Sky Shield: A Sketch-Based Safeguarding Opposed to Application Layer DDos Attacks

Dhanuja K C, Hitaishe Datta B, Harshita R, H P Mohan Kumar

Abstract-- Application layer distributed denials of service (DDoS) attacks have become a severe threat to the security of web servers. DDoS is a rapidly growing problem. These attacks evade most intrusion prevention systems by sending numerous HTTP requests. Since most of these attacks are launched abruptly and severely, a fast intrusion prevention system is desirable to detect and mitigate these attacks as soon as possible. We propose an effective defence system, named sky Shield, which will quickly detect and mitigate application layer DDoS attacks. In this application Admin will add user and send an security key for the users mail using which users will login providing their email id and security key. Admin will send secured data to the user. The data is encrypted by using RSA algorithm and a security key is sent to admin email id through which admin can view records. This improves the efficiency of Sky Shield by avoiding the reverse calculation of malicious hosts.

I. INTRODUCTION

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic.

Recently, application layer DDoS attacks against web servers grow rapidly and bring victims with great revenue losses.

App-layer DDoS attacks attempt to disrupt legitimate access to application services by masquerading flash crowds with numerous benign requests. Flash crowd refers to the situation when many users simultaneously access a popular website, producing a surge in traffic to the website and causing the site to be virtually unreachable.

Dhanuja K C, Hitaishe Datta B, Harshita R, H P Mohan Kumar: Department Of MCA, PES College Of Engineering , Mandya, Karnataka, India

The secret of app-layer DDoS attacks makes most signature-based intrusion prevention system 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 cost of additional delays. Unfortunately, since a few milliseconds extra delay may cause uses to abandon a web page early [4], apply search to all users will negatively affect the quality of experience therefore an effective defense system should mitigate app-layer DDoS attack as soon as possible while posing a limited impact on the access of normal users. The increasingly high speed network link demand and 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 [5]. A series of sketch based approaches have been proposed for anomaly detection in large scale network traffic [5]. 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 infer the IP addresses of malicious host from reversible sketches. This studies attempt to retrieve the anomalous keys either by using reverse hashing methods or by storing parts of keys However, these methods are either computation-intensive or storage demanding, limiting their application intrusion prevention systems [7]. It presents two taxonomies for classifying attacks and defenses, and thus provides researchers with a better understanding of problem and the current solution [1]. It presents a structural approach to the DDoS problem by developing a classification of DDoS

attacks and DDoS defense mechanisms [2]. It provide a framework for comparing the performance and deployment of DDoS defenses. Identify the characteristics in attack detection algorithms [3]. They analyze the design decision in the internet that have created the potential for denial of service attacks [6]. In this application, we use a RSA algorithm for encrypting secure data. RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means it works on two different keys i.e. Public key and private key. As the name describes that public key is given to everyone and private key is kept private.

II. MOTIVATION

Distributed Denial of Service (DDoS) pose a serious threat to network security. There have been a lot of methodologies and tools devised to detect DDoS attacks and reduce the damage they cause. Still most of the most methods cannot simultaneously achieve.

Even though cloud computing apparently offers adequate resistance to attacks. Some review proves that many attacks can still cause great harm to cloud computing, impacting all the important security aspects(confidentiality, integrity, isolation availability, etc).

- Not secure, does not provide required data security.
- These attacks hold the potential to cause similar damaging effect as their low layer counter parts using relatively fewer attacking assets.
- Application layer Distributed Denial of Service(DDoS) attacks have empowered conventional flooding based DDoS with more subtle attacking methods to pose an ever increasing challenge to the availability of internet based web services.

III. PROPOSED SYSTEM

In the proposed system, we provide an effective defense system sky shield against application layer DDoS attacks of web servers from hackers. In this application hacker will try to gain control over network of admin and users to carry out an attack by sending numerous request to the target server in one second. To mitigate this DDoS attack we have to differentiate between attack and normal traffic. Sky shield is effective is effective in mitigating flash crowd mimicking attacks and recognizing the DDoS attack on web server. In this application admin will add user, he can also view, update and delete user. Admin will send an security key for the users by using mail which users will login providing their email id and security key. Admin will send secured data to the user in encrypted format to provide security for users data by using RSA algorithm and a security key is sent to admin email id using which admin can view records and delete records.

IV. SYSTEM IMPLEMENTATION

System Implementation is making the new system available to a prepared set of users and positioning on-going support and maintenance of the system within the performing organization. At a finer level of detail, deploying the system consists of executing all steps necessary to educate the consumers on the use of the new system, placing the newly developed system into production, confirming that all data required at the start of operations is available and accurate, and validating that business functions that interact with the system are functioning properly. Transitioning the system support responsibilities involves changing from a system development to a system support and maintenance mode of operation, with ownership of the new system moving from the project team to the performing organization. A key difference between system implementation and all other phases of the life cycle is that all project activities up to this point have been performed in safe, protected and secure environments, where project issues that arise have little or no impact on day-to-day business operations. Once the system goes live however, this is no longer the case. Any miscues at this point will almost certainly translate into direct operational and/or financial impacts on the Performing Organization. It is through the careful planning, execution, and management of system implementation activities that the project team can minimize the likelihood of these occurrences, and determine appropriate contingency plans in the event of a problem.

