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

Detection of Malicious Client based HTTP/DoS Attack on Web Server

Dhanya Jayan[1], Pretty Babu[2]

[1, 2]Sree Buddha College of Engineering, Alappuzha, Kerala, India

Abstract: A web server side defense system against the Http/DoS attack. The HTTP protocol 1.1 is mainly used to detect the malicious client based Http/DoS attack instead of proxy based Http/ DoS attack on web server. The main goals of the proposed system are accurate detection of malicious client based Http/DoS attack. Behavioral reshaping algorithm improves the quality of services of normal user. The performance of the system is based upon the false negative ratio.

Keywords: Malicious client, Http/DoS attack, HTTP protocol 1.1 web server.

1. Introduction

Proxy server is a server acts as an intermediary between client and server. Client send request to the proxy server, it forwards the request to the web server. Web server evaluates and processed the request and pass conforming responds to each client. Attackers break through the web proxy restrictions using attack browser program and launched the Http/DoS attack on web server shown in figure 1.

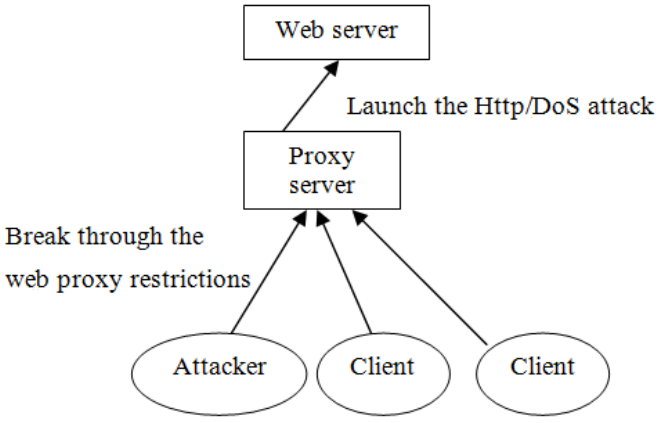

Figure 1: Http/DoS Attack.

Web server has no technique for detecting malicious client penetrate through the web proxies due to hidden information of attacker identity in the HTTP protocol 1.0. Web server cannot directly observe the terminal hosts shielded by the hierarchical web proxy. Traffic is mixed with the regular browser request and the attack browser request forward to web proxy then to the web server. The victim web server is rigid to precisely recognize and filter the attack requests. To protect the web server from the malicious client/browser based Http attacks is equivalent to filtering and grouping of suspicious request sequence from malicious client.

2. Related works

T. Peng et al. introduced traditional defense techniques for the detection of DDoS attack [1]. It uses TCP and IP properties to discover DDoS attack. Advantage of this system is defense mechanism against the DDoS. Limitation is HTTP based DDoS attacks work on the application layer and traditional defense techniques methods are no longer applicable for the detection of application layer DDoS attack and HTTP attack.

J. Yu et al. Introduce effective trust management for the detection of DDoS attack [2]. Clients are evaluated by trust management mechanism and give priority only to trusted users. For the detection of HTTP based DDoS attacks on web servers this defense system are not applicable.

S. Triukose et al. [3] discuss about the communication policies improving forward process of edge servers of content delivery network. Attackers can penetrates the protective shield of edge servers and utilize the edge servers of content delivery network to launch HTTP based DDoS attacks on web servers. Content providers can effectively protect themselves against this vulnerability by changing the setup of their content delivery network service. Limitation of this system is that the content providers can consult with each content delivery network and setup secures communication policies. It is impossible for a server to consult with all internets web proxies.

S. Lee et al. introduced a sequence order of web page requests can be used for detecting the application layer DDoS attack [4]. Reconstruction error of a sequence order of web page is used as a criterion for detecting DDoS attacks. The limitation of this system is the accuracy and efficiency of detecting the attack. Here web browser behavior of web proxy is not considered. It does not consider both temporal and spatial behavior of the web browser behavior for the detection of application layer DDoS attack through web proxy.

