International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Protection of Server from Proxy Based HTTP Attacks

Poonam Uttam Patil[1], Y. V. Chavan[2]

[1]Savitribai Phule Pune University, Padmabhooshan Vasantdada Patil Institute of Technology, Pune, Maharashtra, India
[2]Savitribai Phule Pune University, Padmabhooshan Vasantdada Patil Institute of Technology, Pune, Maharashtra, India

Abstract: ***With the increasing use of the web in last few decades, the numerous types of attacks have also been developed by miscreants. This is most commonly done by Hiding or spoofing IP address. This leads to make it hard and difficult to locate the actual attacker. A novel new defense scheme at server-side to resist the Web proxy-based Distributed Denial of Service (DDoS) attack which can be a better solution is reviewed here. Temporal and spatial locality (TSL) is used in this approach to extract the behavioral features of the traffic to server from the proxy. This will make the method independent of the traffic intensity and the increasingly unreliable web substances. Also a novel method to response the attack is projected in this paper. This method simply converts the suspicious packets into relatively normal packets, instead of just discarding those packets. The quality of service of authenticated users will be shielded by this technique.***

Keywords: Traffic analysis, traffic modeling, distributed denial of service (DDoS) attack, attack detection, attack response, temporal and spatial locality (TSL), Hidden semi-Markov Model (HsMM).

1. Introduction

From the last decade, the Distributed Denial of Service (DDoS) attacks have been an incremental threat to the internet. The implementations of these attacks are evolving and become bigger threat. The edge servers of content delivery networks (CDNs) to launch DDoS attacks to the web server, was utilized in a new attack pattern in [6]. Later a genuine alternative of these attacks was reported [19], the attacks were implemented, using various techniques [6] using the edge servers of CDNs. But using the web proxies that are deployed widely most of the existing attacks are less flexible and covert than the web proxy-based HTTP attack. The detection of this attack is difficult because:

1) The shield of the web proxies makes real attacker unobservable;
2) Unintentionally, a web proxy can become attacker or help attacker;
3) Legal and illegal traffic is received from identical source for a victim, which is a web proxy.

The large scale official proxies cannot avoid from being used for attacks even though they are configured for higher levels of securities. Due to this, the security in existing network is currently been challenged. Hence, in this paper, new resisting techniques are discussed for protecting the origin server from Web proxy-based HTTP attacks.

Network behavior analysis [3] is used as base in many techniques. A hidden semi-Markov model (HsMM) [1], [7] is mapped from the access behavior of a web proxy. This is general model with double stochastic processes. The observable varying process of a proxy-to-server traffic is outlined by the output process of the HsMM. The chain of an HsMM illustrates the transformation of internal behavior states of a proxy server. This method is capable of calculating a proxy-to-server traffic's intrinsic driving mechanism. Behavior model identifies the anomaly of a Web proxy. This can be attained by measuring the deviation between a watched behavior and the Web proxy's historical behavior profile. Long-term and short-term behavior evaluation systems are discussed. Long-term behavior appraisal issues warnings on a huge scale. Transient behavior evaluation places irregular solicitation groupings implanted in the proxy-to-server activity. Another "soft-control" plan is introduced for assault reaction. The plan reshapes the suspicious groupings as indicated by the profile of a proxy's historical behavior. It changes over a suspicious succession into a generally typical one. This can be achieved by halfway disposing of its doubtlessly vindictive demands as opposed to denying the whole grouping. In this way, it can ensure the HTTP requests of real clients to the best degree conceivable from being discarded. In summing up contrasted and the greater part of the current and past works [15], [16], the oddity of this work lies in:

1)It is centered around opposing Web proxy-based HTTP assaults and understands the early discovery without any participation of mid Web substitutes;
2)The methodology is free of movement power and much of the time changing Web substance. It has great dependability and need not every now and again overhaul model's parameters;
3)Long and short behavior evaluation strategies empower the multi-granularity determination. The "soft-control" plan can enhance the nature of administrations of normal users.

