International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Approach to Detect and Block DDOS Attack at Application Layer Using Novel Framework

V. Mogal[1], Shekhar H. Pingale[2]

[1]Professor, Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

[2]Department of Computer Engineering, RMD Sinhgad School of Engineering, University of Pune, India

***Abstract:** Detection and prevention of DDoS is still an area of ongoing research. In network we can't stop attacker, instead we can have a secure methodologies in which we have a solution to DDOS attack. Present methodologies also lagging behind in such case. Here we are studying DDOS attack in network and explain the novel framework at application layer. Here we are trying to develop architecture which is having best result in real time. The required functionality can be added to existing web servers with a minimum of interference with the application code, or implemented in a separate network device.*

Keywords: Distributed denial of service (DDoS) attack, Application layer, Network, Website, Novel Framework.

1. Introduction

Motivation

A Denial of Service (DoS) attack usually either involves attackers sending messages to exploit certain vulnerabilities leading to the abnormality or paralysis of organization, or sending big amount of regular messages to a perticular node to interrupt the system resources resulting in business system failure . A Distributed Denial of Service (DDoS) attack is a DoS attack utilizing multiple distributed attack sources. Typically , the attackers use a large number of controlled bots (also referred to as zombies) distributed in different locations to launch a large number of DoS attacks against a single target or many targets. In case of Development of botnets in recent years, DDoS attacks are increasing, with the target's including not only network servers, but also network set ups such as firewalls, routers and DNS systems as well as network bandwidth.

Overview

Distributed denial-of-service (DDoS) attack make rejection of network resources to exact users. Denial of Service (DoS) is a major threat to network security. As the name implies, aims to deny the service of network resources to legitimate users. One of the most difficult to block forms of DoS is Distributed Denial of Service (DDoS) which uses hundreds or thousands of zombie machines to overwhelm target network devices such as routers and servers indefinitely interrupting or suspending services of a legitimate host connected to the Internet. The severity of DDoS (Distributed Denial of Service) attacks has steadily increased with new emerging attack techniques making detection even harder. A good example is recent reports that accuse North Korea of DDoS attacks on South Korea .On May 17 2007, massive DDoS attacks targeted on Estonia by sources inside Russia made the Internet service unavailable to the whole country. Resulting in financial losses. DDoS is an emerging cold war targeting the public Internet and to maintain public confidence ways must be found to eliminate this threat.

In the OSI model, the DDoS attacks may be targeted at different layers, many concentrate on the network layer. DDoS attacks aimed at network layer, such as ICMP flooding, SYN flooding and UDP flooding are called Net-DDoS attacks. Attacks aimed at the application layers are called App-DDoS. Flash traffic or a flash crowd is where a very large number of users simultaneously access a particular website and this produces a surge in traffic to the Website that might overwhelm a site. For example, websites such as online ticket booking, online share trading or even news websites may have a massive surge in legitimate traffic when there are new breaking events. DDoS and flash crowd traffic posess the same characteristics of bursty traffic with huge volumes so it is very difficult to identify the attack traffic. Detection methods must reject only the attack traffic or they will lose the legitimate (and possibly profitable) flash traffic. Many years ago it was acceptable to lose some legitimate traffic when attack traffic was blocked. In many cases today, such as e-Bay and online shopping, this lost legitimate traffic represents a financial loss that is no longer acceptable [1].

3. Application Layer Methods

- Implementing detection algorithms at the application layer is difficult when compared to network layer. Network blocking methods are carried out in a router or IDS and need not to be on the application's host machine. Blocking at the application layer usually requires one host run both the application and the DDoS detection and blocking software. Further the application may need to be modified to work with the DDoS software. Despite this problem, there are good reasons for working at the application layer and some good algorithms for DDoS detection and blocking [1].
- Ranjan et al and Yen et al used a statistical approach to detect the DDoS at the application layer. Ranjan et al employed rate limiting as the primary detection mechanism and Yen et al constraints any source that makes random web page requests. These statistical methods are used only for monitoring abnormal traffic but cannot distinguish flash traffic from attack traffic. Authors using CAPTCHAs (Completely Automated Public Turing

test to tell Computers and Humans Apart) to detect DDoS include Kandula et al and Boyd et al; implemented as a puzzle authentication mechanism. Users have to enter the letters shown in an image, which is very annoying. David Pogue stated that CAPCHA really stands for "Computer Annoying People with Time-wasting Challenges". Some references block DDoS by using special browsers with different security mechanisms but this limits the people who can access the site. Jung et al filters using IP addresses at the HTTP level but the algorithm will not work on DDoS attack which uses many legitimate IP addresses. The approach may also fail when NAT is used. The work of Yi Xie et al introduces a new way to monitor the DDoS attack using hidden semi Markov model, a key weakness is the assumption that new legitimate flash traffic will have the same statistics as older traffic but this is a highly questionable assumption as discussed earlier.

