SKYSHIELD

A Security Mechanism against DDOS attack in Application Layer

Prof. Umarani Chellapandy
Maria Abraham
MCA
INFORMATION SECURITY MANAGEMENT SERVICES
Jain (Deemed-to-be-University) Bangalore, India

Abstract: **Attacks with the application layer Distributed Denial of Service (DDoS) attacks have turned into a genuine danger to web server security. These assaults dodge most interruption counteractive action frameworks by sending a few benevolent HTTP applications. Since a large portion of these attacks begin suddenly and abruptly, it is better to identify and mitigate these attacks as quickly as possible. In this paper, we propose an effective and well- organized resistance framework called SkyShield that utilizes the information structure of the sketch to rapidly identify and relieve DDoS attacks in the application layer. To begin with, we propose another count of the distinction between two sketches, which lessens the impact of system elements and improves the exactness of recognition. Also, we utilize the irregular sketch to make it less demanding to distinguish malicious hosts of progressing attack. This builds SkyShield 's productivity by keeping the invert computation of pernicious hosts. The preliminary outcomes demonstrate that SkyShield can rapidly decrease malicious requests while influencing normal users just marginally.**

I. INTRODUCTION

In the last decades, Distributed Denial of service (DDOS) attacks has been a serious threat to internet and a countless number of mitigation methods has been adopted to overcome these attacks on the network layer. The App-Layer DDOS attacks are increasing very fast on the web servers. The victims face large loses in the revenue as the DDOS attack multiplies. This attack floods the system by sending huge amount of http requests and denies legitimate access to the users. Flash crowd is a situation where many users access the same website and jerks it with traffic and makes it unreachable to the users. The detection of these Application-layer DDOS attacks are difficult and most of the signature base intrusion prevention systems fails to detect them and is ineffective. Since the DDOS attacks are launched abruptly and it should be mitigated and detected quickly such that they cause very minimal losses on the web servers. The Quality of Experience (QoE) of a user might get affected and abandons a webpage hence an effective defense system has to be designed to mitigate these attacks as soon as possible by having very limited impact on the normal users.

The challenge of coming up with a sketch-based defense system lies within the coordination between the detection and mitigation of attacks. First, since network traffic is inherently dynamic within the real environment, an accurate anomaly detection is important. Second, when an associated attack occurs, the identification of malicious hosts should be accurate while not affecting the access of legitimate users. Third, since most of these attacks are launched abruptly, an effective light-weight defence mechanism has to be adopted for the detection and mitigation of the attack.

In this paper, we propose SkyShield, as a new defense system based on sketches to guard against app-layer DDoS attacks. SkyShield takes advantage of the random aggregation property of sketches to boost its ability in previous studies. In other words, SkyShield mitigates attacks without acquiring the precise information of malicious hosts and thus avoids an intensive process of computation. This scheme's rationality is that attacks usually persist. The abnormal sketch might thus be reused to make it easier to spot the malicious hosts by verifying whether or not an incoming host caused the anomaly in the previous detection cycle. This avoids the reverse calculation of malicious hosts and so greatly improves the potency of the system.

2.Scope of the Product

The proposed system- SkyShield is designed to handle large amounts of DDOS flooding attacks. The bloom filters and Captcha increases the effectiveness and can also diminish the flooding attacks to an acceptable level.

It can reduce the Application-Layer DDOS attacks and can also mitigate the attacks with minimal impact on legitimate user. It is an automatic fast response system for detection and mitigation on application-layer DDOS attack. The detection is done as soon as possible to mitigate malicious requests on a website.

3.Existing System

Distributed denial of service (DDOS) attacks against web servers is growing rapidly and is bringing victim to suffer from great revenue loses. These attacks are not easy to detect and they are even harder to protect against. These automated attacks on the

Application layer of the web can be undetected by Web Application firewalls (WAF). The App-Layer DDOS attack interrupts legitimate access to application services by flooding it with benevolent requests. Recognizing the malicious traffic and ordinary traffic is troublesome, particularly on account of an application layer attack, for example, a botnet playing out a HTTP Flood attack against a victim's server. Since every bot in a botnet makes seemingly legitimate network request, the traffic will not be spoofed and it will appear as original or normal traffic. Since most of these DDOS attacks are launched abruptly and severely it can incur loses if not detected fast.

