Survey On Detection Of Low Rate Denial Of Service Attack

Sujatha P, Kalaivani J

ABSTRACT— **Feedback control is the essential building block of many internet services. The performance controller act as the basic example in the web server. It adjusts the server's configuration inn response to alteration between the current and desired states for meeting expected performance. Feedback control act as a crucial element in the QoS software. Low Rate Denial of Service is the attack where the attacker will make suspicious request by initiating bulk of same URL request to the web proxy and he will force the web proxy to forward those requests to origin server. It degrades the performance of the server thereby prevents the legitimate user from using the service. Using the switched system concept the attacker is detected and blocked temporarily. This paper delivers a survey about the switched system allowing legitimate users to access the service.**

Key words— **Low Rate Denial of Service, Switched system, Feedback Control - based system, Web server, Steady- state error.**

IINTRODUCTION

As the Internet Technology is emerging day by day, all people wish to make their work simple using it. There are lots of services available in the internet like Transaction processing service, Ordering service, Online purchasing service, Online ticket reservation service, etc., Though the number of services increases the level of attacks also increases. The attacks are actually carried out by the attackers (Hackers) in order to degrade the performance of the system as well as to diminish the name and fame of the organization. One of the major attacks which prevent the service from legitimate users is Low Rate Denial of Service (LRDoS) attack. It is actually sent by the attacker in the ON/OFF pattern to the target system, so that the organization or owner of the service may unable to detect and block them. The attacker will send large number of same request from same source to the target or destination to degrade the performance of the system. To reveal the vulnerability of feedback-control based to the LRDoS attacks through theoretical analysis and then we implement a new theory to quantify the impact of the LRDoS attacks. Thus the objective of this paper is to detect the attackers and block them temporarily using the Switched system concept. This methodology is applied to two specific systems: The web server and the feedback-control based IBM Notes server. Switched system is a hybrid system composed of several subsystems and a switching law that indicates the sequence of subsystems. Whenever the attacker tries to attack the system, with the help of switched system technique the attacker is identified and then blocked temporarily. Thus enabling only the legitimate user to access the service. With the help of the web server the attacks are detected. The "switched system" concept is implemented in "Online ticket reservation service". It is used to detect the Low rate Denial of Service attacks (LRDoS). It models under attack with a switched system.An LRDoS attack needs to predict the time instants. It detects the attacks like LRDoS.

