International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 9: September 2015, pp 40-42. www.aetsjournal.com ISSN (Online) : 2394-6237

Preventing the Low-Rate Dos Attacks in Web Server Using Router Based Firewall

J. Prasanth , T. Prem Kumar , M.S. Vidya Sagar , R.Elakiya

Abstract**—** The Quality of Service is the main feature of Internet services. To fault these services of the web server or a website, the attacker uses a Denial of Service (Dos) attack and these Dos attacks nowadays can be easily detected using many attack detection tools. The Low-rate Denial of service (LRDoS) attacks are a new type of Dos attacks that sends high intensity requests in an ON/OFF pattern to degrade victim's performance and evade the detection designed for traditional DoS attacks. It is more difficult for traditional DoS attack detection method to detect LRDoS attack. The existing system analyze only the impact of LRDoS attack on a affected system and the existing detection method focus only on TCP related system. A live firewall is managed in our proposed system to monitor all the invoking requests and IP address of the attackers. The Particle Swarm Optimization technique is combined with Genetic algorithm and Priority scheduling concept to produce Classification rules. The Router based Firewall use these rules and IP address of the client to filter the LRDoS attack.

Keywords**—** Denial of Service (DoS), Distributed Denial of Service(DDoS), Low Rate Denial of Service (LRDoS), Transmission Control Protocol (TCP), Particle Swarm Optimiser (PSO).

I. INTRODUCTION

Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks can bring down an Internet service, by flooding the high amount of request to the web server.DoS attacks send out high-volume requests to the victim.An adversary bent on limiting access to a network can bring down an Internet service by subjecting it to sustained levels of demand that far exceed its capacity, making that service incapable of adequately responding to legitimate requests. The Quality of Service is the main feature of Internet services. To fault these services of the web server or a website, the attacker uses a Denial of Service (Dos) attack and these Dos attacks nowadays can be easily detected using many attack detection tools. Although DoS attacks can inflict significant damage, preparing a DoS attack requires some additional work. In particular, it requires recruiting enough zombie clients to launch the attack. These zombie clients are typically compromised computers scattered all over the Internet. Moreover, just by their brute force nature, these attacks are easily exposed, making it possible for appropriate countermeasures to be taken once attacks are detected. LRDoS attacks send out intermittent (instead of continuous) high-volume requests. It forces the victim away from the desired state, thus deteriorating its performance. Moreover, LRDoS attacks can escape the detection designed for flooding-based DoS attacks because of their ON/OFF traffic patterns.The Low-rate Denial of service (LRDoS) attacks are a new type of Dos attacks that sends high intensity requests in an ON/OFF pattern to degrade victim's performance and evade the detection designed for traditional DoS attacks. It is more difficult for traditional DoS attack detection method to detect LRDoS attack. The existing system analyzes only the impact of LRDoS attack on an affected system and the existing detection method focus only on TCP related system. A live firewall is managed in our proposed system to monitor all the invoking requests and IP address of the attackers. The implementation is done by using Particle Swarm Optimizer (PSO) combined with Genetic algorithm and Priority Scheduling. This produces the Classification rules. The Firewall uses these rules and IP address of the client to filter the LRDoS attack and thus defends the LRDoS attacks.

J. Prasanth , T. Prem Kumar , M.S. Vidya Sagar , UG Scholars, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.
R.Elakiya , Assistant Professor of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai

II. RELATED WORK

DDoS attacks drain bandwidth or system resources to preventnormal users from receiving quality of service. Traditional flood-based attacks can be easily detected because of their continuously high sending rates. In contrast, LRDoS attacks have polymorphic traffic patterns and low average sending rates.