4. Proposed System

The proposed system named SKYSHIELD is a novel defense system against App-layer DDOS attack. SkyShield mitigates the attacks without retrieving the exact IP addresses of malicious hosts, thereby avoiding intensive computing process. The major contributions made in this paper includes a design developed for anomaly detection for App-layer DDOS attack. This scheme does not require a reverse calculation or storage of malicious host. The scheme uses the abnormal sketch detected to directly identify malicious hosts. This circumvents the computational process of concluding malicious hosts and thus greatly improves the systems efficiency. The adaptive mitigation scheme is developed by calculating the number of malicious hosts according to the request volume. The suspicious hosts are differentiated based on the load of the server, if the load on the server is high the more suspicious hosts is differentiated and if the load on the server is less, fewer hosts is differentiated as suspicious. This scheme will increase the attack detection speed and provides accuracy. By developing this we can mitigate the App-layer DDOS attack quickly with minimal impact on legitimate users.

5. System overview

SkyShield is designed to mitigate the App-Layer DDOS attack. It is deployed behind a network firewall which helps in filtering out all the malicious HTTP requests. The process of SkyShield contains two phases namely, the mitigation and the detection phase.
In the Mitigation phase, the incoming HTTP request are differentiated as Whitelist(B1) and Blacklist(B2) and is called as Bloom filters. The Whitelist contains all the legitimate requests or hosts which are confirmed by the Captcha. The ordinary request is verified by the whitelist and passed on to the detection phase where as the requests that are blacklisted are logged. The rest of the requests is inspected based on the abnormal sketch S3.

When there is a suspicious request the SkyShield will first check if the host is present in the whitelist. If it is not present, then it will be checked by the Captcha module. If the host clears the Captcha test it will be added to whitelist if not it will be blacklisted. In the detection phase, the difference between two sketches S1 and S2 is exploited as a signal to detect the anomalies which is caused by large number of requests from a malicious host. All the incoming request is collected in S1(source IP address is the input key) and S2 is the backup sketch that stores the results of S1 sketch. After the detection the differences between the two sketches S1 and S2 is found and if it reaches the threshold then the system can suffer from the attack and the alarm will be raised.

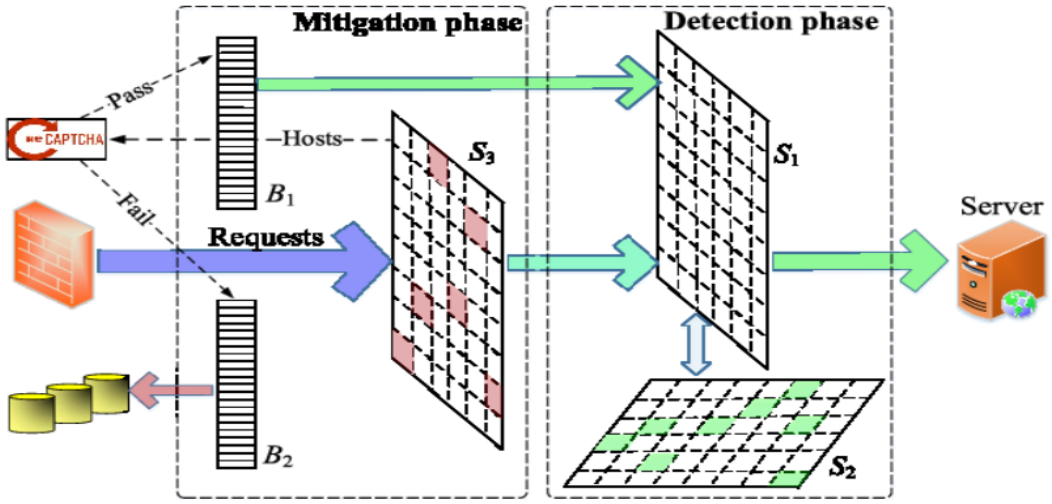

Figure:1 Process of Skyshield [2]

6. Project Module Description

Mitigation Phase Module

- Captcha

- Whitelist IP's (Legitimate IP's)
- Blacklist IP's (Logged)

Detection Phase Module

- Sketch S1 (request originating from malicious host)
- Sketch S2 (store S1 result)
- Divergence of S1 and S2
- Raising of alarms

Captcha Test Module

- The suspicious host undergoes Captcha test.
- If Failed- It will be stored or marked in blacklist
- If Pass- will be passed on to the detection phase.

