International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

A Defense System against Application Layer DDoS Attacks with Data Security

Nagalakshmi S L[1], Kaveri M[2], Jagruthi H[3]

[1]*Student, Dept. of ISE, B N M Institute of Technology, Karnataka, India*
[2]*Student, Dept. of ISE, B N M Institute of Technology, Karnataka, India*
[3]*Assistant Professor, Dept. of ISE, B N M Institute of Technology, Karnataka, India*

Abstract - *Application layer distributed denial of service (DDoS) attacks have become a critical issue for the certainty of web servers. These attacks elude most intrusion prevention systems by sending innumerable benign HTTP requests. Most of these attacks are launched unexpectedly and severely, hence a fast intrusion avoidance system is required to detect and alleviate these attacks as soon as possible. For this, we propose an efficacious defense system, which holds the data structure to quickly detect and alleviate application layer DDoS attacks. Captcha test is performed to decide whether there is an attack or not. Whenever request is coming from blacklisted IP address, it will not allow to access the server. White list IP addresses are genuine IP addresses. This improves the effectiveness by avoiding the reverse calculation of malicious hosts. The experimental results show that application can quickly reduce malicious re-quests, while posing a limited impact on normal users. We have also included Honey Pot Technique used for the file security in the cloud. User can be able to upload the file into the cloud storage.*

1. INTRODUCTION

Distributed denial of service (DDoS) attacks have become a severe problem to the security of Internet users for decades and numerous defense schemes have been proposed to detect and identify DDoS attacks at the network layer. These attacks grow rapidly against web servers and bring victims with great revenue losses. App-layer DDoS attacks attempt to disrupt authorized access to application services by masquerading flash crowds with numerous benign requests. Flash crowd refers to the situation when many users access a popular website simultaneously, producing a surge in traffic to the website and causing the site to be virtually unreachable. The secrecy of app-layer DDoS attacks makes most signature-based intrusion prevention systems ineffective. Since most DDoS attacks are launched abruptly and severely, it is desirable to design a defense system that can detect and mitigate app-layer DDoS attacks as soon as possible to minimize the losses. Turing test schemes based on graphical puzzles have been proposed to address the above problem on the cost of additional delays. Unfortunately, since a few milliseconds extra delay may cause users to abandon a web page early, applying such mechanism to all users will negatively affect the Quality of Experience (QoE). Therefore, an effective defense system should mitigate app-layer DDoS attacks as soon as possible while posing a limited impact on the access of normal users. The increasingly high-speed network links demand an efficient data structure to process a huge volume of network traffic efficiently, especially under HTTP flooding attacks. The sketch data structure can efficiently estimate the original signals by aggregating high dimensional data streams into fewer dimensions, making it very suitable for DDoS attack detection. A series of sketch-based approaches have been proposed for anomaly detection in large scale network traffic.

Since sketches contain no direct information about the malicious hosts, they cannot be directly used for the mitigation of attacks. To tackle this problem, several efficient reverse hashing schemes have been proposed to infer the IP addresses of malicious hosts from reversible sketches. These studies attempt to retrieve the anomalous keys by using reverse hashing methods.

2. SYSTEM OVERVIEW

Whenever there is a request from the user it first identifies whether it is in whitelist or not. If it is in whitelist then S1 is updated. If it is not in whitelist then there is a need to check whether it is in blacklist or not. If it is in blacklist then that request is filtered and blocked. If the request is not in blacklist then we have to identify whether it is suspicious or not. If it is not suspicious request then S1 is updated. Otherwise Captcha test is conducted. Captcha test is conducted to validate the user. If it fails Captcha test then that request is blocked. It is deployed behind a network firewall that will filter out malformed HTTP requests, and the process consists of two phases, namely, mitigation and detection. In mitigation phase skyshield consists of two bloom filters B1 and b2. B1 is whitelisted bloom filter and B2 is blacklisted bloom filter to filter the requests. Whitelist consists of valid users which enters valid username and password and also those which passes the Captcha test. These requests which are verified by whitelist are directly passed to the detection phase. The malicious requests verified by blacklist are filtered and blocked. The remaining requests are filtered based on sketch S3 as shown in fig -1 and fig -2.

