IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 1, Feb-Mar, 2014
ISSN: 2320 - 8791
www.ijreat.org

DDOS Shield & Captcha Generation: Efficient Defending Mechanisms Of Dos Attack

Sunil.P[1], John Deva Prasanna[2]

[1]*PG Student Department of Computer Science, Hindustan University, Padur, Chennai, India.*

[2]*Assistant Professor Department of Computer Science, Hindustan University, Padur, Chennai India.*

Abstract-Application DoS attack, which aims at disrupting application service rather than depleting the network resource, has emerged as a larger threat to network services, compared to the classic DoS attack. Owing to its high similarity to legitimate traffic and much lower launching overhead than classic DDoS attack, this new assault type cannot be efficiently detected or prevented by existing detection solutions. To identify application DoS attack, we propose a novel group testing (GT)-based approach deployed on back-end servers, which not only offers a theoretical method to obtain short detection delay and low false positive/negative rate, but also provides an underlying framework against general network attacks. More specifically, we first extend classic GT model with size constraints for practice purposes, then redistribute the client service requests to multiple virtual servers embedded within each back-end server machine, according to specific testing matrices. Based on this framework, we propose a two-mode detection mechanism using some dynamic thresholds to efficiently identify the attackers. The focus of this work lies in the detection algorithms proposed and the corresponding theoretical complexity analysis. It also provides preliminary simulation results regarding the efficiency and practicability of this new scheme. Further discussions over implementation issues and performance enhancements are also appended to show its great potentials.

KEYWORDS: dos attack, ddos shield, captcha, virtual server.

1. Introduction

Tremendous growing of internet in almost every field of work such as industrial, educational, military etc. Based on the use, its security needs differ. Few applications may need less security and few may need high security. Today various internet attacks are being developed every day, such as dos attack, where client will directly interact with server in order to acquire some services from the server, so there is a possible of dos attack here, in order to prevent this type of attack we are proposing two types of techniques called ddos shield and captcha generation. DDoS shield and captcha-based defense are the representatives of the two major techniques of system-based approaches: session validation based on legitimate behavior profile and authentication using

Human-solvable puzzles. By enhancing the accuracy of the suspicion assignment for each client session, DDoS shield can provide efficient session schedulers for defending possible DDoS attacks. However, the overhead for per-session validation is not negligible, especially for services with dense traffic.

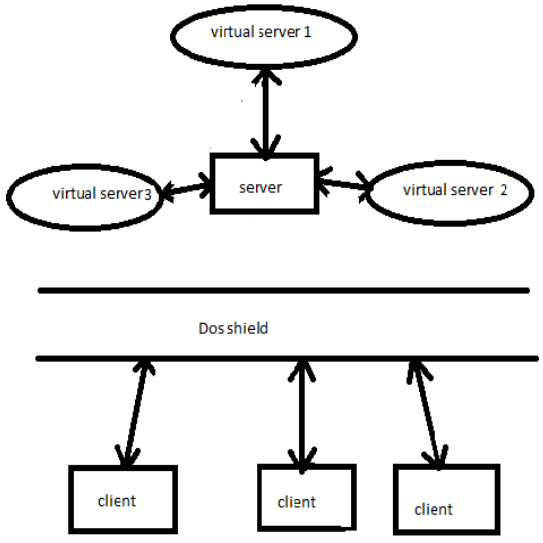
2. Related work

Learning from the previous works as described in M.T. Thai, Y. Xuan, I. Shin, and T. Znati, "On Detection of
Malicious Users Using Group Testing Techniques," Proc. Int'l
Conf. Distributed Computing Systems (ICDCS), in this paper the author proposed some group based testing techniques in order to detect authorized users in the different networks. S.Vries, "A Corsair White Paper: Application Denial of Service
(DoS)Attacks,
040405-application-level-dos-attacks.pdf, described different type of application dos attacks and reasons to attack the system. S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, "DDos-
Resilient Scheduling to Counter Application Layer Attacks under
Imperfect Detection. J. Mirkovic, J. Martin, and P. Reiher, Taxonomy of DDoS
Attacks and DDoS Defense Mechanisms. in order to protect the servers from different types of attacks here we are concentrating mainly on dos attack which mainly deals with the servers, resources and clients so based on different surveys made and concluded that to design an intermediate system between client and server in order to avoid the dos attack by using
Different types of techniques like ddos shield and captcha generation.