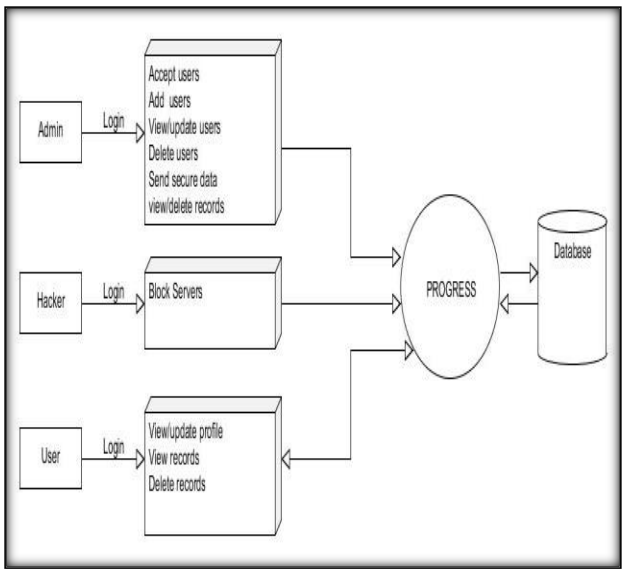

Fig 1: System Architecture

It includes three phases:

Prepare for System Implementation, where all steps needed in advance of actually deploying the application are performed, including preparation of both the production environment and the consumer communities fig [1].

Deploy System, where the full deployment plan, initially developed during system Design and evolved throughout subsequent lifecycle phases, is executed and validated fig [1].

Transition to Performing Organization, where responsibility for and ownership of the application and transitioned from the project team to the unit in the Performing Organization that will provide system support and maintenance fig [1].

V. RESULTS

In this paper, we propose an Application layer distributed denial of service (DDoS) attacks has become a severe threat to the security of web servers. These attacks evade most intrusion prevention systems by sending numerous begin HTTP requests. Since most of these attacks are launched abruptly and severely, a fast intrusion prevention system is desirable to detect and mitigate these attacks as soon as possible. In this paper, we propose an effective defense system, named Sky Shield, which leverages the sketch data structure to quickly detect and mitigate application layer DDoS attacks.

- Using this system, we can protect web clusters from app-layer DDoS attacks by employing required techniques.
- More advanced and effective than existing system.
- Sky Shield avoids the reverse calculation process, which makes it efficient in real time anomaly detection.
- The experimentally results demonstrate that sky shield can effectively mitigate application layer DDoS attacks and pose a limited impact on normal users

VI. REFERENCES

[1] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," in Proc. SIGCOMM, 2004, pp. 39–53.

[2] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," Comput. Netw., vol. 44, no. 5, pp. 643–666, 2004.

[3] L.-C. Chen, T. A. Longstaff, and K. M. Carley, "Characterization of defense mechanisms against distributed denial of service attacks," Comput. Secur., vol. 23, no. 8, pp. 665–678, 2004.

[4] J. Mölsä, "Mitigating denial of service attacks: A tutorial," J. Comput. Secur., vol. 13, no. 6, pp. 807–837, 2005

[5] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack detection techniques," IEEE Internet Comput., vol. 10, no. 1, pp. 82–89, Jan. 2006.

[6] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the dos and DDoS problems," Comput. Surv., vol. 39, no. 1, p. 3, 2007.

[7] Guang Jin, Fei Zhang, Yuan Li, Honghao Zhang, and Jiangbo Qian, "A Hash-Based Path Identification Scheme for DDoS Attacks Defence,"2009 Ninth IEEE International Conference on Computer and In5. formation Technology, Xiamen, 2009, pp.219-224.

Dhanuja K C, received her Bachelor's degree in Computer Applications from Bangalore University, India and she is currently pursuing MCA in VTU, India.

Hitaishe Datta B, received her Bachelor's degree in Computer Applications from Bangalore University, India and she is currently pursuing MCA in VTU, India.

Harshita R, received her Bachelor's degree in Computer Applications from Bangalore University, India and she is currently pursuing MCA in VTU, India.

Mohan Kumar H P, obtained MCA,MSC Tech and PhD from University of Mysore India in 1998,2009 and 2015 respectively. He is working as a professor in department of MCA, PES College of Engineering, Mandya, Karnataka, India. His areas of interest are biometric, video analysis, networking and Data Mining