IOSR Journal of Engineering (IOSRJEN)
ISSN: 2250-3021 Volume 2, Issue 8 (August 2012), PP 187-189
www.iosrjen.org

Assuage Bandwidth Utilization DDoS Attacks by Using Prototype Analyzer and Transfer Scheduling Scheme

Hemanth Kumar .P [1], Arjun Reddy.K.R [2], Nagarjuna.T [3]
[1]*Assistant Professor, Department of CSE, Kmm Institute of Technology and Science, Tirupati, AP*
[2] *Assistant Professor, Department of CSE Kmm Institute of Technology and Science, Tirupati, AP*
[3]*Assistant Professor, Department of CSE, Kmm Institute of Technology and Science, Tirupati, AP*

Abstract: - *Denial-of-service (DoS) attacks occur when the attacks are from a single source, whereas Distributed Denial-of-service (DDoS) attacks occur when many compromised systems flood the resources or bandwidth of a target system. Although we cannot alleviate the denial-of-service or distributed denial-of-service attacks entirely, we can limit the attacks by controlling the Transfer flow. In this paper, we propose a Prototype analyzer and Transfer scheduler scheme that analyzes the Transfer Prototype to distinguish the legitimate Transfer with that of attack Transfer and effectively schedule the Transfer for better bandwidth usage, providing Quality-of-Service (QoS) for the legitimate user.*

Keywords: *- DoS attack, DDoS attack, legitimate flow, attack flow, Prototype analyzer, Transfer scheduler.*

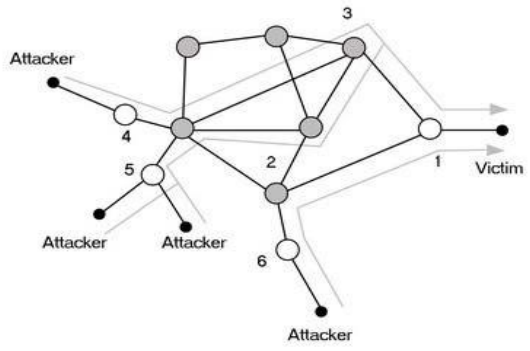
I. INTRODUCTION

Attackers take the advantages of the principles of the Internet such as openness, assessability, resources sharing and so on, to launch Distributed Denial-of-service flooding attacks (or bandwidth Utilization Attacks). Flood packets are generated by hundreds or thousands of compromised machines, called Zombie. Here the attacker's goal is not to break into the target system but to overwhelm its resources and make it unavailable to the legitimate user. So there is a need to effectively manage the malicious user and the legitimate user. Two features of DDoS attacks hold back the advancement of managing the users. First, it is hard to differentiate between DDoS attack Transfer and legitimate Transfer. There is a lack of an effective differentiation mechanism that results in minimal collateral damage for legitimate Transfer. Second, the sources of DDoS attacks are also not easy to find in a distributed environment. Therefore, it is difficult to stop a DDoS attack effectively. The objective of this research is to control unwanted flow by separating the attack Transfer and legitimate Transfer.

To prevent attacks, according to [2], one may adopt methods such as intrusion detection system (IDS) [3] or firewalls, which are effective for known attacks or IP addresses. Other methods including packet filtering, packet marking, and ICMP Traceback [4][5][6] messages, which are effective for identifying sources of attacks and instituting protection measures but are not easy to be deployed since they need supporting routers to maintain information regarding packets that pass through them. A pushback method [7] categorizes packets into "good Transfer", "bad Transfer", and "poor Transfer" packets. It analyzes bad Transfer packets and sends signals to upstream routers to control the flow of suspicious packets. If the router cannot correctly categorize packets, it affects flows of all packets through it. Since the normal packets are possible to use the same flow-controlled route to the server, the bandwidth allocated to normal users is also affected. Attacks on the networks, particularly, denial of service (DoS) and DDoS attacks, will paralyze services. We must protect the normal user by removing the malicious attacks on the network.

II. NETWORK TOPOLOGY

Consider a sample topology as shown in figure below,



The topology considered is similar to the one used traditionally to depict a typical router based network in the Internet. It shows four attackers flooding the victim over a simplistic version of a well connected core (grey nodes). The connected core generally forwards the Transfer through them; the attackers flood the network by utilizing the core. The arrows show the attack propagation path. Thus, the network is prone to attacks.

III. PROPOSED SCHEME

To effectively manage the users, we propose a Transfer scheduler scheme with the combination of Prototype analyzer. This defending scheme consists of the following modules:

- Address Verifier.
- Session Valuator.
- Prototype Analyzer.
- Transfer Scheduler.

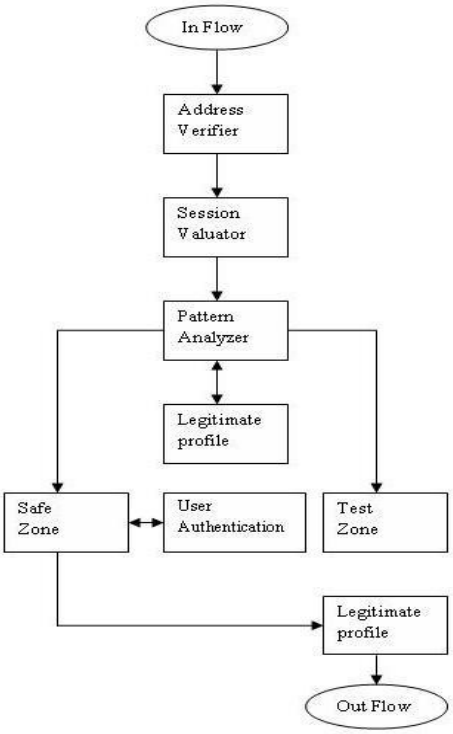


Figure 1: Block Diagram of the Proposed Scheme

The Transfer was checked by the address Verifier for the known attackers. It monitors the Transfer flow and drops any black listed attack packets are found. This blacklist is updated periodically as a new attacker was identified. This helps in the early stage mitigation of DoS and DDoS attacks.