Y. Xie et al. introduced a server defense system against web proxy based HTTP attack [5]. Web proxy based HTTP attack is launched by utilizing the vulnerabilities of HTTP protocol. Malicious web request can be detected by only using locality behavior of web proxy. Behaviors access processes of web proxy mainly consist of both locality and spatial behavior for the accurate detection of http attack. The disadvantage of defense system is that it is not accurate to detect HTTP attack because it does not consider spatial behavior.

P. Garcia et al. introduced anomaly based IDS using hidden markov model [6]. A server defense system against web

Licensed Under Creative Commons Attribution CC BY

proxy based HTTP attack. The limitation of this system is the computational complexity of finding the parameters using markov models. Using hidden semi markov models some of the states are hidden. Due to the lack of whole information some of the attacks are undetected.

S. Yu et al. proposed a new server side detection scheme based on the behavior characteristics of proxy to server web traffic [7]. Proxy's access behavior is extracted from the temporal behavior. It is based on Gaussian mixtures hidden semi markov model is applied to describe the observed variables. The entropy of pending web traffics launched by proxies fit to the model is used as the criterion for attack detection. The limitation of this system is hidden state are present due to the lack of whole information some of the attacks are undetected.

Y. Xie and S. Yu discuss statistical approach defense against DDoS attacks [8]. The statistics of packet attributes in the headers of IP packets are measured and the packets dropped based on these measurements. In this system, challenge of detecting application layer DDoS attacks due to the malicious traffic to mimic the average request rate of the normal users or to produce the low rate attack flows. This makes detection more difficult. Capture the browsing patterns of web users the hidden semi-Markov model (HsMM) model is introduced for detection of the application DDoS attacks. The limitation of this system is hidden state are present due to the lack of whole information some of the attacks are undetected

Yi Xie et al introduced temporal and spatial locality behavior [9]. Proxy anomaly based behavior can be detected by comparing its current behavior with its historical behavior profile, detecting the distributed web proxy based HTTP attacks. TSL are exploited to extract the proxy to server behavior. Soft control was proposed to improve the detection performance. The defense system is use Gaussian-Gamma-Hidden-semi-Markov (GGHsMM) model used for the detection of web proxy based http attack. The disadvantage of this system is that the web server has no technique for identifying malicious client penetrate through the web proxies. Due to the lack of whole information some of the attacks are undetected and not accurate for the detection of Http/DoS attack.

3. Problem Statement

Provide security against Http/DoS attack. HTTP protocol version 1.0 comprise of certain state information are hidden, multiple connections and keep-alive connection allow multiple requests sent to same connection. Web server has no technique for detecting malicious client based Http/DoS attack on web proxy while using HTTP protocol 1.0. Detection of malicious client based Http/DoS attack on web server is main issue.

4. System design

The web server side defense system against the Http/DoS attack shown in the figure 2.

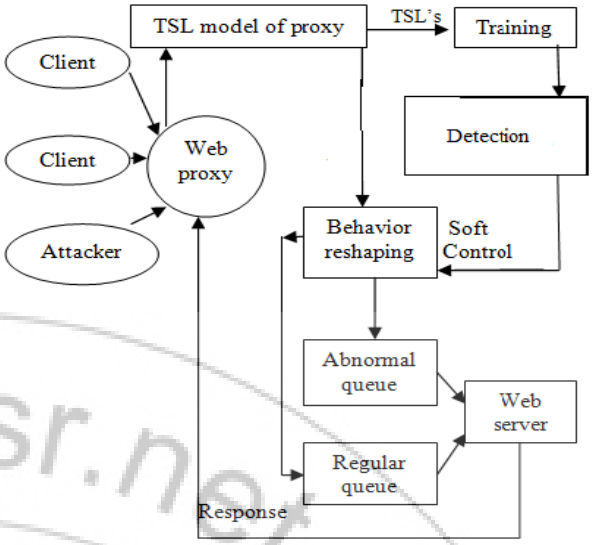

Figure 2: System design

Attacker and browser request are given to the web proxy. The web proxy receives the regular Http request along with the attack Http request is placed in the link list. Sequence of link list along with the index is passed to the TSL model of proxy. TSL model of proxy generates TSL pattern sequence and delivered to the training module for the detection of Http/DoS attack. Training module comprise two sub modules.

