approach is referred to as probabilistic packet marking (PPM) [5]. The PPM approach does not incur any storage overhead at routers and the marking procedure (a write and checksum update) can be easily and efficiently executed at current routers. But due to its probabilistic nature, it can only trace the traffic that consists of a large volume of packets.

III. Conclusion

Our project proposed opportunistic piggyback marking, a novel trace back acceleration mechanism for IP trace back. The main idea is to exploit free ride opportunities for expedited and robust delivery of trace back message fragments to end-hosts. Using this idea we designed a trigger-based IP trace back approach, which supports the trace back of individual packets. We then provided a theoretical analysis of marking-based trace back, and showed the potential of opportunistic piggyback marking. We also presented a flexible marking-based trace back (FMBT) framework, which meets several favorable objectives that previous individual trace back schemes failed to satisfy simultaneously. Comprehensive performance comparisons demonstrated the effectiveness and efficiency of our design for IP trace back. As for our future work, we would like to investigate counter-measures to mitigate the problem of compromised routers in marking-based IP trace back, address the robustness of message delivery in FMBT, and implement OPM/AOPM on a real network environment.

ACKNOWLEDGMENTS

It is my privilege to acknowledge with deep sense of gratitude to my guide Prof. Parth Sagar for his kind cooperation, valuable suggestions and capable guidance and timely help given to me in completion of my CPGCON Paper. I express my gratitude to Prof. Vina M. Lomte, Head of Department, RMDSSOE (Computer Dept.) for her constant encouragement, suggestions, help and cooperation.

References

1. L. Lu, M. C. Chan, and E.-C. Chang, “A general model of probabilistic packet marking for IP traceback,” in Proc. ASIACCS, 2008
2. C. Gong and K. Sarac, “A more practical approach for single-packet IP traceback using packet logging and marking,” IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008.
3. C. Gong and K. Sarac, “Toward a practical packet marking approach for IP traceback,” Int. J. Netw. Security, vol. 8, no. 3, pp. 271–284, 2009.
4. Y. Xiang, K. Li, and W. Zhou, “Low-rate DDoS attacks detection and traceback by using new information metrics,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 426–437, Jun. 2011
5. M.-H. Yang and M.-C. Yang, “RIHT: A novel hybrid IP traceback scheme,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 789–797, Apr. 2012.
6. Network Simulator 2.35. [Online]. Available: http://www.isi.edu/ nsnam/ns/, accessed Oct. 2015
7. T. H.-J. Kim,C. Basescu, L. Jia, S.B. Lee, Y.-C. Hu, and A.Perrig,“Lightweight source authentication and path validation,” in Proc. SIGCOMM, 2014
8. H. Zhang, J. Reich, and J. Rexford, “Packet traceback for software defined networks,” Dept. Comput. Sci.,Princeton University, Princeton, NJ, USA, Tech. Rep. TR-978-15, 201