International Journal of Latest Research In Engineering and Computing (IJLREC) ISSN:2347-6540
Volume 1, Issue 2 : Page No23-25, November-December 2013
www.ijlrec.com

A Framework Extension To Support Flash Crowd Using Service Differentiation At The Application Layer

Gopi R
School of Information Technology and Engineering
VIT University, Vellore, India

Abstract-Software As Service (SAAS) from CLOUD represents an Application Layer of networks. The Security need of Application layer is to protect the DATA or FILE in that layer. Various types of Distributed Denial Of Service Attacks(DDOS) have been performed on this layer in order to steal the DATA or consume the resource from the Application. The current challenge in network security is to propose a framework that separate the ddos attack from the flash crowd thus not punishing the legitimate flash traffic at any cause. In this paper, we propose a model which is an extension of existing novel framework and it is named as SADSD . This SADSD is Source validation And Detection with Service Differentiation which makes the suspicious users to prove their legitimacy whose web requests are delayed once it is detected that their signatures are bad signatures.

Keyword :-**Application Layer, CLOUD, DDOS, Flash Crowd, SADSD.**

Introduction

Distributed Denial Of Service(DDOS) attacks at the application layer of a web server is difficult to prevent as the http traffic will look normal as a legitimate traffic. It is even more difficult to prevent and detect the DDOS attack, when a condition occurs called flash crowd where million of legitimate users give requests to a website at the web server. It is because both flash crowd and the DDOS attack look same. Since the ddos attack at application layer arise from legitimate machines which are compromised which is indistinguishable. The aim of application layer ddos attacks is to steal the information or consume the resource from the web server with pretending like a legitimate user.

Based on [2] there are various detection, protection and prevention methods are used to classify the application layer ddos traffic and normal traffic. These methods are not used individually instead it can be used in combination of two or more methods for an efficient intrusion detection and prevent system. Based on [1] an system for the prevention of ddos at the application layer must need an detection and blocking software unlike network layer ddos attack where the detection software is installed in the router or any network component.

The current challenge in network security is to classify the flash crowd legitimate traffic from ddos traffic without punishing or disturbing the legitimate traffic by the detection and blocking software used for characterization at the victim place.

In this paper, we design a framework which is an extension of framework presented in [1], which is named as SADSD(Source Validation and Detection with Service Differentiation) which makes the suspicious users to prove their legitimacy whose web requests are delayed once it is detected that their signatures are bad signatures using a Service differentiation (SD) Component.

Related Work

Many schemes and methods are available to discriminate the attack traffic and normal traffic at the application layer including flash crowd, based on [2]. With respect to [3] a counter mechanism used to detect application layer attack using an access matrix in which suspicion score is calculated. Based on the suspicion score the attack and normal traffic are classified.

Based on [4] discrimination of flash crowd from the attack traffic is done by flow correlation coefficient which is a statistical method, which classifies based on set of metrics, measures or features. Another technique which categorize based on behavior pattern of normal user and botnets using pearson correlation coefficient, based on [5].

These behavior pattern are analyzed based on the packet transmission that happens toward the victim. The packet delay and changing rate of the port numbers are the other two behavior patterns which are to be tested in future.

Many of the classification methods are statistical methods. It is found that statistical methods are good for classifying the abnormal traffic but not flash crowd from the attack traffic, based on [1]. It is not acceptable to punish the legitimate traffic at any cause. Hence a novel framework is found which is a combination of occasional source validation with signature detection from [1]. This is a calibration of two methods for detection and validation of attack traffic from flash crowd which is first framework which does not punish the legitimate traffic during verification process, since all other existing statistical methods makes incorrect assumption and false positives with the new flash traffic with the old attack traffic. The occasional source validation is done by AYAH(Are You A Human Page or CAPCHA) along with signature detection, where only 1 request of N requests is sent to AYAH and N-1 request are sent for signature verification.

Signature verification based on previous traffic makes incorrect assumption as it is also a statistical method. Therefore when a traffic occurs that 1 request which completes AYAH form determines whether the future traffic is good or bad. But in [1] when the signatures are found to be bad and below the High threshold value the requests are delayed to reach the web server otherwise the requests are rejected when it reaches high threshold value.

It is found from [2] that, rate limiting(delay) to the web requests is done where there is no accuracy, and filtering(block) packets or web requests is done when they are detected accurately. Although delaying may be the best option when classification is based on Statistical signature verification, it is not acceptable that requests from suspicious users which may be a combination both normal user and botnets are delayed.

Problem Definition

Although when the rate is below high threshold value, delay to the suspicious users web requests after signature verification is another type of punishing legitimate traffic where those requests may be of both normal as well as abnormal users. It is no longer acceptable that both attack traffic and legitimate traffic are delayed after signature verification found to be bad, which results in reduced performance of the website.

