Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA2012-3, February 10, 2012

Reliable Determination of Zombies Based on Entropy Variation

Anitha G
Department of computer science[PG],
SKP Engineering College,
Thiruvannamalai, Tamilnadu, India.
Email:deiva.anitha@gmail.com

Abstract - A zombie is a computer, connected to the internet that has been compromised by a cracker. Zombie computers are often used to launch distributed denial-of-service attacks. Distributed denial-of-service (ddos) attacks are a critical threat to the internet. However, the memoryless feature of the internet routing mechanisms makes it extremely hard to trace back to the source of these attacks. As a result, there is no effective and efficient method to deal with this issue so far. In this paper, I propose a novel traceback method for ddos attacks that is based on entropy variations between normal and ddos attack traffic, then compare this variation with the router's buffer's capacity, which is fundamentally different from commonly used packet marking techniques.

Key words: *IP Traceback, DDOS, Zombie, entropy variation.*

I. INTRODUCTION

IT is an extraordinary challenge to traceback the source of Distributed Denial-of-Service (DDoS) attacks in the Internet. In DDoS attacks, attackers generate a huge amount of requests to victims through compromised computers (zombies), with the aim of denying normal service or degrading of the quality of services. The key reason behind this phenomenon is that the network security community does not have effective and efficient traceback methods to locate attackers as it is easy for attackers to disguise themselves by taking advantages of the vulnerabilities of the World Wide Web, such as the dynamic, stateless, and anonymous nature of the Internet. IP traceback means the capability of identifying the actual source of any packet sent across the Internet. Because of the vulnerability of the original design of the Internet, we may not be able to find the actual hackers at present. In fact, IP traceback schemes are considered successful if they can identify the zombies from which the DDoS attack packets entered the Internet. Research on DDoS detection mitigation and filtering has been conducted pervasively. However, the efforts on IP tracebackare limited.

A number of IP traceback approaches have been suggested to identify attackers and there are two major methods for IP traceback, the probabilistic packet marking (PPM) and the deterministic packet marking (DPM). Both of these strategies require routers to inject marks into individual packets. Moreover, the PPM strategy can only operate in a local range of the Internet (ISP network), where
the defender has the authority to manage. However, this kind of ISP networks is generally quite small, and we cannot traceback to the attack sources located out of the ISP network.

The DPM strategy requires all the Internet routers to be updated for packet marking. However, with only 25 spare bits available in as IP packet, the scalability of DPM is a huge problem. Moreover, the DPM mechanism poses an extraordinary challenge on storage for packet logging for routers. Therefore, it is infeasible in practice at present. Further, both PPM and DPM are vulnerable to hacking, which is referred to as packet pollution.

II. RELATED WORK

It is obvious that hunting down the attackers (zombies), and further to the hackers, is essential in solving the DDoS attack challenge. In general, the traceback strategies are based on packet marking. Packet marking methods include the PPM and the DPM. The PPM mechanism tries to mark packets with the router's IP address information by probability on the local router, and the victim can reconstruct the paths that the attack packets went through.

The PPM method is vulnerable to attackers, as attackers can send spoofed marking information to the victim to mislead the victim. The accuracy of PPM is another problem because the marked messages by the routers who are closer to the leaves (which means far away from the victim) could be overwritten by the downstream routers on the attack tree. At the same time, most of the PPM algorithms suffer from the storage space problem to store large amount of marked packets for reconstructing the attack tree.

Moreover, PPM requires all the Internet routers to be involved in marking. Based on the PPM mechanism, Law et al. tried to traceback the attackers using traffic rates of packets, which were targeted on the victim. The model bears a very strong assumption: the traffic pattern has to obey the Poisson distribution, which is not always true in the Internet. Moreover, it inherits the disadvantages of the PPM mechanism: large amount of marked packets are expected to reconstruct the attack diagram, centralized processing on the victim, and it is easy be fooled by attackers using packet pollution.

The deterministic packet marking mechanism tries to mark the spare space of a packet with the packet's initial router's information, e.g., IP address. Therefore, the receiver can identify the source location of the packets once it has sufficient information of the marks. The major problem of DPM is that it involves modifications of the current routing software, and it may require very large amount of marks for packet reconstruction. Moreover, similar to PPM, the DPM mechanism cannot avoid pollution from attackers. Savage et al. first introduced the probability-based packet marking method, node appending, which appends each node's address to the end of the packet as it travels from the attack source to the victim.

III. PROBLEM STATEMENT

1. Network Construction: This module is developed in order to create a dynamic network. In a network, nodes are interconnected with the admin, which is monitoring all the other nodes. All nodes are sharing their information with each others.

2. Attacker: The attacker first establishes a network of computers that will be used to generate the huge volume of traffic needed to deny services to legitimate users of the victim. To create this attack network, attackers discover vulnerable hosts on the network. DDoS

attack, the master computer orders the zombies to run the attack tools to send huge volume of packets to the victim.

