ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242

Volume 3 Issue 5 may, 2014 Page No. 5901-5904

Survey Paper for Resisting Web Proxy Based Http Attacks by Locality Behavior

Lakshmi B, Silja Varghese

Department of Computer Science and Engineering
Nehru College of Engineering and Research Centre, Pampady, Thrissur, Kerala.
lachulakshmi111@gmail.com

Department of Computer Science and Engsineering
Nehru College of Engineering and Research Centre, Pampady, Thrissur, Kerala.
varghesesilja287@gmail.com

Abstract—A novel attack detection scheme is proposed to prevent web proxy based http attacks.Here the detection is carried out at server.The scheme utilize locality behaviors such as temporal and spatial localities to obtain features of proxy-to-server traffic. A Gaussian-mixture and Gamma distribution hidden semi markov model is used to describe the time-varying traffic behavior of web proxies. Soft control scheme is used as the attack response it convert malicious traffic into relatively normal one by behavior reshaping rather than rudely discarding so that legitimate users get service and prevent attacker from receiving service.DDoS attack is a key threat to internet applications by comparing existing network security systems the primary aim of the proposed system is to protect origin server from web proxy based http attacks.

Keywords-Http attack, Temporal and Spatial locality, DDoS, HsMM

I. INTRODUCTION

Distributed Denial Of Service attacks are large scale DoS attacks which employ a large number of attackers distributed across the network. There are two classes of DoS attacks which are infrastructure level and application level attacks. Infrastructure level attacks directly attack the resources of the service such as the networks and hosts of the application services. Incontrast, application level attacks are through the application interface for example, the attackers overload an application by sending abusive workload malicious requests which crash the application. There are two stages in such attacks. First attackers build large zombie networks by compromising many internet hosts and installing a zombie program on each. Second, attacker activates this large zombie network. In computer networks, a proxy server is a server that may be a computer system or an application that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Today, most proxies are web proxies, facilitating access to content on the World Wide Web. A web proxy turn into attacker by two steps first step, the attacker send request to web proxy and force it to forward to the original server. In second step the attacker disconnect the connection between itself and web proxy[1]. It is very difficult to identify such kind of attack because the origin server cannot directly observe and diagnose the terminal hosts shielded by hierarchical proxy system also the attack traffic is mixed with regular client to proxy traffic. Thus the victim server is hard to accurately identified and filter the attack requests. The scheme is based on network behavior analysis[2]. Here a Hidden semi-markov Model is used to obtain the access behavior of web proxy [3],[4].HsMM is a double stochastic process. The upper layer is a markov process whose states are not observable. The lower layer is a normal markov process where

emitted outputs can be observed. HsMM is a powerful tool for modeling and analyzing network behavior. Based on this behavior model, detecting the abnormality of a Web proxy can be achieved by measuring the deviation between an observed behavior and the Web proxy's historical behavior profile. Long-term and short-term behavior assessment methods are proposed. Long-term behavior assessment issues warnings on a large scale, while short-term behavior assessment locates abnormal request sequences embedded in the proxy-to-server traffic. A new "soft-control" scheme is proposed for attack A soft control scheme is used as an attack response. This approach block the server for providing service to the malicious sequences and allow server for providing services to the normal users [1]. Compared with most of the existing network security systems proposed scheme is focused on:1) resisting Web proxy-based HTTP attacks and early detection without any cooperation of mid

web proxies; 2) the approach it is independent of traffic intensity and frequently varying web contents. It has good stability and need not frequently update model's parameters; 3) long and short term behavior assessment methods enable the multi granularity diagnosis, while the "soft-control" scheme can improve the quality of services of normal users[1].

The remainder of the paper is organized as follows. Section II reviews some related works.Proposed work is in Section III. Finally, the paper is concluded in Section IV.

II. RELATED WORK

Distributed Denial of Service attack became threat to internet application. In[5],DDoS attack refers to the attempt to prevent a server from offering services to the legitimate users typically by sending requests to exhaust the server's resources .Application layer DDoS attack that sends out requests following the communication protocol and these requests are indistinguishable from legitimate requests. Here Trust Management Helmet is introduced against application layer DDoSattacks. Trust is used to evaluate the visiting history of client. There are four types of trust evaluated short term trust, long term trust, negative trust, misuse trust. Based on these overall trust is calculated.

In [6],a sequence order independent scheme is introduced for detecting application layer DDoS attacks. Here first extract the sequence order independent informative attributes from web page request sequences which are then represented in matrix and use multiple PCS to model the browsing patterns then uses reconstruction error of multiple PCA as a criterion for distinguishing App-DDoS attacks from normal usage.