A. Low-Rate DoS Attacks

LRDoS attacks were first proposed to throttle the throughput of TCP connections by causing intermittent packetlosses. Zhang and Schuchard showed that an attacker can launch LRDoS attacks on BGPsessions for crippling the Internets control plane. Recently,researchers examined the vulnerability of other applicationsto LRDoS attacks, including Internet services, load balancers, wireless networks, and peer-to-peernetworks. Guirguis found that an LRDoS attack can force a feedback control system to oscillate between the desired state and another state, and analyzed the effect of such attack on a web server. Guirguis described the possibility of launching the LRDoS attack on a feedback-control based system. We formally show that the LRDoS attack can compel a feedback control system to stay at a state other than the desired state by proving that thesystem under attack is *Lyapunov* and *Lagrange* stable. A novel methodology is used to systematically evaluatethe impact of an LRDoS attack on specific systems. Thismethodology enables us to obtain many *new* insights that arenot reported before. Guirguisonly examined the third type of LRDoS attack.Moreover,we thoroughly analyze each type of LDRoS attack, includinggiving closed-form expressions for the throttled admissionrate, determining the conditions under which the LRDoS attackwill make the web server Lyapunov and Lagrange stable,deciding the bound of the system's state and the relationshipbetween the bound and the LRDoS attack, and identifying therelationship between the damage caused by an LRDoS attackand its cost.

B. Defending Against LRDoS

As LRDoS attacks have ON/OFF traffic patterns, they canevade detection schemes targeting flooding-based DoS attacksand therefore have motivated the design of new detectionapproaches. However, these approachescannot be directly used to detect LRDoS attacks against Internetservices for two reasons. First, as all of these approachesaim at LRDoS attacks targeting TCP or other systems (e.g.,wireless networks, P2P networks, etc.), they rely on featuresspecific to TCP and those systems. For example, we proposedthe detection of anomalies in incoming TCP data traffic andoutgoing TCP ACK traffic. Shevtekar regardeda TCP flow as malicious if its period is equal to the fixedminimal RTO and its burst length is no less than other connections'RTTs. To detect LRDoS attacks using spoofedIP addresses, Shevtekar . captured anomalies that shortlivedflows occupy a high percentage of the total traffic goingthrough a link. We proposed a new metric named thecongestion participation rate (CPR) to infer attack flows thattry to send more packets during congestion. To detectdistributed LRDoS attacks, Xiang used generalizedentropy and information distance to quantify anomalies inpackets, and required the control of all routers in the network.However, the detection of LRDoS attacks aimed at Internetservices requires new metrics.Second, the majority of the previous work focuses on theShrew attack that has a fixed attack period equal to TCP'sminimal RTO. However, LRDoS attacks can changetheir attack periods for mimicking normal flows. Sunsuggested using autocorrelation and dynamic time warping(DTW) to detect Shrew attacks, because their traffic burstsare the same and have fixed periods. However, it isunnecessary for LRDoS attacks to have invariable periods andsimilar attack pulses.

C. Particle Swarm Optimisation

Particle swarm optimization (PSO) is a computational method that optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measure of quality. PSO optimizes a problem by having a population of candidate solutions, here dubbed particles, and moving these particles around in the search-space according to simple mathematical formulae over the particle's position and velocity. Each particle's movement is influenced by its local best known position but, is also guided toward the best known positions in the search-space, which are updated as better positions are found by other particles. This is expected to move the swarm toward the best solutions. The algorithm was simplified and it was observed to be performing optimization. PSO is a metaheuristic as it makes few or no assumptions about the problem being optimized and can search very large spaces of candidate solutions. However, metaheuristics such as PSO do not guarantee an optimal solution is ever found. More specifically, PSO does not use the gradient of the problem being optimized, which means PSO does not require that the optimization problem be differentiable as is required by classic optimization methods.

III. SYSTEM REALISATION

A. Existing Approach

The present system focus towards the DOS attack by providing the feedback controller in the mid of the data access.The Prediction of client access and the timing difference between the data access arise from the specific client provides a notable portion of analysis by the server.In this case, the server invokes the proxy site which is considered as the feedback controller which can take care of reducing the rate of DOS attack.The feedback controller will take care of evaluating the robot access or human access followed by reducing the DOS attack by prioritizing the direct request from the client to the website when compared to the request coming in from the feedback controller page. The drawbacks of the present system are:1)The LRDoS attacks cannot force the system's state error to oscillate along with the attack.2)The LRDoS attack can be sent out continuously,to drive the system to a state other than the desired state.3)There is no precautions to block the LRDoS attacks on a feedback control system.