Though, enough research has been on done this topic, there is always a room for to do something new. Thus, it is necessary to study this topic in more details. The remaining paper is summarized as follows: Section II gives all the related work, that has been done previously in this field or using some similar techniques. The section III concludes the paper with some future works to done in further studies.

2. Literature Survey

Countering DDoS attacks has pulled in much consideration among the previous 10 years. There is only couple of steps, using which a web proxy can turn into an attacker. Firstly, an attacker needs to send attack requests to the web proxy server. Then attacker can force it to forward it to the victim. And second, attacker only needs to disconnect its connection with the proxy server, so that it cannot be identified. Customary resistance systems, for instance, [15], [18], concentrate on the network-layer DDoS attacks and utilization TCP and IP properties to find attack signals. The synopses of these techniques can be found in [11]. Since the HTTP-built DDoS attacks work with respect to the application layer and utilize another attack system, the traditional systems intended for the network-layer attack are no more relevant.

As of late, HTTP-based DDoS attacks have been accepting more consideration. In [2], customers are assessed by trust administration system, and Thereafter the application layer DDoS is relieved by offering need to great clients. In [13], the zombies are distinguished via consequently evolving riddle, and after that the HTTP requests of suspected hosts are blocked. A model introduced in [4], is used to profile the ordinary access conduct focused around four traits of web page appeal successions. The reproduction mistake of a given appeal arrangement is utilized as a basis for discovering DDoS attacks. In [10], the flow correlation coefficient was utilized to measure the comparability among suspicious flows, and after that the HTTP based DDoS attacks from ordinary blaze swarms were separated by the consequences of estimation. A traceback system was investigated for the DDoS attacks focused around entropy varieties in [9]. This scheme provides detection of source of attack, but not prevention to the attack.

In [15], client scanning conduct is connected to recognize the bizarre HTTP demands from those of ordinary clients. In [17], a multidimensional access framework is characterized to catch the activity conduct of glimmer swarms and discover HTTP attacks that copy or happen amid the blaze swarm occasion of a prominent Web webpage. In any case, the potential supposition of all these plans is that the attacking hosts are specifically joined with the victimized person server. Therefore, the victimized person server can recognize the movement propelled by diverse hosts. When a host's movement does not fit to the predefined rule of a given model, the protective framework will treat it as a suspect hub and piece its HTTP activity. Then again, a large portion of terminal hosts are protected by the various leveled Web-proxy framework in the real Web situation. Hence, the wellspring of an approaching HTTP solicitation saw by the exploited person server. It normally the last Web-proxy that interfaces with the exploited person server specifically and it can be confirmed by the victimized person server. Since it is troublesome for the cause server to induce the real wellspring of every HTTP appeal, opposing the attacks by conventional routines may diminish the nature of administrations of typical clients.

In [6], Triukose et al. imagined a way that attackers can use the edge servers of CDNs to dispatch HTTP-based DDoS attacks to source servers. Their solution improves the correspondence arrangements in the middle of CDNs and substance suppliers, and finally it enhances the forward procedure of edge servers of CDNs. Nonetheless, these arrangements are not suitable. Since practically all CDNs are business frameworks, content suppliers. So, it counsel with every CDN and setup secure correspondence arrangements. On the other hand, it is incomprehensible for a server to counsel with all Web substitutes (counting official and informal).

Proxy conduct and its abnormality identification were initially researched in [16]. Notwithstanding, its conduct model is not completely parametric and autonomous of movement power. The Hidden Markov Model (HMM) is an established methodology for displaying time arrangement with the suspicion that the concealed state procedure is a Markov chain. On the other hand, the state stay in the HMM is certainly thought to be steady or exponentially circulated, which restrains its viable application. Contrasted and the HMM, the discrete HsMM takes into account more general stay distributions, which make it generally connected in numerous territories, for instance, portability following, movement recognition, and induction for organized feature groupings [7].