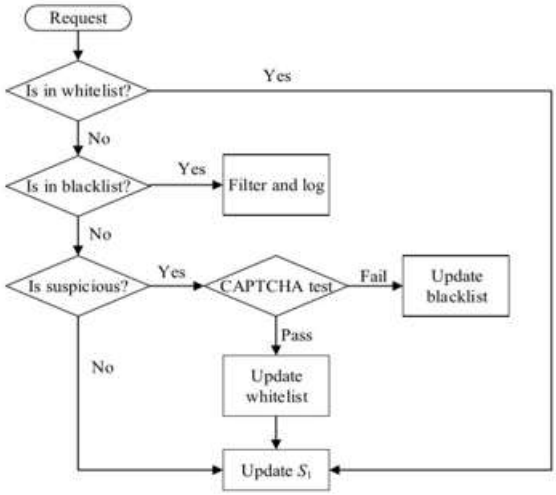

Fig -1: Flow chart of the process

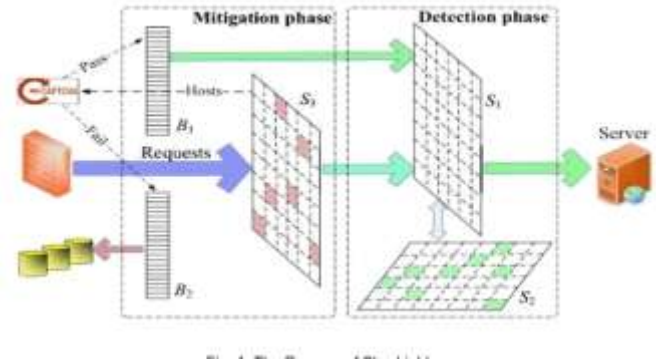

Fig -2: Process of Skyshield

Mitigation phase checks whether the host is blacklist or whitelist. If not then that request is considered as suspicious and Captcha test is conducted for that host. If it passes the Captcha test then that host is placed in whitelist otherwise the host is pushed to the blacklist. Both blacklist and whitelist are cleaned periodically. Cleaning of blacklist and whitelist will not affect the accuracy of the detection phase.

3. IMPLEMENTATION

3.1Modules

The entire project is divided into 5 modules as shown below.

1. Mitigation Phase Module
2. DDos Attack Detection Phase Module
3. Captcha Test Module
4. Blacklist White list Management
5. Honey-pot Module

1) Mitigation Phase Module: Mitigation Identification means whenever users will access the web server, System has to identify whether it is a mitigation or not. Mitigation means slowing down the server process. It has to identify whether particular IP address is slowing down the service process or not. This is called Mitigation process.

2) DDoS Attack Detection Phase Module: When there is mitigation happening or mitigation is detected, this system has to identify whether it is an attack or not. For that we are using a captcha test. Based on the captcha test, we will decide that whether it is an attack or not. If it is an attack means, it will be added to the blacklist IP address. If it is not an attack, it will be added to the white list IP address.

3) Captcha Test Module: When there is mitigation happening or mitigation is detected, this system has to identify whether it is an attack or not. For that we are using a captcha test. CAPTCHA is used for ignorance of robots or sets of program to do a specific task without any human intervention.

4) Blacklist White list Management: In this module white list and black list concept is used. White list IP addresses are genuine IP addresses, even there are many request coming within the stipulated time also, even if the server is slowing down also, due to the white list IP address, it is not attack. Black list IP addresses are suspicious or it is a non-genuine IP address. Whenever request is coming from blacklisted IP address, it will not allow to access the server.

5) Honey-pot Module: Honey Pot is a concept for the file security in the cloud, with the help of Honey Pot Technique, User can able to upload the file into the cloud storage. Whenever user is uploading a file, for each file, it will generate a unique code. And that Unique code will be sent to user through email. Whenever user is downloading the file, User has to give the corresponding unique code to the respective file. If the user has given the correct code only, user will be able to get the original file. If user is giving the guessing code or some other wrong code, it will not show the error message but, it gives a duplicate file to the user. This concept is called Honey Pot Concept.

3. RESULTS

This section discusses the results obtained by implementing different modules of the proposed system. It contains the snapshots of the results obtained from different modules of the system. Whenever there is a request from the user, if the user enters correct username and password, that user is allowed to access the homepage. Once the user Logged in properly he/she can upload the file. Once the file is uploaded a passkey for that particular file is sent to the user via mail. While downloading the file the user has to enter the respective passkey and then only the file will be downloaded. If the user enters the wrong passkey, a dummy file will be downloaded. If the user enters the incorrect username and password, the number of such attempts is calculated. This threshold is different in trusted and

untrusted system. If it crosses the threshold then the user has to perform the Captcha test. This is shown in Fig -3.

Fig -3: Images in Captcha test

4. CONCLUSION

In order to prevent application layer DDoS at-tack, there is a need for fast response system to detect and prevent harmful requests automatically as soon as possible. In this method we designed and implemented such a mechanism which can identify and prevent these DDoS attacks at the application layer. First, the divergence between the two sketches are calculated. Second, the abnormal sketch S3 is used to identify the harmful hosts. Third, the Captcha test is conducted for suspicious hosts to increase the effectiveness of this mechanism. Finally a prototype of this is developed and the performance is evaluated. This result indicates that this mechanism can effectively identify and prevent DDoS attack at application layer and poses a limited impact on normal users.

REFERENCES

[1] ChenxuWang , Tony T. N. Miu, Xiapu Luo , and Jinhe Wang SkyShield: A Sketch Based Defense System Against Applica-tion Layer DDoS Attacks IEEE Transactions On Information Forensics And Security, 2018

[2] Sujatha Sivabalan , Dr P J Radcliffe A Novel Framework to detect and block DDoS attack at the Application layer IEEE 2017

[3] Zhang Chao-yang Towards defeating DDoS attacks IEEE International Conference on Intelligence Science and Information Engineering, 2017

[4] Peter Reiher Detection of Denial-of-Service Attacks Based on Computer Vision Techniques IEEE 2017

[5] Aikaterini Mitrokotsa A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis IEEE 2017

[6] Opeyemi A Osanaiye IP Spoofing Detection for Preventing DDoS Attack in Application layer International Conference On Intelligence In Next Generation Networks, 2016.