7. Flow Diagram

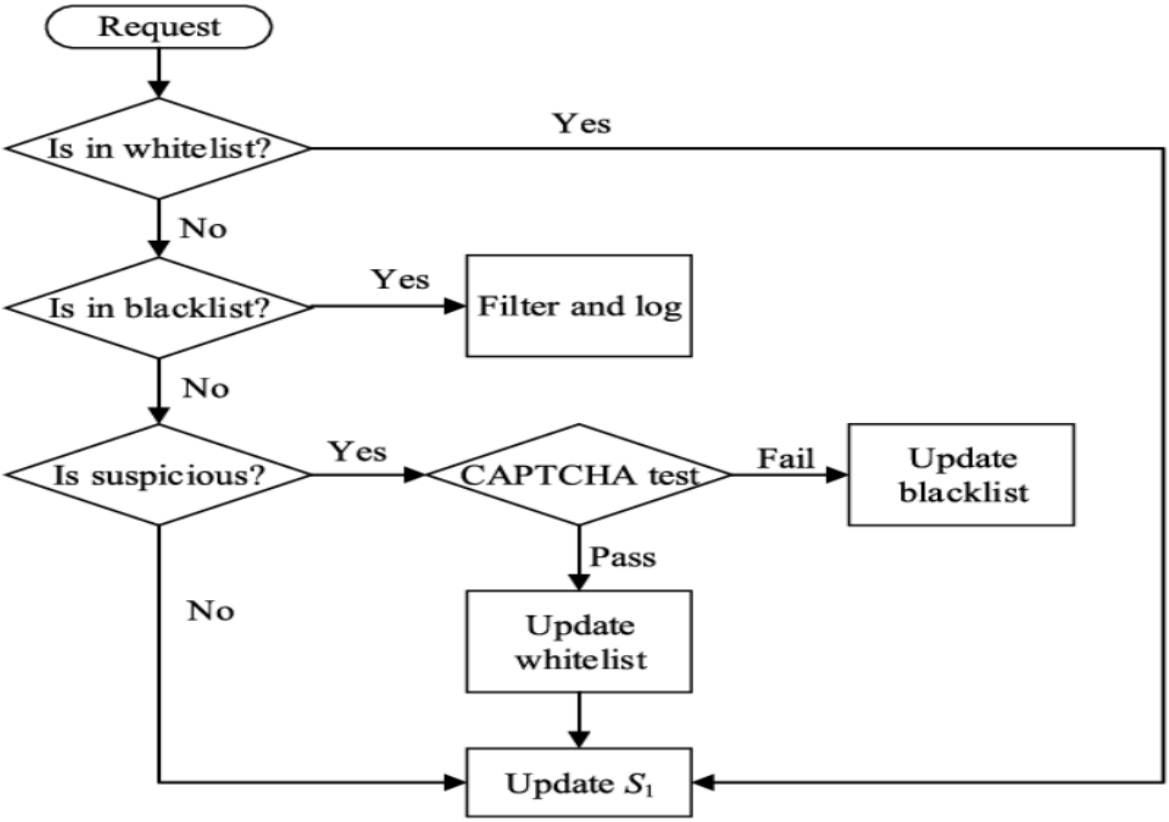

Figure:2 The Identification procedure [2]

8. Advantages

- This System increases the detection speed of the Application- layer DDOS attack
- Helps in filtering out the legitimate hosts from the malicious ones.
- SkyShield increases efficiency and effectiveness and reduces the flooding request to an acceptable level in about two or three detection cycles.
- Attacks occurred in flash crowds can be detected easily by using SkyShield.

- SkyShield can detect anomalies and prevent malicious traffic.
- SkyShield can handle large scale flooding attacks by using throughput of hashing which can be as high as 88,250 requests per second.
- Compared to the other methods like State-of-the-art method, SkyShield can handle HTTP request more effectively and quickly mitigate those attacks.
- It is adaptive to the request volumes thus it in an intensive attack it can filter out more malicious requests.

9. Limitations

- Even though SkyShield can mitigate the flash crowd attacks effectively, it still has limitations. One of the ways to evade SkyShield is by producing a real flash crowd event using large number of bots.
- Waves of new bots can be another method for evading SkyShield, where the malicious host detected in the first detection cycle will not be seen in the second detection cycle and hence will not get added in the blacklist.