- Implementation of the Markov chain depends on the time from the first web page access Consider accessing 10 web pages at a web site, each has an acceptable time window based on the time from the first web page access. Variations in the viewing times of earlier web pages may push later web pages out of the acceptable range. As mentioned, all the techniques make the incorrect assumption that old traffic matches the statistics of new flash traffic. From the recent survey by Veronika et al confirms the necessity of new research on DDoS attack detection at the application layer. Overall, what is needed is a new algorithm at the application layer that does not punish legitimate flash traffic and successfully detects attack traffic.

4. Background

Due to Distributed denial of service (DDoS) attack in network servers suffer damages and will create Internet services problem . Traditionally, DDoS attacks are carried out at the network layer, such as ICMP flooding , and UDP flooding, which are called Net-DDoS attacks in this paper. The intent of these attacks is to consume the network bandwidth and deny service to legitimate users of the victim systems. Since many studies have noticed this type of attack and have proposed different schemes (e.g., network measure) to protect the network from attacks, it is not as easy as in the past for attackers to launch the DDoS attacks based on network layer. To misguide detection, they attack the Web servers by HTTP GET requests called as HTTP Flooding and pull big amount of image files from the victim server. In another case, attackers fire number of queries through the victim's search engine or database query to slow down server performance [2].We call such attacks application-layer DDoS (App-DDoS) attacks. The MyDoom worm and the CyberSlam are all instances of this type attack. Because burst traffic and high volume are the common characteristics of App-DDoS attacks and flash crowds, it is hard for current techniques to explain them merely with characteristics of traffic. Since, application layer DDOS attacks may be stealthier and more dangerous for the popular Websites than the general Net-DDoS attacks when they mimic (or hide in) the normal flash crowd.

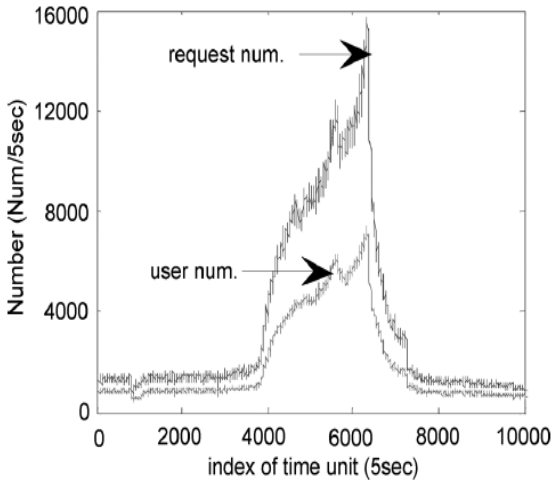

Figure 1: Flash Crowd

Cloud computing has created a lot of buzz lately and many companies have started venturing in this domain and providing cloud-based services. Likewise, most companies have also started moving some of their IT operations on the Cloud. Cloud computing has become the latest craze in a series of popular industry terms. Flexible computing is an adorable proposition; It offers convenience in setup, on-demand capacity and a highly dependable computing platform while requiring little maintenance. [3]With cloud computing, companies can scale up to massive capacities in an instant without having to invest in new infrastructure, train new personnel, or license new software. Cloud computing is benefitial to small and medium-sized businesses who wish to completely outsource their data-center infrastructure. In both instances, service consumers use what they need on the Internet and pay only for what they use.

- However, a DDoS can rack up a cloud adopter's utilization bill resulting in an economic DDoS (eDDoS). In an EDDoS, the elasticity of the cloud and surplus of available resources might be used in such a way that large botnets generating seemingly legitimate "targeted" requests for service causing the victim to cloud burst in order to keep pace with the scale of the requests. Distributed Denial of Services (DDoS) attacks target websites, hosted applications or network infrastructures by absorbing all available bandwidth. As cloud-based eDDoS mitigation mechanism itself is susceptible to eDDoS, it is imperative to drop eDDoS traffic before it triggers the billing mechanism. Most existing distributed denial-of-service (DDoS) mitigation proposals are reactive in nature, i.e., they are deployed to limit he damage caused by attacks after they are detected.
- We present congestion puzzles (CP), a new countermeasure to bandwidth-exhaustion attacks. A typical puzzle is composed of a moderately-hard function; solving the puzzle requires a brute-force search in the solution space [4]. Once a link adjacent to a router implementing the CP mechanism (a puzzle router) is congested, the router requires the traffic flow to be accompanied by a corresponding computation flow, i.e., a continuous flow of puzzle solutions, thereby imposing a computational burden on clients who transmit via this router. The rate of the computation flow (average number

of searching steps per second) is tied to the bandwidth consumed (bytes per second) by a puzzle-based rate limiter (PRL) implemented in the router. As a result, this coarsely requires from clients a computation flow commensurate with their bandwidth usage on the congested link, thereby impairing their ability to sustain a flooding attack. The consumption of CPU cycles in zombie computers may additionally alert the unwitting owners of those computers to their contribution to the attack, and motivate them to repair their computers.