IILITERATURE SURVEY

The survey is about detection of various forms of Low Rate Denial of Service attacks. [1] Describes the investigation of a class of low-ratedenial of service attacks. It is different from other High Rate attacks. Using a combination of analytical modeling, simulations and Internet experiments, the maliciously chosen low-rate DoS traffic patterns that exploit TCP's retransmission time-out mechanism can throttle TCP flows to a small fraction of their ideal rate while eluding detection. In this paper, we study low-rate DoS attacks, which we term "shrew attacks". The author present background on TCP's retransmission timeout (RTO) mechanism. TCP detects loss via either timeout from non-receipt of ACKs, or by receipt of a triple-duplicate ACK. The impact of TCP flow aggregation and heterogeneity on the effectiveness of the shrew attack. Two classes of candidate counter-DoS mechanisms are intended to mitigate the effects of shrew attacks: (a) router-assisted, and (b) end-point mechanisms. The effectiveness of low-rate DoS attacks depends critically on the attacker's ability to create correlated packet losses in the system and force TCP flows to enter retransmission timeout. This paper presents denial of service attacks that are able to throttle TCP flows to a small fraction of their ideal rate while transmitting at sufficiently low average rate to elude detection. It is showed that(1) low-rate DoS attacks are successful against both short- and long-lived TCP aggregates and thus represent a realistic threat to today's Internet; (2) in a heterogeneous-RTT environment, the success of the attack is weighted towards shorter-RTT flows; (3) low-rate periodic open-loop streams, even if not maliciously generated, can be very harmful to short-RTT TCP traffic if their period matches one of the null TCP frequencies; and (4) both network-router and end-point-based mechanisms can only mitigate, but not eliminate the effectiveness of the attack. [2] Describes the discoveries and studies of new instances of Reduction of Quality (RoQ) attacks that target the dynamic operation of load balancers. The exposition is focused on a number of load balancing policies that are either employed in current commercial products or have been proposed in literature for future deployment. Through queuing theory analysis, numerical solutions, simulations and Internet experiments, we are able to assess the impact of RoQ attacks through the potency metric. The key factors, such as feedback delay and averaging parameters, that expose the trade-offs between resilience and susceptibility to RoQ attacks are identified. These factors could be used to harden load balancers against RoQ attacks. To the best of our knowledge, this work is the first to study adversarial exploits on the dynamic operation of load balancers.RoQ attacks are a relatively new breed of attacks that target adaptation mechanisms with the premise to hinder an adaptive component from converging to steady-state. Load balancers are integrated in the design of most scalable and distributed applications and services. Typically, they are embedded as part of the infrastructure supporting these applications and services—*e.g.,* as part of routers and network switches, routing protocols, firewalls and traffic shapers, HTTP and database server farms, among others. The feedback delay inherent in the design of any dynamic load balancer constitutes the "Trojan Horse" through which a RoQ attack would be mounted. The new vulnerabilities are exposed that is associated in the operation of dynamic load balancers against new instances of RoQ attacks. The impact of RoQ attacks has been assessed based on factors, such as the number of resource managed, the feedback delay and the averaging parameters. [3] The author innovatively propose using two new information metrics such as the generalized entropy metric and the information distance metric to detect low-rate DDoS attacks by measuring the difference between legitimate traffic and attack traffic. The proposed generalized entropymetric can detect attacks several hops earlier than the traditional Shannon metric. The proposed information distance metric outperforms the popular Kullback–Leibler divergence approach as it can clearly enlarge the adjudication distance and then obtain the optimal detection sensitivity. The Distributed Denial of Service (DDoS) attack typically exhausts bandwidth, processing capacity, or memory of a targeted machine or network. A DDoS attack is a distributed, cooperative and large-scale attack. An attacker can use botnets to launch a low-rate DDoS attack, producing network behavior that appears normal. Therefore, it is difficult to detect andmitigate such attacks [4]. DDoS attack detection metrics are mainly separated into two categories: the signature-based metric and anomaly-based metric. The signature-based metric depends on technology that deploys a predefined set of attack signatures such as patterns or strings as signatures to match incoming packets. The anomaly-based detection metric typically models the normal network (traffic) behavior and deploys it to compare differences with incoming network behavior. The two effective detection algorithms and an IP trace back scheme are proposed. In this paper, the author makes the following reasonable assumptions: 1) Having full control of all the routers; 2) Having extracted an effective feature of network traffic (e.g., the unforged source IP addresses) to sample its probability distribution; 3) Having obtained and stored the average traffic of the normal, as well as the local thresholds and on their own routers in advance; 4) On all routers, the attack traffic obeys Poisson distribution and the normal traffic obeys Gaussian noise distribution. The IP trace back analysis [5] is the ability to find the source of an IP packet without relying on the source IP field in the packet, which is often spoofed. The author combines the DDoS attacks detection metric with IP traceback algorithm and filtering technology together to form an effective collaborative defense mechanism against network security threats in Internet. In hop-by-hop IP tracing, the more hops the more tracing processes, thus the longer time will be taken. In order to convenience for IP trace back algorithm analysis. The proposed metrics can increase the information distance (gap) between attack traffic and legitimate traffic, they can effectively detect low-rate DDoS attacks early and reduce the false positive rate clearly. The proposed information distance metric overcomes the properties of asymmetric of both Kullback–Leibler and information divergences. [6] The author describes about the batch scheduling has dominated the management of High Performance Computing (HPC) resources. One of the most significant limitations using this approach is an inability to predict both the start time and end time of jobs. Although existing research such as resource reservation and queue-time-prediction partially address this issue, a more predictable HPC system is needed, particularly for an emerging class of adaptive real-time HPC applications. In this paper the author presents a design and implementation of a predictable HPC system using feedback control and admission control.