Proposed Work

The proposed work is based on Service Differentiation. Research studies shows that, users who are willing to prove their legitimacy in case of incorrect assumption may receive a better service at the cloud environment after they are verified. The delay period to the web requests can be matched alternately with the legitimacy verification of the willing users. The system architecture is shown in Figure 1. The newly included system components such as Load and Delay analyzer(LD) and Service Differentiation(SD) component are explained as follows.

A. Load and Delay analyzer

In the existing framework based on [1], load and delay analyzer is included additionally. This component is defined to calculate the load of web requests at the website and the delay rate that occurs to the web requests after the signature is detected as bad. The delay rate is analyzed so that if it exceeds a very minimal threshold of delay, the IDS/IPS system can make the users to prove their legitimacy. Since the delay time can be matched with the process legitimacy verification.

B. Service Differentiation(SD) component

This SD component is defined to predict the users who will exceed the minimal threshold of delay and make those users to actively participate in the legitimacy proving criterion. The SD component and load and delay analyzer component are interconnected. The delay rate happening to the web requests is analyzed and sent to the SD component.The legitimacy proving criterion can be any of the protection techniques based on [2]. Source validation using CAPCHA can be done. Since CAPCHA is used as AYAH in [1], we can use AYAH web page for the legitimacy proving by the users. The web requests are forwarded to the AYAH web page and rest of the web requests are still in the delay stage only.

Note that, the minimum threshold of delay is chosen such that the minimum time taken by a user to complete the AYAH page and get the fast service from the website.

D. Algorithm for the proposed work

The steps involved in the proposed work is as follows :

1. Choose minimum threshold of delay value MIN_d
2. For each web request from user i
3. Calculate the delay rate Dr_i
4. If $Dr_i >= MIN_d$
5. Forward request to the AYAH page
6. Else
7. Let the requests in Delay stage

By default, the AYAH page asks the user to fill the words given in the image[2], checks whether it is a normal user of botnet and forwards to the web server or rejects the request.

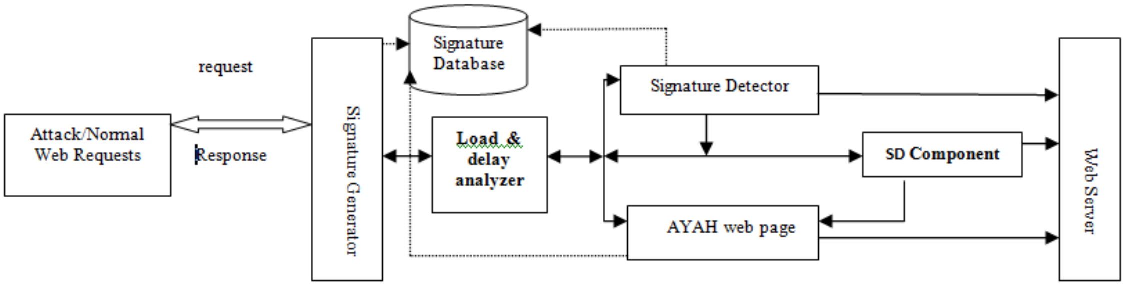

Fig 1. Overall System Model

Conclusion

Although in existing framework legitimate traffic and attack traffic can be discriminated without giving burden to the legitimate users, it is not acceptable that web requests from the users are delayed even after the signature detection. Even though rate limiting the web requests is one of the safety way to prevent the ddos attack after detection, users are still get punished by the delay to get the service from website. Thus a service differentiation(SD) component is included to make the delayed users to prove their legitimacy using a source validation technique. The highlight of this proposed work is existing AYAH page can be used as a source validation. Thus the performance can be increased on demand basis. Future work can be done on Over provisioning to support verification process on large amount of web requests. New methods and techniques to prevent ddos attack can be enhanced based on current attack trends and technology.

References

1. Sujatha Sivabalan and Dr P J Radcliffe, " A Novel Framework to detect and block DDoS attack at the Application layer" , IEEE , 2013.
2. Yash Pravinkumar Raithatha and Chirag Suryakant Thaker, "Various Methods used for the Protection, Detection and Prevention of Application Layer DDOS Attacks" , IEEE, Vol 2 Issue 5 May 2013.
3. S. Renuka Devi and P. Yogesh, "An Effective Approach to Counter Application Layer DDoS Attacks" , IEEE, 2012.
4. Shui Yu, Weijia Jia, Yong Xiang, and Feilong Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient" , IEEE Transactions On Parallel And Distributed Systems, VOL. 23, NO. 6, JUNE 2012.
5. Theerasak Thapngam, Shui Yu, Wanlei Zhou and Gleb Beliakov," Discriminating DDoS Attack Traffic from Flash Crowd through Packet Arrival Patterns" , IEEE, 2011.