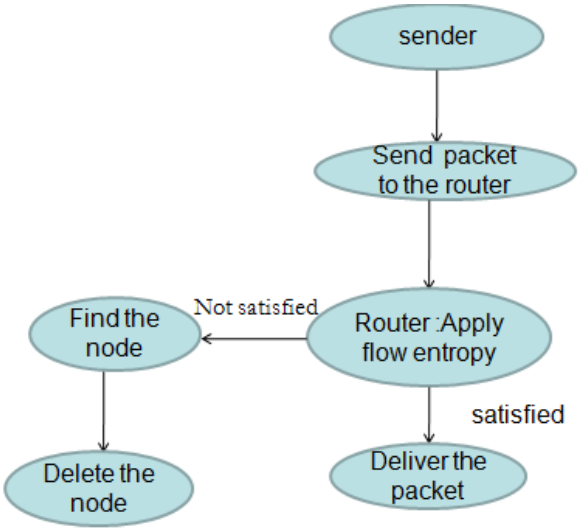

Figure 1: Architecture Diagram

3. Flow Entropy Variation: We categorize the packets that are passing through a router into flows. A flow is defined by a pair the upstream router where the packet came from, and the destination address of the packet. Entropy is an information theoretic concept, which is a measure of randomness. We employ entropy variation in this paper to measure changes of randomness of flows at a router for a given time interval. We notice that entropy variation is only one of the possible metrics. Change point of flows, to identify the abnormality of DDoS attacks however, attackers could cheat this feature by increasing attack strength slowly. We can also employ other statistic metrics to measure the randomness, such as standard variation or high-order moments of flows.

4. IP Traceback: Another defensive countermeasure is trace back, which enables law enforcement agencies to identify the original worm propagators and punish them. A trace back scheme typically involves a number of routers, which monitor all through-traffic and store traffic logs in a storage server. When a "trace back" order is given, the traffic logs (e.g., flow-level recorded logged by the networks) are postmortem analyzed in order to identify the origins of the worm propagator. When the source of the worm is detected the system alerts the node about the source and blocks all packets from that particular source.

5. Removal of Source Attacker: Once we apply the IP Trace back system, we can identify the exact source of the system which is involved in spreading of the worms. We are identifying the Source of the Worm creator & we can eliminate that system from the network. This process of elimination would create more secured communication.

REFERENCES

1. C. Patrikakis, M. Masikos, and O. Zouraraki, "Distributed Denial of Service Attacks," The Internet Protocol J., vol. 7, no. 4, pp. 13-35, 2004.
2. Y. Kim et al., "PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 2, pp. 141-155, Apr.-June 2006.
3. Y. Chen and K. Hwang, "Collaborative Detection and Filtering of Shrew DDoS Attacks Using Spectral Analysis," J. Parallel and Distributed Computing, vol. 66, pp. 1137-1151, 2006.
4. M.T. Goodrich, "Probabilistic Packet Marking for Large-Scale IP Traceback," IEEE/ACM Trans. Networking, vol. 16, no. 1, pp. 15-24, Feb. 2008.
5. T.K.T. Law, J.C.S. Lui, and D.K.Y. Yau, "You Can Run, But You Can't Hide: An Effective Statistical Methodology to Traceback DDoS Attackers," IEEE Trans. Parallel and Distributed Systems, vol. 16, no. 9, pp. 799-813, Sept. 2005.
6. [6] S. Savage, "Network Support for IP Traceback," IEEE/ACM Trans. Networking, vol. 9, no. 3, pp. 226-237, June 2001.
7. Belenky and N. Ansari, "IP Traceback with Deterministic Packet Marking," IEEE Comm. Letters, vol. 7, no. 4, pp. 162-164, Apr. 2003.
8. "IP Flow-Based Technology," ArborNetworks, http://www.arbornetworks.com, 2010.
9. C. Patrikakis, M. Masikos, and O. Zouraraki, "Distributed Denialof Service Attacks," The Internet Protocol J., vol. 7, no. 4, pp. 13-35,2004.
10. T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoSProblems," ACM Computing Surveys, vol. 39, no. 1, p. 3, 2007.
11. J. Mirkovic et al., "Testing a Collabotative DDoS Defense in a Red/Blue Team Exercise," IEEE Trans. Computers, vol. 57, no. 8, pp. 1098-1112, Aug. 2008.
12. H. Aljifri, "IP Traceback: A New Denial-of-Service Deterrent?" IEEE Security & Privacy, vol. 1, no. 3, pp. 24-31, May/June 2003.
13. Z. Gao and N. Ansari, "Tracing Cyber Attacks from the Practical Perspective," IEEE Comm. Letters, vol. 43, no. 5, pp. 123-131, May 2005.
14. Yaar, A. Perrig, and D. Song, "FIT: Fast Internet Traceback," Proc. IEEE INFOCOM, pp. 1395-1406, 2005.
15. A.C. Snoeren et al., "Hash-Based IP Traceback," Proc. ACM
16. SIGCOMM, 2001.
17. A.C. Snoeren et al., "Single-Packet IP Traceback," IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 721-734, Dec. 2002.
18. M. Sung et al., "Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Information-Theoretic Foundation,"IEEE/ACM Trans. Networking, vol. 16, no. 6, pp. 1253-1266, Dec. 2008.