By creating a virtualized application layer and opportunistically multiplexing concurrent applications through the application of formal control theory, we regulate a job's progress such that the job meets its deadline without requiring exclusive access to resources even in the presence of a wide class of unexpected events. Admission control regulates access to resources when oversubscribed. Our experimental results using five widely used applications show the feedback and admission controller achieves highly predictable HPC system. The designed feedback controller regulates the HPC job's progress accurately, close to the prediction by theory, thereby showing the successful application of classic control theory to HPC workloads. In week-long experiments, over 90% of jobs met deadlines and the jobs missing deadlines still finished close to the requested deadlines (12.4% error). Real-time data-driven applications have emerged, often using scientific modeling and high performance computing (HPC) to directly support mission-critical decision making. For example, people explore if weather forecasting infrastructure can be transformed to an adaptive one that can predict me-so scale weather events such as tornadoes in real-time [7]. Similarly, coastal hazard prediction attempts to predict the impact of storm surge in real-time to dynamically facilitate life-saving decisions such as evacuation orders [8]. In medical applications, clinicians would use simulation results on patient-specific data to diagnose and treat patient‗s medical problems [9]. Their common properties include that 1) there is a chain of application components where, 2) the in-field sensors generate real-time data at unpredictable cycles, 3) the high-bandwidth networks transport sensor data to computational sites, 4) the long-running simulation codes are invoked with the data, and 5) optionally the simulation‗s results guide the next course of actions to the sensors. It is an adaptive application since the entire loop including sensors and simulations should react to unpredictable changes in the field. They require deadline-guaranteed execution of long-running simulation codes, which is a challenging task to traditional HPC centers. The black-box modeling approach is used to establish a linear model in control theory, to derive the linear equation that models the relationship between provisioned resources and job‗s progress. The jobs instrumented with sensor library are run with varying credit values, and the changes in CPU allocation (C (k)) and job‗s measured progress (P (k)) are used to create linear model via least-square regression. The feedback controller is equivalent to a virtual CPU that dynamically throttles its clock speed to keep the job‗s progress at a target goal. After determining the ranges, the algorithm computes settling time and maximum overshoots and stores the computed values to tables. Finally, the rank function chooses the best candidates for gain and zero by examining the tables. In the author's implementation, he uses simple rank function that finds the zero-gain pair achieving the shortest settling time while maximum overshoot is subject to a fixed thresholds.

III CONCLUSION

In this paper we propose a new system called "switched system". Firstly we allow users to login which is stored in the Relational Database (RDBMS). Then using our new system we separate the legitimate users and suspicious users. Then the suspicious user is blocked for certain time period then released. Using this technique we can avoid the degradation of system performance and can prevent the spoilage of name and reputation of the service providing organization. Meantime the legitimate users can access their required service. This technique is also applicable in areas like Social networks and Hospital management.

REFERENCES:

1. A. Kuzmanovic and E. Knightly, "Low-rate TCP-targeted Denial-ofservice attacks: The shrew vs. the mice and elephants," in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. Aug. 2003,
pp. 75–86.

2. M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of quality (RoQ) attacks on internet end-systems," in Proc. IEEE 24th Annu. Joint Conf. Comput. Commun. Soc., vol. 2. Mar. 2005, pp. 1362–1372.

3. Yang Xiang, Member, IEEE, Ke Li, and Wanlei Zhou, Senior Member, IEEE, "Low -Rate DDoS Attacks Detection and Trace back by Using New Information Metrics" IEEE HPCC 10/09.

4. A. Shevtekar, K. Anantharam, and N. Ansari, "Low rate TCP Denial-of-Service attack detection at edge routers," IEEE Commun. Lett. vol. 9, no. 4, pp. 363–365, Apr. 2005.

5. Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An IP trace back system to find the real source of attacks,"
IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 4, pp. 567–580, Apr. 2009.

6. S. Park and M. Humphrey, "Predictable high-performance computing using feedback control and admission control," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 3, pp. 396–411, Mar. 2011.

7. B. Plale, et al. Towards Dynamically Adaptive Weather Analysis and Forecasting in LEAD. ICCS workshop on Dynamic Data Driven Applications, Atlanta, Georgia, May 2005.

8. SURA Coastal Ocean Observing and Prediction (SCOOP):http://scoop.sura.org

9. M. Guirguis, A. Bestavros, I. atta, and Y. Zhang, "Exploiting the transients of adaptation for RoQ attacks on internet resources," in Proc. 12th IEEE ICNP, Oct. 2004, pp. 184–195.

10. X. Luo, R. Chang, and E. Chan, "Performance analysis of TCP/AQM under Denial-of-service attacks," in Proc. 13th IEEE Int. Symp. MASCOTS, Sep. 2005, pp. 97–104.

12. M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Adversarial exploits of end-systems adaptation dynamics," J. Parallel Distrib. Comput., vol. 67, no. 3, pp. 318–335, 2007.

13. Y. Seung, T. Lam, L. Li, and T. Woo, "Cloud Flex: Seamless scaling of enterprise applications into the cloud," in Proc. IEEE INFOCOM, Apr. 2011, pp. 211–215.

15. 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, pp. 13–24, Jun. 2011.

BIOGRAPHY

Ms.P.Sujatha Currently pursuing B.Tech, Information Technology at IFET College of Engineering, Villupuram, India. Her area of interests includes OOPS concepts, Cryptography and Data mining.

Ms.J.Kalai vani received her B.E in CSE from VRS College of Engineering and Technology, Villupuram and M.Tech in CSE from Manonmaniam Sundaranar University. She is currently working as Assistant Professor in Department of Information Technology, IFET College of Engineering, and Villupuram, India. She has published a book on Computer Graphics. She has published four papers in international journals. Her area of interests includes Computer Networks, Cryptography and Network Security and Computer Graphics.