B. Proposed Approach

We present the design and implementation of an automated system that performs specific instruction execution management on LRDOS attacks. A website is managed in our proposed system which involves Monitoring of invoked requests and automating redirection of temporary feedback controlled sites for Low Rate DOS.Restricting the High privilege instruction executable users from further accessing on the server.The implementation provides more priority to the direct access users when compared to the request received through proxy feedback controlled users. LRDOS attack is one of the most vulnerable attack through which users can send attacks in ON/OFF patterns. To overcome the above penetration, our proposed system focuses towards avoidance of multiple feedbacks from a same proxy in a particular piece of time.The LRDoS attacks can force the system's steady-state error to oscillate along with the attack. The existence of a LRDoS attacks can be intermittent, to drive the system to a state other than the desired state. We implement firewall to block the LRDoS attacks on a feedback control system.

The Particle Swarm Optimization technique is combined with Genetic algorithm and Priority scheduling concept to produce Classification rules. This Firewall uses these rules and IP address of the client to filter the LRDoS attack.

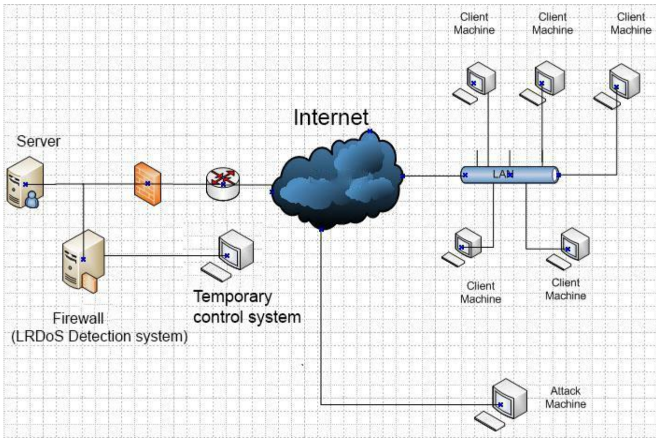

Fig 3.1 LRDoS Detection Mechanism

IV. IMPLEMETATION

A. LRDoS Attacker

The LR-DoS attack tool will first connect to the database of the feedback form and acquire the ip address. Then we will input the url address of the website of the feedback form to input the n number of comments to the feedback database. By providing these false data, the admin and the user will be totally disturbed and various false data may lead to the in quality product and the trust worthiness of the website will be in danger. Thus the user will pose a unworthiness of the website and may degrade the website .By using the LRDoS tool ,the website steady state will be disturbed and random feedback will be entered into the module while the feedback will be sent according to the connection type.

B. Defending the LRDoS Attack

The detection of LRDoS attack is done by managing a live firewall. It monitors the invoked request and IP address of the user. Thusrestricting the High privilege instruction from further accessing on the server. This avoids multiple feedbacks from a same proxy in a particular piece of time. This implementation is done by using Particle Swarm Optimiser(PSO) combined with Genetic algorithm and Priority Scheduling. This produces the Classification rules. The Firewall uses these rules and IP address of the client to filter the LRDoS attack and thus defends the LRDoS attacks.

V.CONCLUSION

We investigate the vulnerability of Internet services to the LRDoS attacks. We first examine the impact of the LRDoS attacks on a web server and prove that LRDoS attacks can damage the web server and causes loss of time and data. Our methodology proves as an efficient mechanism to defend the LRDoS attacks on specific servers by managing a live firewall and mitigating its impacts. In future work, the system can be upgraded by enhancing the security provided by the firewalls.