In [7], introduce a method for finding malicious web request by using locality behavior of proxy. The existing scheme [1], uses statistical methods. It uses temporal locality and spatial locality [7], to extract the access behavior of web proxies. Then a stochastic process based on Gaussian mixture hidden markov model is used to describe the variety of normal access behavior and implement anomaly detection for the proxy to server web traffic. In [8],introduced a scheme to capture the spatial-temporal patterns of a normal flash crowd event and to implement App- DDoS attack detection. Flash crowd refers to the situation when a very large number of users simultaneously access a popular website which produces a surge in traffic to the website and might causes the site to be virtually unreachable. However the potential assumption of all these schemes [5],[6],[7],[8],is that the attacking hosts are directly connected to the victim server. So the server can identify the attacking hosts. But in the proxy based network the attacking and non attacking hosts are shielded by hierarchical of web proxies the server cannot identify the actual attacking hosts because it only knows the information of proxy.

Hidden Markov Model is defined as double stochastic process. The upper layer is a markov process whose states are not observable. The lower layer is a normal markov process where emitted outputs can be observed.HMM is a powerful tool for modeling and analyzing proxy's access behavior. An extension of HMM is a Hidden semi Markov Model whose underlying process is a semi markov chain and each state has variable duration. In [9], state duration of the HsMM was first parameterized by Gamma distribution. The important difference between HMM and HsMM is that one observation per state in HMM while in HsMM each state can emit sequence of observations. The existing system [1], uses Gaussian distribution Gamma distribution HsMM because it requires fewer parameters to be estimated than the discrete HsMM which reduce computational complexity

III. GENERAL SYSTEM MODEL

The objective of proposed system is to protect the victim server from web proxy based http attacks. In the existing system the attack traffic is assumed to begin from web proxies instead of its real sources and the victim server can only observe the intermediate proxy .Web proxy access behavior is depends on locality behavior such as temporal locality and spatial locality. The access behavior can be directly mapped into an HsMM. It is a double stochastic process. The upper layer is a markov process whose states are not observable. The lower layer is a normal markov process where emitted outputs can be observed. The attack detection is based on searching the abnormality in the requests and blocks those attacking requests by receiving service from the victim server and providing service to those requests which are not attacking requests.

A. Temporal and Spatial Pattern Analysis

Web proxy's access behavior is obtained using locality principle such as temporal locality and spatial locality principle. Temporal locality refers to the property that referencing behavior in the recent past is a good predictor of the referencing behavior in the near future [1]. Temporal locality is obtained using stack distance model. According to [7],stack distance model is often utilized to capture the temporal locality relationship. Here reference stream Ri={r1,r2,….ri} where ri denotes the i th requested document name.

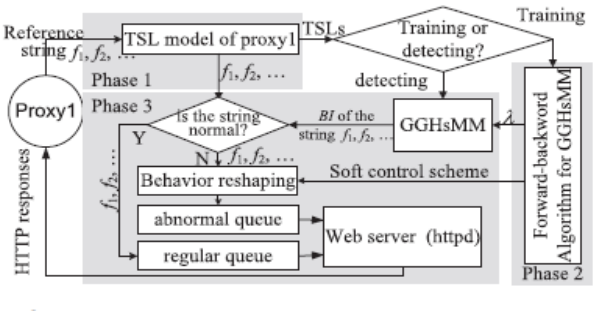

FIG.1. SYSTEM DIAGRAM

Index i indicate that i requests have already arrived at the server. Here use least recently used stack Liwhich is an ordering of all documents of a server by recent usage. Whenever a reference is made to a document the stack must be update. The reference symbol stream is transformed to a numerical stream based on stack distance model. Spatial locality refers to the property that objects neighboring an object frequently accessed in the past are likely to be accessed in the near future [1].Spatial locality is calculated by counting the occurrence of a particular pattern within a time window.Comparisons of above described papers are shown in the table1 below.

Existing Systems	Scheduling Method	Advantage	Disadvantage
Measuring the normality of web proxies behavior based on locality principles	Stack distance model	Preserve pattern of activity, Practical method.	Time consuming
Light weight mechanism to mitigate application layer DDoS attacks	Trust Management Helmet	Portable,Reduce processing delay,light weight.	Difficult to deal with some kind of attacks.
Monitoring application layer DDoS attacks for popular website	Locality behavior	Early attack detection	Depends traffic intensity
Sequence order independent network profiling for detecting application layer DDoS attacks	Sequence order independent method	Practical,Efficient,Additional information can easily inserted into model	Sometimes make incorrect decision

Table 1.Comparison table of existing system

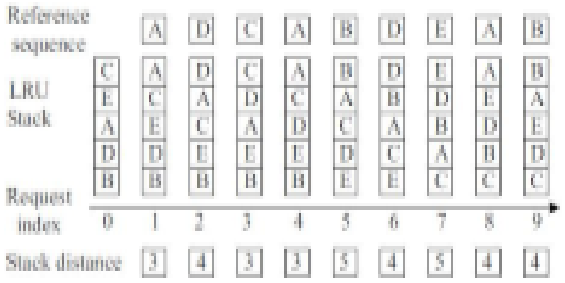

FIG.2. STACK DISTANCE MODEL

B. TRAINING AND DETECTION

The training phase find different request pattern to develop a training model. Here different possibilities are obtained using Temporal and Spatial locality behavior. To overcome the short comings of the Existing Algorithms a new iterative methods based on the forward backward algorithm is used. In detection Phase develop a System for detecting abnormal pattern.