- Attack learning phase.
- Temporal & spatial behavior pattern identifier analysis phase.

Attack learning phase maintain an attack class. Http requests/packets are correctly classified as an attack type based on the parameter values. Attack class created based on the parameter values such as

- temporal_threshold.
- spatial_threshold.
- inter_spatial_threshold.
- min_length.
- min_inter_node_distance.
- min_inter_sequence_distance.
- threshold_value.

Adding extra parameter values such as unsupported HTTP method, oversized header and body data size, large or small time out interval, minimum incoming data, url path traversal, packet size, arrival rate and HTML inter arrival time (sequence order of same web page requests) also increase the accuracy of Http/DoS attack detection. In temporal & spatial behavior pattern identifier analysis phase incoming request are converted to term vectors.

In detection phase, detects Http/DoS attack by comparing term vector from temporal & spatial behavior pattern identifier analysis phase against each attack class parameter values from attack learning phase. Merge all Http requests of a specific attack type into separate_attack_sequences based on the parameter values. Decision rule are used to represent incoming Http request sequence into valid or invalid request. Separate_attack_sequences are considered as the abnormal

Licensed Under Creative Commons Attribution CC BY

Http request or invalid request or Http/DoS attack. Valid request sequences of Http requests are considered as non-attack type.

Web browser access behavior is also used for the detection of Http/DoS attack. Behavior of web proxy has both temporal and spatial behavior of the web browser. Hidden-semi-markov-model, the system in which observable states and hidden state are present, from these state estimates a threshold value using forward HsMM algorithm [10], [9] these threshold value is used for the detection of the anomaly behavior of web browser. Parameter values from attack learning phase and threshold value from forward HsMM are used for the accurate detection of Http/DoS attack.

Behavioral reshaping algorithm with soft control improves the quality of services (QoS) to normal user. The parameter values from attack learning phase are used to find out the attack_sequence. Using the parameter values, Http request are correctly classified into valid or invalid request sequence. Invalid requests are considered as attack_sequence are marked and grouped as separate_attack_sequences or suspicious request sequences. Discard all marked attack sequences.

Valid request from behavioral reshaping passed to the regular queue and separate_attack_sequences passed to the abnormal queue. It improves the quality of services of normal user. Web server response is passed to the proxy server. Proxy servers forward it to the consistent client. Web server side defense system provides security against http attack /DoS attack.

5. Implementation

Existing HTTP protocol 1.0 comprise of hidden state information, multiple connections and keep-alive connection allow multiple request sent to same connection [11]. Due to hidden state information and keep-alive connection, malicious client can send multiple requests sent to web server. These issues resolved by design and implement a new modified HTTP protocol version 1.1. Advantage of HTTP protocol 1.1 use persistent connections and pipelining [11] for the detection of malicious client based Http/DoS attacks. Due to persistent connections doesn't allow multiple request sent to same connection.

HTTP protocol 1.1 hidden states information are observable. HTTP protocol 1.1 inserts custom headers in HTTP protocol. These custom headers contain browser information initial from client to proxy server then to web server.

For example attacker send attack request using HTTP protocol 1.1. HTTP protocol 1.1 uses pipelining. Custom header of HTTP protocol 1.1 contains browser information preliminary from attacker IP address 192.168.0.8 and IP address of proxy server 192.168.0.27 shown in figure 3. Web server can identify which client sends the webpage request using machine_id (ip address). So web server can group each request from different client separately in the attack learning phase.