After verifying the address the session valuator comes into picture. It analyzes Transfer sessions for abnormalities. It considers previous session records for analyzing and logs present session's information into the session record. If it finds any abnormality then it is considered of having attack traces, because attack Transfer disturbs the normal flow. When any changes are observed the Transfer was forwarded to the Prototype analyzer.

The Prototype analyzer contains a legitimate profile, which does not refer to the session behavior. Instead it contains the legitimate user behavior. This legitimate user profile was renewed periodically, so as to adapt to the environment. On the basis of the user profile the Transfer was distinguished. If any violation was found, the Prototype analyzer forwards the Transfer into the test zone; else the Transfer is forwarded into the safe zone. The Transfer in the safe zone is considered to be of the legitimate users, so it is forwarded directly to the Transfer scheduler providing Quality-of-service (QoS) to the legitimate user. Where as, the Transfer in the test zone was prompted for authentication. The authentication was a simple real time signature. If the test condition is failed, then the corresponding packets were dropped and this user address was updated in the blacklist. If it test condition is fulfilled the Transfer is forwarded to the Transfer scheduler.

The Transfer forwarded into the Transfer scheduler was scheduled in a timely fashion such that the Transfer from the safe zone was allocated with more bandwidth. If the available bandwidth is more and Transfer is low from the safe zone then it is balanced with the Transfer from test zone. That is, more bandwidth is

allocated to the test zone Transfer, after fulfilling the test conditions. If the bandwidth is available in a huge considerable rate then the Transfer in test zone is managed in such a way that there is a low occurrence of packet drops. The Transfer scheduler plays vital role in allocation of bandwidth for effectively providing the services.

IV. CONCLUSION AND FUTURE WORK

In this manner our proposed scheme, analyzes the Transfer Prototype to distinguish the legitimate Transfer with that of attack Transfer and effectively schedule the Transfer for better bandwidth usage, providing Quality-of-Service (QoS) for the legitimate user. As a future work we can consider the problem of IP spoofing in the validation module so as to address IP spoofing DDoS attacks.

Reference:

[1] Rufus Chakravarthy Sharma, Chanakya G.M, " A Compromised Multi-Level Detection and Mitigation of DDoS Attacks Using Watch-Dog Mechanism," Proc. of International Conference on Advances in Mathematical and Computational Methods (AMCM), vol.2, no.19, pp. 129-133, Jan. 2011.

[2] Chu-Hsing Lin, Jung-Chun Liu, Fuu-Cheng Jiang, Chien-Ting Kuo, "An Effective Priority Queue-based Scheme to Alleviate Malicious Packet Flows from Distributed DoS attacks," Proc. of International Conference on Multimedia and Ubiquitous Engineering, 2008.

[3] D. Nagamalai, C. Dhinakaran, J. K. Lee, "Multi Layer Approach to Defend DDoS Attacks Caused by Spam," Proc .of International Conf. of Multimedia and Ubiquitous Engineering, April, 2007.

[4] B. T. Wang, H. Schulzrinne, "An IP traceback mechanism for reflective DoS attacks," Proc. of IEEE Electrical and Computer Engineering 2004, May 2004.

[5] M. Song and J. Xu, "IP Traceback-Based Intelligent Packet Filtering: A Novel Technique for Defending against Internet DDoS Attacks," *Proc. of 10th IEEE Int'l Conf. Network Protocols (ICNP 2002)*, Nov. 2002.

[6] K. Park and H. Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attacks," *Proc. of IEEE INFOCOM 2001*, Mar. 2001.

[7] Y. Chen, Y. K. Kwok, and K. Hwang, "MAFIC: Adaptive Packet Dropping for Cutting Malicious Flows to Push Back DDoS Attacks," *Proc. of 25th IEEE Int' Conf. Distributed Computing Systems Workshops 2005*, June 2005.

[8] A Taxonomy of DDoS attacks and DDoS defense Mechanisms. Jelena Mirkovic, Janice Martin and Peter Reiher. Computer Science Department. University of California, Los Angeles, Technical Report #020018.

[9] CERT coordination center. Denial of Service attacks.

[10] Trends in Denial of Service Technology. http://www.cert.org/archive/pdf/DoS_trends.pdf

[11] http://en.wikipedia.org/wiki/SYN_flood

[12] H. Wang, D. Zhang, and K.G. Shin, "SYN-dog: Sniffing SYN Flooding Sources," *Proc. of 22nd Int'l Conf. Distributed Computing Systems (ICDCS '02)*, July 2002.

[13] http://en.wikipedia.org/wiki/Harmonic_Mean

[14] http://www.isi.edu/nsnam/ns/

[15] Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites. Jaeyeon Jung, Balachander Krishnamurthy. Proceedings of the International World Wide Web Conference, pages 252--262. IEEE, May 2002

[16] T. Peng, C. Leckie, and K. Ramamohanarao, "Detecting Distributed Denial of Service attacks using Source IP monitoring", draft, November 2002. <http://citeseer.ist.psu.edu/peng02detecting.html>.

[17] H. Takada and U. Hofmann, "Application and Analyses of Cumulative Sum to Detect Highly Distributed Denial ofService attacks using Different Attack Transfer Prototypes", *1STINTERMON newsletter* issue 7, Feb 2004