- Distributed denial-of-service, [5] abbreviated as DDoS, attack is considered as one of the most serious attacks over internet. It is an attempt by the malicious users to make a networked resource unavailable to users. A DOS attack can be worked either by flooding a network or by disrupting a server by sending more requests than it can possibly handle. There are many other forms of DDoS attacks. A better taxonomy is available in. High-profile internet servers as well as premium sites with huge customer utilization are the basic targets of the attackers.
- Availability attacks, or denial-of-service (DoS), pose [6] significant problems to enterprise networks as they attack the core of the information economy paradigm—connectivity. These attacks prevent legitimate network users from accessing services or resources to which they are entitled. In addition, these at- tacks may target a remote host or network that would otherwise be used to serve legitimate users. Such attacks can be launched in a number of ways, from malicious use of common applications such as e-mail, to subverting Internet protocols. Irrespective of the modus operandi, DoS attacks are prevalent as the tools needed for such attacks are freely available on the Internet, simple to launch, effective, and difficult to prevent. Thus, large numbers of attacks are continuously being launched.
- A DDoS attack is a simultaneous network attack on a victim (e.g., a Web server or a router) from a large number of compromised hosts, [7] which may be distributed widely among different, independent networks. By exploiting asymmetry between network-wide resources and local capacities of a victim, a DDoS attack can build up an intended congestion very quickly at an attacked target. The Internet routing infrastructure, which is stateless and based mainly on destination addresses, appears extremely vulnerable to such coordinated attacks.

5. Architecture

The dotted arrow represents the flow of signatures and continuous line represents the flow of web requests. The web request made by 1st, 2nd, 3rd and Nth user are represented as USER 1, USER 2, USER 3, and USER N. The signature generator analyse the web page requests and timing, generates signatures for each user and updates the signature database.It depicts a key novel aspect of the algorithm in that the user's signatures are calibrated using occasional CAPTCHAs or AYAH (Are You A Human) page. A signature is generated for each user that determines whether a user is "suspicious" or not.

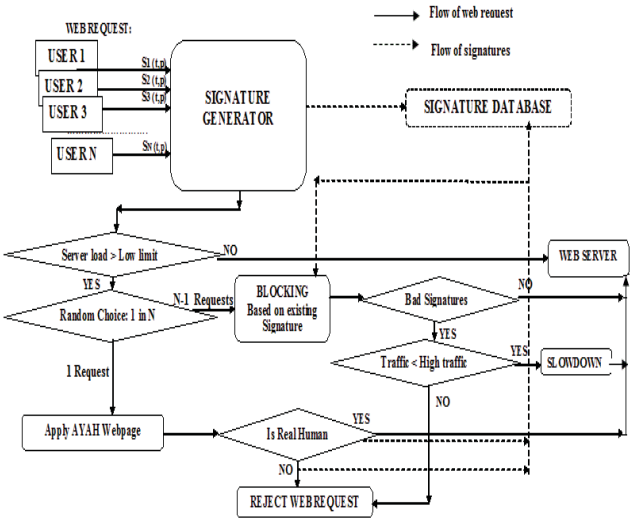

Figure 2: System Architecture

The AYAH result allows dynamic determination of whether a signature really represents an attack or non-human user like robots, or a legitimate human user. This calibration provides a measure of certainty which is missing in other published methods and so satisfies a major objective of our work, not to punish human traffic (which may relate to profit and income) while blocking the DDoS attack and robots (which do not provide any income).Without this calibration provided by the occasional AYAH page this goal would not be achievable.

6. Conclusion

The modern web is now relied upon by many people for fast and certain information. It is becoming an important commercial highway and as such its performance must be protected and enhanced. It is no longer acceptable to block both attack traffic and legitimate users as this will reduce reliability, performance and profitability of a web site.

References

[1] A Novel Framework to detect and block DDoS attack at the Application layer Sujatha Sivabalan, Dr P J Radcliffe, IEEE 2013.
[2] Monitoring the Application-Layer DDoS Attacks for Popular Websites Yi Xie and Shun-Zheng Yu, Member, IEEE 2009.
[3] Mitigation of Economic Distributed Denial of Sustainability (EDDoS) in cloud computing International Conference on Advances in Engineering and Technology, (ICAET-2011), May 27-28, 2011.
[4] Mitigating Bandwidth-Exhaustion Attacks using Congestion Puzzles ACM, 2004.
[5] Defending against Distributed Denial-of-Service Attacks with Weight-Fair Router Throttles.
[6] Early Detection and Prevention of Denial-of-Service Attacks: A Novel Mechanism With Propagated Traced-Back Attack Blocking, IEEE 2005.
[7] Monitoring the Macroscopic Effect of DDoS Flooding Attacks, IEEE 2005.

Author Profile

Prof. V. Mogal received the B.E. and M.E. Degrees in Computer engineering. He is working as Assistant Professor in Department of Computer Engineering, RMD Sinhgad School of Engineering Pune, India.

Shekhar Pingale Reseach Scholar at RMD Sinhgad School of Engineering, University of Pune. He has received B.E. in Computer Engineering from University of Pune, Pune. Currently he is pursuing M.E. in Computer Engineering from RMD Sinhgad School of Engineering, Pune, University of Pune, Pune