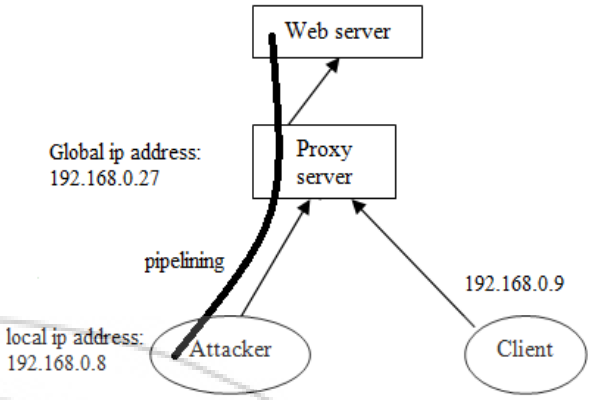

Figure 3: Malicious client based Http/DoS attacks

In detection phase/attack finder, detects Http/DoS attack by comparing term vector against each attack class using parameter values and checksum_id. Parameter values, machine_id and checksum_id are used for the accurate detection of Http/DoS attack.A request message from a client to a web server through proxy server includes request line and request header. The format of a request line is 'method' space 'request URL' space 'HTTP version'(example GET http://127.0.0.1:8000/home.html HTTP/1.1). For calculating the checksum_id using default MD5 algorithm in Java. It will overcome the disadvantage of high false negative ratio in existing system.

In behavioral reshaping algorithm attack_request_ sequence (example R1, R2, R3, R4 etc) is marked and grouped as separate_attack_sequences (R1, R2, R3, R4 webpage request can grouped into G1). Mark separate_attack_sequences (G1). Discard all marked request sequences. It improves the quality of services of normal user and accurate detection of malicious client based Http/DoS attack on web server.

6. Results

HTTP protocol 1.1 custom headers contain browser information from to proxy server (127.0.0.1) then to web server (8000 port) shown in figure 4.

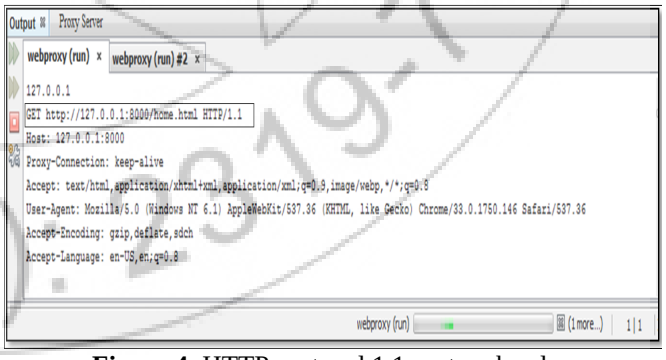

Figure 4: HTTP protocol 1.1 custom header.

Http request/packet is correctly classified as an attack based on the parameter values shown in the figure 5. The calculated term vector value is less than the parameter value, and then the Http request is an attack type.

Licensed Under Creative Commons Attribution CC BY

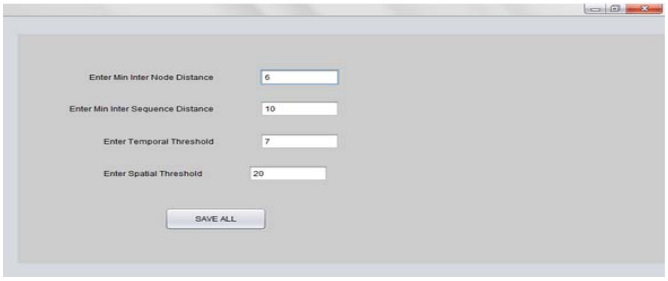

Figure 5: Parameter values setting

Performance of the detection system based upon the false positive and false negative ratio. False positive ratio is the no of attack_type minus no of non_attack_type divided by total no of requests. False negative ratio is the no of non_attack_type detected as an attack_type divided by total no of requests. In resisting web proxy based Http/DoS attack [9] high false negative ratio old are shown in fig. 6. Due to high false negative ratio attacker attempt to prevents legitimate users from accessing the service. Detection of malicious client based Http/DoS attack on web server has low false negative ratio new are shown in figure 6. So it avoid attacker attempt to prevent valid users from accessing the service.