3. Proposed system

A novel group testing (GT)-based approach deployed on back-end servers, which not only offers a theoretical method to obtain short detection delay and low false positive/negative rate, but also provides an underlying framework against general network attacks. More specifically, we first extend classic GT model with size constraints for practice purposes, then redistribute the client service requests to multiple virtual servers embedded within each back-end server machine, according to specific testing matrices. Based on this framework, we propose a two-mode detection mechanism using some dynamic thresholds to efficiently identify the attackers. DDoS shield and CAPTCHA-based defense are the representatives of the two major techniques of system-based approaches: session validation based on legitimate behavior profile and authentication using human-solvable puzzles. By enhancing the accuracy of the suspicion assignment for each client session, DDoS shield can provide efficient session schedulers for defending possible DDoS attacks. CAPTCHA-based defenses introduce additional service delays for legitimate clients and are also restricted to human interaction services. This method only counts the number of incoming requests rather than monitoring the server status, it is restricted to defending high-rate DoS attacks and cannot handle high-workload ones. The system architecture is classified into four parts they are node details declaration, server creation, server monitoring, and captcha generation.

System architecture



3.1. Node details declaration:

In node details declaration, the node is register to network topology. That is specified the node IP address, Port Number and status. Node login to the network topology while it check the user authentication Then only server system, allows the node in to the transmission .Node can send the packets to the destination or otherwise can send to server system. Node can add and relive is very easy in the network. Status also monitory server system.

3.2. Server creation:

In server creation, the centralized server system design for whole network. It has one centralized database and collects the details of each node. And store in to the centralized database. Server maintains these details, it very useful for node calculation and node details identification. Server can receive the request from all clients and the provide the corresponding response.

3.3 .server monitoring:

In Server Monitoring, describe the Server monitoring, In Server monitoring if have any problem in network it will be take the action. The action is particular packet is discard and also the particular node details collect from database then that particular node remove from the network. Server system can identify the node v\by using the capuche. Monitoring process also detect the attacker node in the whole network. Monitoring result also store in the server side.

3.4. Captcha generation:

In Captcha generation, each request notified by using this unique captcha. This captch unique for all system. Captcha has two parts one is node id and another one is process id. Each node has the node id as node name and port number combination. And each Process id started from the process name and combine with process count. It used for identify the node and type of process from DOS attacking node.

4. Conclusion

By using the two proposed group based testing techniques ddos shield and captcha generation up to the maximum extent we can reduce the dos and ddos attack from the unauthorized users and network resources can be prevented from the attackers.

5. References

[1] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, "DDos-Resilient Scheduling to Counter Application Layer Attacks under
Imperfect Detection," Proc. IEEE INFOCOM, Apr. 2006.

[2] S. Vries, "A Corsaire White Paper: Application Denial of Service (DoS) Attacks," http://research.corsaire.com/whitepapers/ 040405-application-level-dos-attacks.pdf, 2010.

[3] S. Kandula, D. Katabi, M. Jacob, and A.W. Berger, "Botz-4-Sale:
Surviving Organized DDoS Attacks That Mimic Flash Crowds,"
Proc. Second Symp. Networked Systems Design and Implementation
(NSDI), May 2005.

[4] S. Khattab, S. Gobriel, R. Melhem, and D. Mosse, "Live Baiting for Service-Level DoS Attackers," Proc. IEEE INFOCOM, 2008.

[5] M.T. Thai, Y. Xuan, I. Shin, and T. Znati, "On Detection of Malicious Users Using Group Testing Techniques," Proc. Int'l Conf. Distributed Computing Systems (ICDCS), 2008.

[6] J. Mirkovic, J. Martin, and P. Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms,"TechnicalReport020018, Computer Science Dept., UCLA, 2002.

[7] M.J. Atallah, M.T. Goodrich, and R. Tamassia, "Indexing Information for Data Forensics," Proc. Int'l Conf. Applied Cryptography and Network Security (ACNS), pp. 206-221, 2005.

[8] F. Kargl, J. Maier, and M. Weber, "Protecting Web Servers from Distributed Denial of Service Attacks," Proc. 10th Int'l Conf. World Wide Web (WWW '01), pp. 514-524, 2001.

[9] J. Kurose and K. Ross, Computer Networking: A Top down Approach, fourth ed. Addison-Wesley, July 2007.