C. SOFT CONTROL

Soft control Scheme is used as the attack response mechanism. It identify Malicious requests out of all requests and block attacking request by receiving service from the server and allow normal users to getting service from the server this improve the quality of service to the legitimate users.

IV. PERFORMANCE DIAGRAM

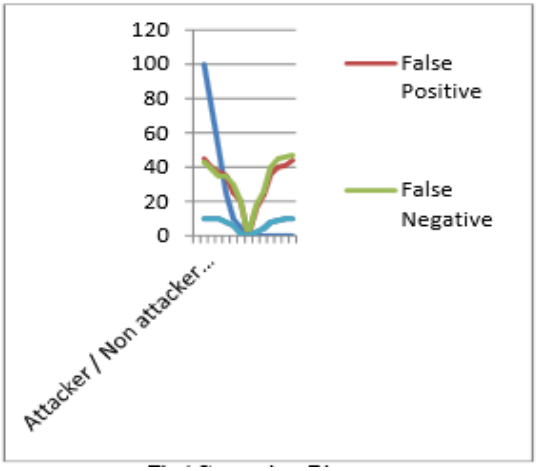

FIG.4.PERFORMANCE DIAGRAM

Above Performance diagram shows the False Positive and False Negative Ratio According to the number of users. The disadvantage with these system is that False Positive and False Negative ratio increase with the number of users increase. These can be reduced in the future by Providing client information to the server

IV CONCLUSION

Web proxy based HTTP attacks are difficult to detect. These kind of attacks introduce challenges to the existing network security system. There are numerous techniques exist for

detecting such kind of attack but all these schemes in which attacking hosts are directly connected to the victim server. So the server can identify attacks hosts. The proposed scheme introduces a method that can detect and respond to such kind of attacks. But the disadvantage with the scheme is that false positive and false negative ratio increases when the number of users increases. these can be solved in future work The main advantage of this approach include:1) reduced false positive and false negative rate; 2) it can realize early detection; 3) reduced computational overhead.

REFERENCES

[1]YIXIE, S.TANG, Y.XIANG AND J.H, "RESISTING WEB PROXY BASED HTTPATTACKS BY TEMPORAL AND SPATIAL LOCALITY BEHAVIOR," *IEEE TRANSACTIONSON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 7, JULY2013.*

[2] P. GARCIA-TEODORO, J. DIAZ-VERDEJO,G. MACIA-FERNANDEZ AND E. VAZQUEZ, "ANOMALY-BASED NETWORK INTRUSION- DETECTION: TECHNIQUES, SYSTEMS ANDCHALLENGES*," COMPUTERS AND SECURITY,VOL. 28,NOS. 1/2, PP. 18-28, 2009.*

[3] J. FERGUSON, "VARIABLE DURATION- MODELS FOR SPEECH,"*PROC. SYMP. APPLICATION OF HIDDEN MARKOV MODELS TO TEXT AND SPEECH, PP. 143-179, 1980.*

[4] S. YU, "HIDDEN SEMI-MARKOV MODELS," *ARTIFICIAL INTELLIGENCE,VOL. 174,NO.2, PP.215-243, 2010.*

[5] J. YU, C. FANG, L. LU AND Z. LI, "MITIGATING APPLICATION LAYER DISTRIBUTED DENIAL OF SERVICE ATTACKS VIA EFFECTIVETRUST MANAGEMENT," *IET COMM.,VOL. 4, NO. 16, PP. 1952-1962, NOV. 2010.*

[6] 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.*

[7] Y. XIE AND S. YU, "MEASURING THE NORMALITY OF WEBPROXIES BEHAVIOR BASED ON LOCALITY PRINCIPLES*," NETWORK AND PARALLEL COMPUTING, VOL. 5245, PP. 61-73, 2008.*

[8] Y. XIE AND S.-Z. YU, "MONITORING THEAPPLICATION-LAYER DDOS ATTACKS FOR POPULAR WEBSITES,"*IEEE/ACM TRANS. NETWORKING, VOL. 17, NO. 1, PP. 15-25, FEB. 2009.*

[9] S. LEVINSON, "CONTINUOUSLY VARIABLE DURATION HIDDEN MARKOV MODELS FOR AUTOMATIC SPEECH RECOGNITION," *COMPUTER SPEECH AND LANGUAGE, VOL. 1, NO. 1, PP. 29-45, 1986.*

[10] S.-Z. YU AND H.KOBAYASHI, "ANEFFICIENT FORWARD-BACKWARD ALGORITHMFOR AN EXPLICIT-DURATION HIDDEN MARKOV MODEL*," IEEE SIGNAL PROCESSING LETTERS, VOL. 10, NO. 1, PP. 11-14, JAN2003.*