Nonetheless, the established calculation [1] intended for the discrete HsMM is computationally excessively lavish to be of down to earth use in numerous applications [7]. In [5], state terms of the HsMM were initially parameterized by Gamma distribution. Be its principle downside is that the traditional Newton's strategy with second-request meeting is used to explain the parameters of Gamma-distribution. But its iterative union rate is moderate for extensive scale constant applications. Considering the constant prerequisite of oddity recognition, another iterative system focused around the Forward- Retrograde calculation [8] and eighth-request joining [12] is discussed in this paper.

3. Conclusion

In this paper, we attempted to channel the attack traffic from the collected proxy-to-server traffic, which is another issue for the DDoS recognition. A novel opposing plan was focused around TSL. Gaussian distributions and Gamma distributions HsMM (GGHsMM) multi-precision demonstrative strategy and soft-control were put forward for consideration to enhance the identification execution. Analyses affirmed the viability and heartiness of the given scheme. The fundamental preferences of given methodology indicated in the tests include:

1) Its recognition execution is superior to the pure statistical techniques;
2) It is independent of the traffic power and the as often as possible shifting Web substance;
3) It can understand the early discovery.

Additionally, the Detection Rate (DR), False Positive Rate (FPR), and the computational overhead can help a large portion of viable applications.

References

[1] J. Ferguson, "Variable Duration Models for Speech," Proc. Symp. Application of Hidden Markov Models to Text and Speech, 1980.
[2] J. Yu, C. Fang, L. Lu, and Z. Li, "Mitigating Application Layer Distributed Denial of Service Attacks via Effective Trust Management," IET Comm., 2010.
[3] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges", Computers and Security, 2009.
[4] S. Lee, G. Kim, and S. Kim, "Sequence-Order-Independent Net-work Profiling for Detecting Application Layer DDoS Attacks," EURASIP J. Wireless Comm. and Networking, 2011.
[5] S. Levinson, "Continuously Variable Duration HMM for Automatic Speech Recognition," Computer Speech and Language, 1986.
[6] S. Triukose, Z. Al-Qudah, and M. Rabinovich, "Content Delivery Networks: Protection or Threat?" Proc. 14th European Conf. Research in Comp. Security, 2009.
[7] S. Yu, "HsMM," Artificial Intelligence, 2010.
[8] S. Yu and H. Kobayashi, "An Efficient Forward-Backward Algorithm for an Explicit-Duration Hidden Markov Model", IEEE Signal Processing Letters, 2003.
[9] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS Attacks Using Entropy Variations," IEEE Trans. Parallel and Distributed Systems, 2011.
[10] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," IEEE Trans. Parallel and Distributed Systems, 2012.
[11] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems," ACM Computing Surveys, 2007.
[12] W. Bi, Q. Wu, and H. Ren, "A New Family of Eighth-Order Iterative Methods for Solving Nonlinear Equations," Applied Math. and Computation, 2009.
[13] X. Ye, W. Wen, Y. Ye, and Q. Cen, "An Otp-Based Mechanism for Defending Application Layer DDos Attacks," Applied Informatics and Comm., 2011.
[14] Y. Xiang, K. Li, and W. Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," IEEE Trans. Information Forensics and Security, 2011.
[15] Y. Xie and S. Yu, "A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors," IEEE/ACM Trans. Networking, 2009.
[16] Y. Xie and S. Yu, "Measuring the Normality of Web Proxies Behavior Based on Locality Principles," Network and Parallel Computing, 2008.
[17] Y. Xie and S. Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," IEEE/ACM Trans. Networking, 2009.
[18] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures," J. Network and Computer Applications, 2012.
[19] Z.L.C. Zhonghua and W. Xiaoming, "Research on Detection Methods of CC Attack," Telecomm. Science, 2009