10. Context Diagram

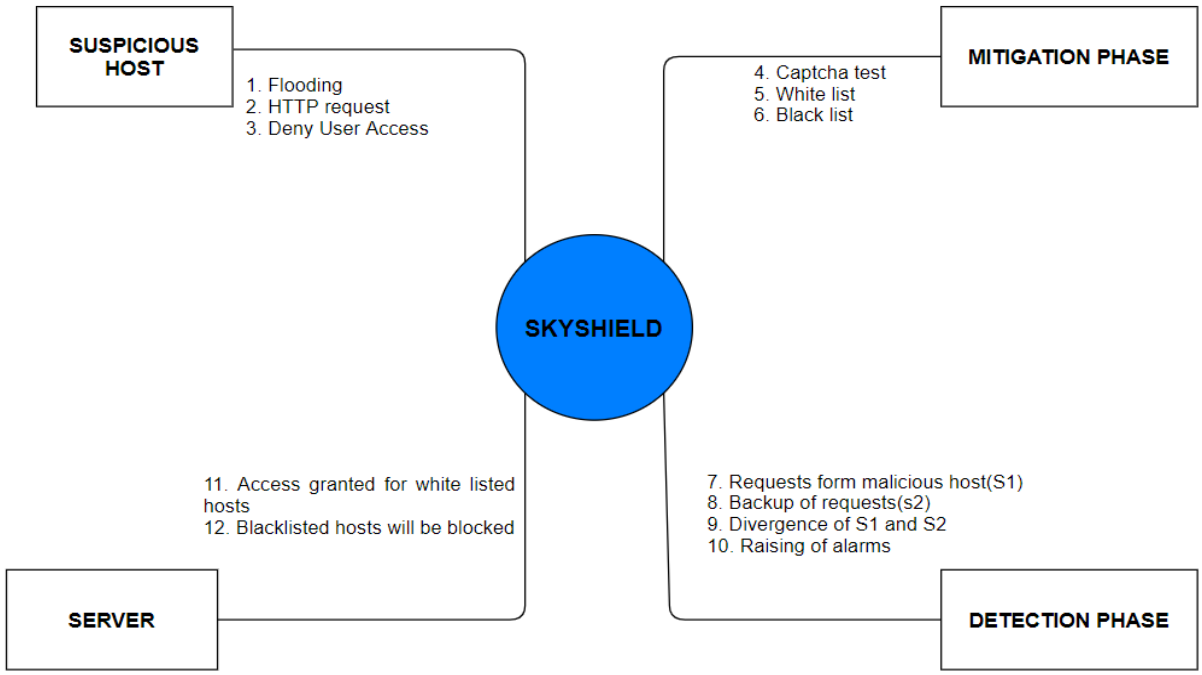

Figure:3 Context analysis diagram

11. Conclusion

To defend against Application-layer DDOS attack it is necessary to have a system that can automatically detect and mitigate malicious request quickly. In this paper we have designed and implemented such system where the divergence between the two sketches is detected in two continuous detection cycle. To avoid reverse calculation of IP address the malicious hosts is identified efficiently from the abnormal sketch that obtained from the mitigation phase. Techniques like captcha and bloom filters is also added to identify the suspicious requests and to guarantee the effectiveness of skyShield. The experimental results show that Skyshield can mitigate DDOS attacks by posing limited threats on the legit users.

12. Acknowledgment

This research is partially supported by Jain Deemed-to-be- University Jayanagar Bangalore.

13. REFERENCES

[1] https://www.semanticscholar.org/paper/SkyShield%3A-A-Sketch-Based-Defense-System-Against-Wang-Miu/d26148c446fe3b3684e35a7fe8d9074a573fa4a9

[2] https://www4.comp.polyu.edu.hk/~csxluo/SkyShield.pdf.

[3] file:///C:/Users/mariaabraham/Downloads/6147-12976-1-SM%20(1).pdf

[4] file:///C:/Users/mariaabraham/Downloads/6147-12976-1-SM%20(2).pdf

[5] J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in Proc. CCS, 2008, pp. 543–554.

[6] M.-Y. Su, "Real-time anomaly detection systems for denial-of-service attacks by weighted k-nearest-neighbor classifiers," Expert Syst. Appl., vol. 38, no. 4, pp. 3492–3498, 2011.

BIOGRAPHY

Prof. Umarani Chellapandy
Faculty & Guide Department of Computer Science & IT-MCA
Jain (Deemed-to-be University) Bangalore, India

Maria Abraham
Jain (Deemed-to-be-university) Jayanagar, Bangalore