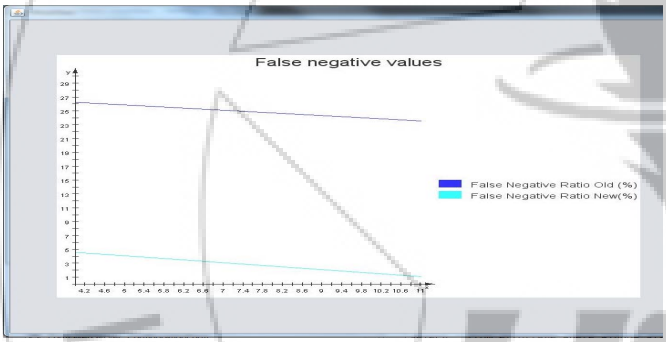

Figure 6: False negative ratio.

7. Conclusion

A web server side defense system against the Http attack. The main goals of the proposed system are accurate detection of Http/DoS attack and identifying malicious client based Http/DoS attack. It improves the quality of services of normal user by using the soft control schema. The performance analysis of detection system increases due to low false negative ratio.

References

[1] T. Peng, C. Leckie, and K. Ramamohanarao, Survey of Network Based Defense Mechanisms Countering the Dos and DDos Problems, ACM Computing Surveys, vol. 39, no. 1, p. 3, 2007.
[2] J. Yu, C. Fang, L. Lu, and Z. Li, Mitigating Application Layer Distributed Denial of Service Attacks via Effective Trust Management, IET Comm., vol. 4, no. 16, pp. 1952-1962, Nov. 2010
[3] S. Triukose, Z. Al-Qudah, and M. Rabinovich, Content Delivery Networks: Protection or Threat?, Proc. 14th European Conf. Research in Computer Security (ESORICS), pp. 371-389, 2009.
[4] S. Lee, G. Kim, and S. Kim, Sequence-Order-Independent Network Profiling for Detecting Application Layer DDos Attacks, EURASIP J. Wireless Comm. and Networking, vol. 2011, no. 1, p. 50, 2011.
[5] Y. Xie and S. Yu, Measuring the Normality of Web Proxies Behavior Based on Locality Principles, Network and Parallel Computing, vol. 5245, pp. 61-73, 2008.
[6] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez, Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges, Computers and Security, vol. 28, nos. 1/2, pp. 18-28, 2009.
[7] S. Yu, W. Zhou, R. Doss, and W. Jia, Traceback of DDos Attacks Using Entropy Variations, IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 3, pp. 412-425, Mar. 2011.
[8] Y. Xie and S. Yu, A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors, IEEE/ACM Trans. Networking, vol. 17, no. 1, pp. 54-65, Feb. 2009.
[9] Yi Xie, S. Tang, Y. Xiang and J. Hu, Resisting Web Proxy-Based HTTP Attacks by Temporal and Spatial Locality Behavior, IEEE transactions on parallel and distributed systems, VOL. 24, NO. 7, JULY 2013.
[10] Shun-Zheng Yu and Hisashi Kobayashi, An Efficient Forward–Backward Algorithm for an Explicit-Duration, 2003 IEEE.
[11] Jeongeun Julie Lee and Maruti Gupta, A new traffic model for current user web browsing behaivor, Intel corporation 2007.

Author Profile

Dhanya Jayan: M Tech, Sree Buddha College of Engineering, Pattoor, Alappuzha, Kerala, India.

Pretty Babu: Assistant professor, Sree Buddha College of Engineering, Pattoor, Alappuzha, Kerala, India.

Licensed Under Creative Commons Attribution CC BY