REFERENCES

[1] Yajuan Tang, Xiapu Luo, Qing Hui, and Rocky K. C. Chang,” Modeling the Vulnerability of Feedback-ControlBased Internet Services to Low-Rate DoS Attacks”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 3, MARCH 2014
[2] H. Lim, S. Babu, J. Chase, and S. Parekh, “Automated control in cloudcomputing: Challenges and opportunities,” in Proc. 1st Workshop ACDC,Jun. 2009.
[3] A.Sharifi, S. Srikantaiah, A. Mishra, M. Kandemir, and C. Das, “METE: Meeting end-to-end QoS in multicores through system-wide resource management,” ACM SIGMETRICS Perform. Eval. Rev., vol. 39, no. 1,p. 13–24, Jun. 2011.
[4] Z.Wang, Y.Chen, D.Gmach, S.Singhal, B.Watson, W.Rivera, et al., “AppRAISE: Application-level performance management in virtualized server environments,” IEEE Trans. Netw. Service Manag., vol. 6, no. 4, pp. 240–254, Dec. 2009.
[5] Kai Chen, Huiyu Liu, Xiaosu Chen,” A Real-time Detection Method of LDoSBased on Shewhart ControlChart DetectionTheory”, The 2nd International Conference on Computer Application and System Modeling (2012)
[6] WU Zhijun, CUI Yi, YUE Meng, MA Lan, and WANG Lu,” Cross-correlation Based Synchronization Mechanism of LDDoS attacks”, JOURNAL OF NETWORKS, VOL. 9, NO. 3, MARCH 2014
[7] Yang Xiang, Member, IEEE, Ke Li, and Wanlei Zhou,” Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011
[8] Changwang Zhang, ZhipingCai, Weifeng Chen, XiapuLuo, Jianping Yin,” Flow level detection and filtering of low-rate DDoS”, Computer Networks 56 (2012) 3417–3431
[9] Ying Zhang, Z. Morley Mao, Jia Wang,” Low-Rate TCP-Targeted DoS Attack Disrupts Internet Routing”
[10] G. Loukas and G. Oke, “Protection against denial of service attacks: Asurvey,” Comput. J., vol. 53, no. 7, pp. 1020–1037, 2010.
[11] Y. Xiang, K. Li, and W. Zhou, “Low-rate DDoS attacks detection andtraceback by using new information metrics,” IEEE Trans. Inf. ForensicsSecurity, vol. 6, no. 2, pp. 426–437, Jun. 2011.
[12] W. Haddad, V. Chellaboina, and S. Nersesov, Impulsive and Hybrid Dynamical Systems: Stability, Dissipativity, and Control. Princeton, NJ, USA: Princeton Univ. Press, 2006.
[13] S. Parekh, N. Gandhi, J. Hellerstein, D. Tilbury, T. Jayram, and J. Bigus, “Using control theory to achieve service level objectives in performance management,” Real-Time Syst., vol. 23, nos. 1–2, pp. 127–141, 2002.
[14] [14] J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” ACM SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39–53, 2004.
[15] T. Peng, C. Leckie, and K. Ramamohanarao, “Survey of network-based defense mechanisms countering the DoS and DDoS problems,” ACM Comput. Surv., vol. 39, no. 1, pp. 1–3, 2007.
[16] G. Loukas and G. Oke, “Protection against denial of service attacks: A survey,” Comput. J., vol. 53, no. 7, pp. 1020–1037, 2010.
[17] X. Luo, E. Chan, and R. Chang, “Vanguard: A new detection scheme for a class of TCP-targeted Denial-of-service attacks,” in Proc. 10th IEEE/IFIP NOMS, Apr. 2006, pp. 507–518.
[18] Y. Zhang, Z. Mao, and J. Wang, “Low-rate TCP-targeted DoS attack disrupts internet routing,” in Proc. NDSS, 2007, pp. 1–15.
[19] M. Schuchard, A. Mohaisen, D. Kune, N. Hopper, Y. Kim, and E. Vasserman, “Losing control of the internet: Using the data plane to attack the control plane,” in Proc. NDSS, 2011, pp. 1–15.
[20] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, “Reduction of quality (RoQ) attacks on dynamic load balancers: Vulnerability assessment and design tradeoffs,” in Proc. 26th IEEE Int. Conf. Comput. Commun., May 2007, pp. 857–865.
[21] W. Chen, Y. Zhang, and Y. Wei, “The feasibility of launching reduction of quality(RoQ) attacks in 802.11 wireless networks,” in *Proc. 14th IEEE ICPADS, Dec. 2008, pp. 517–524.*
[22] Y. He, Q. Cao, Y. Han, L. Wu, and T. Liu, “Reduction of quality (RoQ) attacks on structured peer-to-peer networks,” in *Proc. IEEE IPDPS, May 2009, pp. 1–9.*